

## NIS Supplementary Guidance and CAF Overlay for DGE Sector

<b>Publication date:</b>	01/08/2023	<b>Contact:</b>	Cyber Security Team
		<b>Directorate:</b>	Cyber Regulation
		<b>Tel:</b>	N/A
		<b>Email:</b>	<a href="mailto:cybersecurityteam@ofgem.gov.uk">cybersecurityteam@ofgem.gov.uk</a>

### Overview

This document is for Operators of Essential Services (OES), as defined within the Network and Information Systems Regulations 2018 (NIS Regulations), with undertakings in the Downstream Gas and Electricity (DGE) sectors in Great Britain.

The document provides DGE sector-specific guidance to OES which will assist them to achieve and demonstrate the security outcomes in the NCSC's Cyber Assessment Framework (CAF). Effective use of the CAF, and this DGE supplementary guidance, will assist OES in meeting their security duties as set out at Regulation 10 of the NIS Regulations.

---

## Revision History

No.	Date	Change Summary
1.0	13th Dec 2022	Initial Version
2.0	1st August 2023	Final Version revised to incorporate feedback from consultation
3.0	06 February 2024	Modified to improve accessibility prior to publication on Ofgem Website

© Crown copyright 2023

The text of this document may be reproduced (excluding logos) under and in accordance with the terms of the [Open Government Licence](#).

Without prejudice to the generality of the terms of the Open Government Licence the material that is reproduced must be acknowledged as Crown copyright and the document title of this document must be specified in that acknowledgement.

Any enquiries related to the text of this publication should be sent to Ofgem at:

10 South Colonnade, Canary Wharf, London, E14 4PU. Alternatively, please call Ofgem on 0207 901 7000.

This publication is available at [www.ofgem.gov.uk](http://www.ofgem.gov.uk). Any enquiries regarding the use and re-use of this information resource should be sent to: [psi@nationalarchives.gsi.gov.uk](mailto:psi@nationalarchives.gsi.gov.uk)

---

## Contents

List of Tables.....	5
NIS Supplementary Guidance and CAF Overlay for DGE Sector.....	6
Introduction.....	7
Status of NIS Supplementary Guidance and CAF Overlay for DGE Sector.....	9
Document Aim.....	9
How should OES assess the appropriateness of security measures?.....	11
How should OES assess the proportionality of security measures?.....	16
Cyber-security for obsolete devices.....	17
Management of physical risks to network and information systems.....	18
Capturing NIS Scope.....	19
Cyber Security Management Systems (CSMS).....	20
Evidential Requirements.....	21
Annexes.....	22
Annex A - Document Map.....	24
Annex B - CAF Overlay.....	26
Annex B.1 - Objective A - Managing Security Risk.....	28
A1 Governance.....	28
A2 Risk management.....	41
A3 Asset Management.....	55
A4 Supply Chain.....	61
Annex B.2 - Objective B – Protecting against cyber attacks.....	73
B1 Protection Policies and Processes.....	73
B2 Identity and Access Control.....	84
B3 Data security.....	105
B4 System Security.....	122
B5 Resilient networks and systems.....	142
B6 Staff awareness and training.....	151
Annex B.3 - Objective C. Detecting cyber security events.....	156
C1 Security monitoring.....	156
C2 Proactive Security Event Discovery.....	211
Annex B.4 - Objective D. Minimising the impact of cyber security incidents.....	223
D1 Response and Recovery Planning.....	223

---

D2 Lessons learned .....	259
Annex C – Ofgem Supplementary Objective – Physical Security, Principles and Guidance .....	273
Annex C.1 - Objective E: Protecting against non-cyber risks.....	273
Principle E1: Physical security of network and information systems .....	274
Principle E2: Broader network and information systems resilience risks.....	283
Annex D – Representative Scopes .....	286
Background.....	286
Aim.....	287
Use of Functional Viewpoints .....	287
Customer Impact Thresholds and Site Criticality .....	287
Time to Impact.....	288
Functional Viewpoints .....	290
Electricity Transmission, ESO and Interconnector.....	290
Gas Transmission, Distribution and Interconnector.....	290
Electricity Distribution.....	290
Generation.....	290
Annex E – Cyber Security Framework Mappings .....	291
Annex E-1 – NIST CSF to CAF.....	291
Annex E-2 - Mitre Attack-ICS to CAF.....	304
Annex E-3 – Mitre Enterprise to CAF .....	313
Annex E-4 – ISO27002/19 to CAF .....	318
Annex E-5 – ISA/IEC 62443-2-1 mapped to CAF .....	328
Annex E-6 – ISA/IEC 62443-3-3 mapped to CAF .....	335

---

## List of Tables

Table 1 - Document Relationships .....	10
Table 2 - Risk Assessment and Security Activity Sequencing .....	13
Table 3 - Mapping of NIST Cyber Security Framework to CAF.....	291
Table 4 - Mitre Attack-ICS mitigations mapped to the CAF.....	304
Table 5 - Mitre Enterprise mitigations mapped to the CAF.....	313
Table 6 - ISO / IEC 27002-19 Controls mapped to the CAF.....	318
Table 7 - IEC 62443-2-1:2009 Security Requirements mapped to the CAF.....	328
Table 8 - IEC 62443-3-3:2013 Security Requirements mapped to the CAF.....	335

# **NIS Supplementary Guidance and CAF Overlay for DGE Sector**

---

## Introduction

1.1. This document is for Operators of Essential Services (OES), as defined by the Network and Information Systems Regulations 2018 (as amended) (NIS-R), within the downstream gas and electricity<sup>1</sup> (DGE) sector in Great Britain.

1.2. This document supplements Ofgem's existing NIS Guidance for DGE v2.0<sup>2</sup> and complements the NCSC's Cyber Assessment Framework (CAF) Collection<sup>3</sup>. The relationships between these documents are described in Table 1 and illustrated at Annex A.

1.3. NIS-R, Ofgem's NIS Guidance for DGE v2.0, and NCSC's CAF, all follow an outcomes-based regulatory approach, which gives OES the freedom to choose security systems and controls that are tailored to their specific requirements. However, it is acknowledged<sup>4</sup> that this approach has the potential to create uncertainty for OES, particularly regarding whether chosen solutions are sufficient to meet Ofgem's regulatory expectations. This document is intended to reduce uncertainty by describing Ofgem's expectations through the use of the CAF, the CAF profiles and Ofgem's CAF overlay. Ofgem uses each of these documents in the following way:

- a. NCSC's CAF – Ofgem uses the CAF as a means of systematically and comprehensively assessing the extent to which cyber risks are being managed by OES.
- b. NCSC's CAF Profiles – Ofgem uses the CAF profiles as follows:
  1. The Basic Profile (BP) is used to describe a level of cyber resilience that is appropriate to defend against limited capability attacks. Ofgem have used the BP as a reference point that OES were expected to have met by May '20 and then have moved quickly beyond.
  2. Since its release, the Enhanced Profile (EP) has been used to represent the joint Competent Authorities (CA's) initial view of what the appropriate and

---

<sup>1</sup> This refers to OES within the electricity subsector as set out at paragraph 1 and the gas subsector as set out at paragraph 3 (with the exception of sub-paragraphs 3(5) to (8)) of Schedule 2 of the NIS Regulations.

<sup>2</sup> Ofgem, NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in Great Britain v2.0, dated 1 Apr 2022.

<sup>3</sup> [NCSC CAF guidance - NCSC.GOV.UK](https://www.ncsc.gov.uk/ncsc-caf-guidance)

<sup>4</sup> See DESNZ (formally BEIS), Goals-Based and Rules-Based Approaches to Regulation, BEIS Research Paper Number 8, dated May 2018 for an analysis of outcomes/goals-based approaches to regulation.

proportionate security measures are, in relation to regulation 10<sup>5</sup>. Use of the word 'initial' acknowledges that this view is likely to be modified by an OES' own risk assessment. The EP uses the Indicators of Good Practice (IGPs) in the CAF to detail indicative actions and behaviours that illustrate or exemplify achievement of a contributing outcome. The IGPs are provided on a non-binding basis with the intention of guiding OES toward achieving and demonstrating attainment of the security outcomes.

- c. Ofgem's CAF Overlay – Ofgem uses the CAF Overlay to provide sector-specific interpretations of the CAF contributing outcomes and IGPs. The aim is to better clarify their meaning within the DGE sector and help OES to demonstrate their attainment. The information provided in Ofgem's interpretations detail indicative actions and behaviours that illustrate or exemplify achievement of a contributing outcome. The interpretations are provided on a non-binding basis with the intention of guiding OES toward achieving and demonstrating attainment of the security outcomes.

1.4. In addition to Ofgem's NIS guidance for DGE v2.0, Ofgem has also published its RIIO-2 Cyber Resilience Guidelines<sup>6</sup>. The guidelines were only issued to those OES subject to the RIIO price control mechanism. They were intended to assist in the development of OES' Cyber Resilience OT plans which are submitted as part of the RIIO-2 process. Several OES have made extensive use of these guidelines and have used them to inform their NIS compliance frameworks<sup>7</sup> as well as their RIIO-2 resilience plans.

1.5. Ofgem has built upon the success of the RIIO-2 Cyber Guidelines by producing the CAF overlays which are included as an annex to this document. The CAF overlays draw heavily from the RIIO-2 Cyber Guidelines and provide additional guidance derived from Ofgem's experience of implementing the NIS Regulations. In contrast to the RIIO-2 Cyber Guidelines, the CAF overlays have been produced for the benefit of all<sup>8</sup> DGE OES, thereby increasing their utility and contributing to standardisation across the whole sector. It is intended that the CAF overlays will replace the RIIO-2 Cyber Guidelines. However, there will be a period of dual running for price-controlled OES during which

---

<sup>5</sup> Regulation 10 of NIS-R

<sup>6</sup> Ofgem RIIO-2 Cyber Resilience Guidelines, dated 05 Feb 2020.

<sup>7</sup> It is important to note that the RIIO Cyber Resilience Guidelines were not written as a compliance benchmark, the document provides guidelines and is not a set of requirements.

<sup>8</sup> RIIO price controlled and non RIIO price controlled.



either document can be used. This period will last for 6 months following the publication of our decision document and is intended to minimise disruption to those OES who are currently relying upon RIIO-2 guidelines to help inform their self-assessments or NIS inspection preparations. The relationships between the documents are described in Table 1.

## **Status of NIS Supplementary Guidance and CAF Overlay for DGE Sector**

1.6. Responsibility for compliance with the NIS Regulations lies with OES boards and management teams. Ofgem guidance is intended to support OES in achieving and maintaining compliance. OES should not rely solely on Ofgem guidance for this purpose. OES should seek such legal or other professional advice as they consider appropriate to ensure compliance with their obligations under the NIS Regulations.

1.7. Any references to external resources made in the guidance are correct and applicable at time of publication. It remains an OES's responsibility to verify if such resources are applicable to it at any given point in time and in so doing ensure ongoing compliance with NIS Regulations. OES are responsible for seeking such independent legal or other professional advice as they may need where there are changes or variation to the content or context of any such external resources to ensure they remain in compliance with the NIS Regulations.

1.8. The guidance contained in this document (including any external resources referenced in the guidance) is not exhaustive. The guidance does not state the law and is not intended to provide a comprehensive guide to compliance with the NIS Regulations. The guidance sets out Ofgem's interpretation of certain relevant obligations under the NIS Regulations and Ofgem's expectations associated with the same.

## **Document Aim**

1.9. The aim of this document is to reduce uncertainty for OES by clarifying Ofgem's expectations regarding the appropriateness and proportionality of security measures. This is achieved by:

- a. responding to questions that are frequently asked by OES during NIS engagement sessions<sup>9</sup>. These questions are:

---

<sup>9</sup> Engagement sessions are routine meetings during which Ofgem assists OES to understand and meet their NIS security duties.

1. how should OES assess the appropriateness of security measures?
  2. how should OES assess the proportionality of security measures?
  3. what security outcomes do OES need to demonstrate regarding management of physical risks to network and information systems?
  4. how should OES manage cyber-security for obsolete devices?
- b. providing guidance<sup>10</sup> that will help OES to avoid common NIS regime non-conformities which have been identified during Ofgem’s NIS inspections. These common non-conformities are:
1. inadequate definition of NIS Scope.
  2. inadequate implementation of Cyber Security Management Systems (CSMS).
  3. inadequate presentation of evidence.
- c. detailing Ofgem’s interpretations of the CAF Indicators of Good Practice (IGPs). These interpretations are presented as a DGE Sector CAF Overlay in Annex B. The interpretations describe the type and nature of security measures that Ofgem would typically<sup>11</sup> expect to see implemented by an OES. These interpretations complement NCSC’s CAF Guidance.

*Table 1 - Document Relationships*

<b>Document</b>	<b>Relationship to the NIS Supplementary Guidance and Overlay for the DGE Sector (this document)</b>
Ofgem NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in Great Britain v2.0	Ofgem’s NIS guidance describes the activities that OES are required to complete as part of their NIS compliance framework. These activities include scoping, CAF self-assessments, and the production of cyber improvement plans.

<sup>10</sup> This guidance supplements that provided in Ofgem’s NIS Guidance for DGE.

<sup>11</sup> The use of the word ‘typically’ acknowledges that there will be relevant factors and special circumstances in which security objectives may be better achieved via alternative means. These circumstances will be identified through the OES’ own risk assessment process.

	<p>Ofgem’s NIS Supplementary Guidance and CAF Overlay (this document) provides guidance to help OES complete these activities.</p>
<p>NCSC CAF Collection</p>	<p>The NCSC’s CAF collection has been designed to <i>‘help an organisation achieve and demonstrate an appropriate level of cyber resilience in relation to certain specified essential functions performed by that organisation’</i>.</p> <p>Ofgem’s NIS Supplementary Guidance and CAF Overlay (this document) interprets the CAF IGPs. These interpretations aim to clarify Ofgem’s regulatory expectations, whilst retaining an outcomes-based approach.</p>
<p>Ofgem RIIO-2 Cyber Resilience Guidelines</p>	<p>Ofgem’s RIIO guidelines were produced to assist RIIO price-controlled OES in the development of the Cyber Resilience OT plans. The guidance was written to supplement the information provided in the CAF and draws on the following sources: NCSC website, ISO 27019, IEC 62443, NIST 800-82, HSE OG86.</p> <p>Ofgem’s NIS Supplementary Guidance and CAF Overlay (this document) has incorporated much of the guidance provided in the RIIO-2 Cyber Resilience Guidelines and provides additional guidance which is derived from Ofgem’s recent NIS experience. It will be issued to all OES, thereby increasing its utility and contributing to standardisation across the whole sector. The RIIO-2 guidance will be withdrawn 6 months after the publication of our decision document.</p>

## **How should OES assess the appropriateness of security measures?**

1.10. NCSC have designed the CAF as a tool for assessing cyber resilience. The CAF describes a systematic and comprehensive approach that enables an organisation to assess the extent to which it is managing its cyber risks. The CAF is presented as a set

---

of IGP tables, each of which relate to a specific security outcome and its associated objectives and principles.

1.11. The IGP tables themselves are only a sub-set of the wider CAF Collection. The CAF Collection also contains a 'CAF – Principles and Guidance' webpage which provides descriptions and guidance notes that relate to the IGPs in the CAF tables. These descriptions, and associated references, are intended to assist OES to select **appropriate** security controls.

1.12. OES are not limited to using sources of guidance referenced by the CAF Collection and are free to use alternative guidance as they see fit. However, OES are to be aware that Ofgem uses the CAF collection as its primary source of reference when making determinations as to the **appropriateness** of security controls.

1.13. Ofgem's NIS Guidance for DGE v2.0 explains that that *'the relationships between scoping, risk management, position against the CAF and improvement plans are key when considering whether certain measures are **appropriate** and proportionate'*. The following paragraphs provide supplementary guidance on how the relationships between these four factors influence Ofgem's assessment of the **appropriateness** of security measures.

- a. Scoping – Accurate scoping is fundamental to network and information system cyber resilience and this requirement is explained in more detail at para 1.30 and in Ofgem's NIS Guidance for DGE v2.0. Ofgem's view is that if an OES fails to accurately capture its scope, it will have failed to appropriately manage its NIS security risks.
- b. Risk Management and Improvement Plans – Ofgem has identified three issues relating to existing guidance on NIS risk management that have to led to confusion. These three issues, and Ofgem's clarifications, are as follows:

**Issue 1** – Ofgem's NIS Guidance for DGE v2.0 lists 'risk management' and 'position against the CAF' as 2 separate factors in the determination of **appropriateness**, even though risk management is embedded within the CAF as a discrete principle. This has caused confusion regarding how risk assessments are to be sequenced, and how the output of the risk assessments is to be used alongside with the CAF.

**Clarification 1** – Ofgem generally<sup>12</sup> only expects OES to implement and demonstrate a single cyber risk management process. Ofgem expects OES to sequence their risk assessment and CAF assessments as described in Table 2<sup>13</sup>.

*Table 2 – Risk Assessment and Security Activity Sequencing*

Step	Activity	Output
1	<b>Scoping</b> – Identify all network and information systems on which the essential service relies, or which are used for the provision of the essential service.	Scoping document presented in accordance with Part A of Ofgem’s NIS Guidance for DGE v2.0.
2	<b>Risk Assessment</b> – Conduct risk assessment against complete NIS scope.	Prioritised risk register.
3	<b>Improvement Plan</b> – Develop NIS security improvement plan based on prioritised risk register.	NIS improvement plan and initial target security posture <sup>14</sup> .
4	<b>Gap Analysis</b> – Use the CAF and relevant CAF profile to assess the initial target security posture.	Gap analysis between the relevant CAF profile and initial target security posture.  The gap analysis may identify instances where the initial target security posture falls short of the relevant CAF profile (a negative gap) and instances where it exceeds the relevant CAF profile (a positive gap).
5	<b>Revised Improvement Plan</b> – Assess each gap (identified by gap analysis) and determine required action. Actions will be either:  For negative gaps:	1. Revised improvement plan.  2. A completed DGE Sector CAF Report Template (v3.0). The CAF report will provide details of any systems that are deviating from the CAF profiles. These systems are to be listed at Table 0 of

<sup>12</sup> There may be circumstances in which an OES chooses to conduct multiple risk assessments.

<sup>13</sup> OES are to be aware that steps 2-5 are cyclic and that the process of risk management is continuous. This process is illustrated at Figure 1 of Ofgem’s NIS Guidance for DGE v2.0.

<sup>14</sup> The combination of the OES’ existing security posture (the as-is security state) and a fully delivered improvement plan describes the target security posture (the to-be security state).

	<ol style="list-style-type: none"> <li>1. Accept the recommendation of the profile and revise the improvement plan so your security practises match the profile.</li> <li>2. Reject the recommendation of the profile and leave the improvement plan as-is. This amounts to a planned deviation from the relevant CAF profile.</li> </ol> <p>For positive gaps:</p> <ol style="list-style-type: none"> <li>1. Accept the recommendation of the risk assessment and leave the improvement plan as-is.</li> <li>2. Assess that the initial target security posture presents an unrealistic goal at this time, and revise improvement plan down, so that it meets the profile (rather than exceeds it).</li> </ol>	<p>the template (List of Exception Systems). The CAF report will also provide details of any relevant factors and special circumstances that OES have considered when making their self-assessment decisions for each contributing outcome.</p>
--	---	---

**Issue 2** – Ofgem considers it inappropriate for OES to use the IGP tables as an inflexible and exhaustive checklist to be applied verbatim<sup>15</sup>. Using the tables in this way fails to take account of the OES’ own risk assessment.

**Clarification 2** – Ofgem expects OES to meet the attainment levels<sup>16</sup> for contributing outcomes as specified in the relevant CAF profile. However, assessment of contributing outcomes is primarily a matter of expert judgement. The indicators in the IGP tables will usually provide good starting points for these judgements but should be used flexibly and in conjunction with guidance contained in NCSC’s CAF collection. Conclusions about the level of attainment against the CAF contributing outcomes can only be drawn after considering additional relevant factors and special circumstances. This means that it is feasible for OES to meet achievement levels specified in the profiles without

<sup>15</sup> NCSC’s CAF guidance states that CAF tables are not to be used in this way.

<sup>16</sup> Attainment levels are defined in the profiles as a RAG assessment for each contributing outcome and are linked to specified IGPs.

demonstrating all the specified IGPs. OES can choose to provide evidence to demonstrate the requisite achievement level by evidencing the specified IGPs, or by alternate means which the OES considers more appropriate.

Ofgem acknowledges that within the NCSC CAF tables the language for the 'Achieved' and 'Partially Achieved' columns for each of the contributing outcomes includes the instruction that 'All of the following statements [IGPs] are true'<sup>17</sup>. This gives the impression that there is a requirement for all IGPs to be achieved, contradicting the outcomes-based approach. However, the documentation provided by NCSC to support OES in their use of the CAF<sup>18</sup> makes it clear that the intent is for assessments to be made using an outcomes-based approach. Ofgem reiterates that OES should take this outcomes-based approach when completing their self-assessments.

**Issue 3** – The NCSC use descriptions of attacker sophistication to describe the levels of resilience offered by the CAF profiles. This has led some OES to believe that they are only required to consider the threats presented by attackers that match these descriptions of attacker sophistications.

**Clarification 3** – Ofgem expects OES to develop their risk assessments (Step 2 of Table 2) based on the assumption that they will be subject to threats from the full range of attacker capabilities. This includes espionage and targeted attacks from malicious actors such as hostile states and criminals<sup>19</sup>. Doing so will ensure that risk assessments are comprehensive. Steps 4 and 5<sup>20</sup> of Table 2 describe how OES can use then use the CAF profiles to justify why they have not fully mitigated risks that are only associated with sophisticated attackers.

1.14. Ofgem has produced a DGE sector CAF overlay to help OES to understand Ofgem's sector-specific expectations and to achieve and demonstrate those IGPs which they (the OES) have selected as being **appropriate** and proportionate. The overlay details Ofgem's interpretations of the CAF IGPs. The interpretations have been provided in instances where Ofgem feels it beneficial to:

- a. provide Ofgem's interpretations of specific words or phrases used in the CAF and to clarify their meaning in the context of the DGE sector.

---

<sup>17</sup> Ofgem is in discussion with NCSC regarding the possibility of changing this text used in future versions of the CAF tables.

<sup>18</sup> NCSC's Introduction to the CAF can be found at: [Cyber Assessment Framework - NCSC.GOV.UK](https://www.ncsc.gov.uk/industry/cyber-assessment-framework)

<sup>19</sup> [CNI Hub - NCSC.GOV.UK](https://www.ncsc.gov.uk/industry/cni-hub)

<sup>20</sup> This situation is discussed as a positive gap.

- b. describe the types of evidence that Ofgem would typically expect to see during NIS inspections. This evidence would enable OES to effectively and efficiently demonstrate that they are achieving the contributing outcomes.

## **How should OES assess the proportionality of security measures?**

1.15. CAF Profiles are produced by the NCSC in consultation with the DGE joint Competent Authority<sup>21</sup>. NCSC's website states that they are intended to '*correspond to an **initial** view of appropriate and **proportionate** cyber security for that organisation*'<sup>22</sup>. CAF profiles can only provide an **initial** view of proportionality as, in accordance with the outcomes-based approach, it is also necessary to take an OES' risk assessment into account.

1.16. As the joint Competent Authority, we use profiles to communicate our initial expectation of the attainment levels necessary to provide resilience against differing levels of attacker sophistication<sup>23</sup>. The profiles are described below:

- a. The Basic Profile describes a level of cyber resilience matched to the threat presented by attackers employing unsophisticated techniques.
- b. The Enhanced Profile describes a level of cyber resilience matched to the threat presented by attackers employing moderately sophisticated techniques.

1.17. As the joint Competent Authority, we may periodically update the expected cyber resilience attainment levels for the DGE subsector. The current expectations are documented in DESNZ's '*Initial Target Attainment Levels of Expected Cyber Resilience by the DGE Subsectors*'. The expected attainment levels are described in terms of resilience against differing levels of attacker sophistication and the associated CAF profiles.

1.18. It is acceptable, and sometimes necessary, for an OES to deviate from a CAF profile either by exceeding it or by not achieving it. Such decisions will need to be made

---

<sup>21</sup> Department for Energy Security and Net Zero (DESNZ) (formally the Department for Business, Energy & Industrial Strategy (BEIS)) and Ofgem are the designated DGE joint Competent Authority.

<sup>22</sup> Where the organisation in question is the organisation on which the assessment framework is being applied.

<sup>23</sup> OES are to be aware that the CA may issue further, more demanding, profiles in the future.



on a system-by-system basis. OES may find it necessary to exceed the target set by a profile where their own risk appetite has determined that it is necessary to do so. Examples would be where an OES' risk assessment has identified a specific threat that will clearly overmatch the security controls described by the target profile. Conversely, OES may choose not to meet a profile where their own risk assessment for a specific system has determined that the profiles achievement levels and/or the IGPs are neither appropriate nor proportionate.

1.19. The Competent Authority uses CAF Profiles as **initial** targets for the purpose of assessing NIS compliance. The use of the word initial provides OES with the freedom to deviate from the profiles, on a system-by-system basis, in accordance with their view of appropriate and proportionate security controls. Ofgem's DGE Sector CAF Report Template v3.0 enables OES to document and justify these deviations.

## **Cyber-security for obsolete devices**

1.20. NCSC provides guidance on the management of obsolete products as part of its device security guidance. This guidance is equally applicable to Information Technology (IT) and Operational Technology (OT) environments and will assist OES to appropriately and proportionately manage obsolete devices.

1.21. Ofgem, uses the term obsolete to describe devices that are no longer receiving security updates or are older products that lack the latest security measures. This definition is the same as that used by NCSC. Ofgem recognises that some OES in the DGE sector employ a high proportion of devices that lack the latest security measures but continue to be functional from an engineering perspective. Consequently, some OES describe these devices as legacy, rather than obsolete. Ofgem considers that, from a NIS reporting perspective, the term obsolete is more appropriate as it is referring specifically to security functionality and aligns with the terminology used by NCSC.

1.22. The prevalence of obsolete devices in the OT estates of OES, and the risk they present, means that Ofgem expects specific assurances that the security of obsolete devices is being appropriately managed. Details of these assurances can be found in the DGE CAF overlay, under A3.a (Asset Management).

1.23. If OES take a risk-based decision to continue to use obsolete devices, Ofgem will expect them to implement compensating controls to mitigate the residual risks. Securely designed network and information systems (Secure by Design) are considered to be the most appropriate means for reducing the risks posed by obsolete devices. In instances

where an OES is employing obsolete devices that present a significant risk to the functioning of the essential service, Ofgem will expect the OES to evidence network architectures that incorporate secure-by-design principles<sup>24</sup>. Ofgem will assess the adequacy of these designs on a case-by-case basis. Ofgem encourages OES to discuss the issue of obsolete devices during engagement sessions.

## **Management of physical risks to network and information systems**

1.24. The Department for Science, Innovation and Technology (DSIT)<sup>25</sup> has the role of overseeing the implementation of the NIS Regulations across the UK. DSIT's interpretation of OES' security duties<sup>26</sup> includes the management of the risk of physical events that might have an adverse effect on networks and information systems.

1.25. The NCSC have produced the CAF collection to assist organisations improve the security of network and information systems. The CAF collection focuses on cyber-based threats to networks and also covers supply chain and personnel risks. However, the CAF's treatment of physical risk is limited<sup>27</sup>.

1.26. Ofgem, in consultation with the National Protective Security Authority (NPSA)<sup>28</sup> have produced a DGE supplementary security objective, DGE Objective E. Objective E is intended to help OES achieve and demonstrate appropriate and proportionate management of physical risks that could impact network and information systems. Objective E can be found at Annex C. To help with consistency and ease of understanding, Ofgem have produced DGE Objective E in the same format as NCSC's CAF security objectives<sup>29</sup>. DGE Objective E specifies security outcomes relating to two distinct categories of physical risk. Principle E1 relates to the risks presented by malicious threat actors gaining physical access to the components of network and information systems. Principle E2 relates to non-malicious risks such as those caused by environmental hazards and accidents.

---

<sup>24</sup> Secure by Design principles are described at CAF Objective B4.a.

<sup>25</sup> Formally the Department for Digital, Culture, Media and Sport (DCMS).

<sup>26</sup> DSIT, Security of Network and Information Systems, Guidance for Competent Authorities, dated Apr 2018.

<sup>27</sup> This is intentional as the National Protective Security Authority (NPSA) is responsible for the provision of technical guidance on the management of physical security risk.

<sup>28</sup> Formally known as the Centre for the Protection of National Infrastructure (CPNI).

<sup>29</sup> OES should note that the NCSC is not involved in the production or maintenance of DGE Objective E. All queries relating to DGE Objective E should be directed to Ofgem.

1.27. Objective E makes numerous references to the NPSA website and extranet. These sites host a wide range of relevant advice, guidance and resources on the subject of physical and personnel protective security. OES are to be aware that the NPSA's advice is not intended solely for Critical National Infrastructure (CNI). NPSA's mission is 'building resilience to national security threats', meaning that the advice and guidance that it publishes is relevant to OES sites that are CNI and non-CNI. Furthermore, this advice and guidance has been developed such that it is scalable to meet the diverse security requirements of a broad range of users and follows a risk-based methodology. Ofgem will use the NPSA's website as its primary source of reference when making determinations as to an OES' level of attainment against the contributing outcomes in Objective E.

1.28. Objective E provides guidance that will assist OES in meeting Ofgem's expectations regarding appropriate and proportionate management of physical risks to network and information systems. Objective E emphasises the importance of the governance structures and risk management processes that lead to effective management of physical risk and signposts the expert guidance that is provided on the NPSA's internet and extranet sites. Objective E does not, and is not intended to, provide detailed guidance on the design and specification of specific physical security controls.

1.29. Ofgem expects OES to incorporate DGE Objective E into their security management systems and to include it in all future self-assessment submissions.

## **Capturing NIS Scope**

1.30. Assuring the resilience of the network and information systems that are used for provision of the essential services, or on which the essential service relies, is dependent on accurately defining the systems that are in scope. The principles to be used to define scope, and the processes to be used to document it, are specified in Part A of Ofgem's NIS Guidance for DGE v2.0.

1.31. Annex D gives examples of scopes for each of the DGE sub-sectors. Those being, Electrical Transmission and Interconnectors, Electrical Distribution, Gas Distribution and Transmission, Generation and System Operators. These example scopes illustrate the type of network and information systems that Ofgem would expect to see in scoping documents for OES in each sub-sector. It is intended that OES use these examples to prompt the further development of their own scoping documents. The examples are indicative only, and OES may identify network and information systems in their own

scopes that are not represented in the examples. It is also possible that some OES determine that their essential services do not rely on the systems represented on the examples. Ofgem may require OES to explain these decisions during engagement and feedback sessions.

1.32. When developing their scopes from the examples, OES should ensure that their view of the essential service is sufficiently broad to capture all the networks and information systems on which they rely to meet the conditions of their licence<sup>30</sup>, and relevant regulations and codes. These conditions include (but are not limited to) those relating to safety, quality of supply, data exchange and emergency response.

1.33. Ofgem expects OES to have regard to the relevant example scope detailed at Annex D, meaning that they should use the examples as a start point for fully defining their own scopes.

## **Cyber Security Management Systems (CSMS)**

1.34. The CAF requires that OES have developed a set of policies and processes which govern the approach to their security of network and information systems. This suite of documentation is referred to in Ofgem's NIS Guidance for DGE v2.0 as a security management system<sup>31</sup>.

1.35. Observations made during Ofgem's initial NIS inspections have revealed that some OES rely on CAF self-assessments as their sole means of security management. It is important for OES to recognise that the act of conducting a CAF self-assessment does not equate to implementing a security management system. The CAF self-assessment is a tool by which an OES assesses the effectiveness of the underlying security management system (comprising of the necessary structures, policies and processes). A CAF self-assessment **is not** a security management system in its own right, even when it is accompanied by a security improvement plan.

1.36. The NIS scope for most OES will include OT and IT systems. This is because most OES host applications and services on their IT environments that their essential service relies upon. Most notably, these services will include the IT network boundary protection

---

<sup>30</sup> Gas Transporter, Gas Interconnector, Electricity Transmission, Electricity Distribution, Electricity Generation licenses

<sup>31</sup> Such management systems are also referred to as Information Security Management Systems (ISMS) – which are often associated with enterprise networks – and Cyber Security Management Systems (CSMS) – which are often associated with OT networks.

and security services, all of which the essential service relies upon as part of its defence in depth. Therefore, it is feasible that some of an OES' NIS scope is managed under an Information Security Management System (ISMS) by an IT security team, whilst other elements of the scope are managed under a CSMS by an OT security team. In fact, this situation may well be preferable as OES will be able to select security management systems that are most closely tailored to the systems under management.

1.37. OES are free to choose whether their NIS scope is managed collectively under a single security management system or is managed across several security management systems. The decision will be informed by the size and nature of the NIS scope and the presence of pre-existing security management systems. However, in all cases, Ofgem expects that OES can evidence that all individual network and information systems that are in scope are subject to an appropriate security management system, and that the management systems are aligned to the CAF security outcomes.

1.38. OES should choose the IT and OT security management systems that they consider most appropriate and proportionate to their environments. The CAF collection provides guidance as to some of the options available. Annex E contains a set of a framework mappings that detail how several of the most popular security management systems align to the CAF.

## **Evidential Requirements**

1.39. The CAF has been designed to assist OES achieve and **demonstrate** an appropriate level of cyber resilience. It achieves this by detailing a framework against which OES can be assessed – either through self-assessments or external assessments.

1.40. In accordance with DSIT's direction<sup>32</sup> Ofgem, as part of the joint Competent Authority, is responsible for '*assessing the compliance of operators to the requirements of the NIS Regulations*'. Ofgem satisfies this responsibility through implementation of its NIS Inspection Framework for DGE<sup>33</sup> and its wider compliance and enforcement activities. Ofgem's NIS Inspection Framework requires OES to present evidence that supports the achievement claims made in their CAF self-assessments.

---

<sup>32</sup> DCMS, Security of Network and Information Systems, Guidance for Competent Authorities, dated Apr 2018.

<sup>33</sup> Ofgem, NIS Inspection Framework for Downstream Gas and Electricity, dated Nov 2020

---

1.41. The DGE Sector CAF Overlay (Annex B) includes examples of evidence that Ofgem would typically expect an OES to provide to demonstrate that they are achieving contributing outcomes<sup>34</sup>, and the relevant profiles. It is our intent that this additional guidance on Ofgem’s expectations of evidential requirements will reduce uncertainty for OES during NIS inspections.

1.42. The examples of evidence detailed in the DGE CAF Overlay represent Ofgem’s understanding of how a typical OES could effectively and efficiently demonstrate good practice and achievement of contributing outcomes. Ofgem does not expect OES to generate the evidence listed in the overlay purely for the purposes of demonstrating regulatory compliance. Ofgem anticipates that the security processes implemented by OES as part of their security management systems would typically include the maintenance of those evidence types - or something equivalent. Ofgem invites discussion in instances where OES do not believe this to be the case.

## **Annexes**

- Annex A - Document Map
- Annex B - DGE Sector CAF Overlay
- Annex C - DGE Supplementary Objective, Objective E – Physical Security
- Annex D – Representative Scopes
- Annex E - Framework Mapping

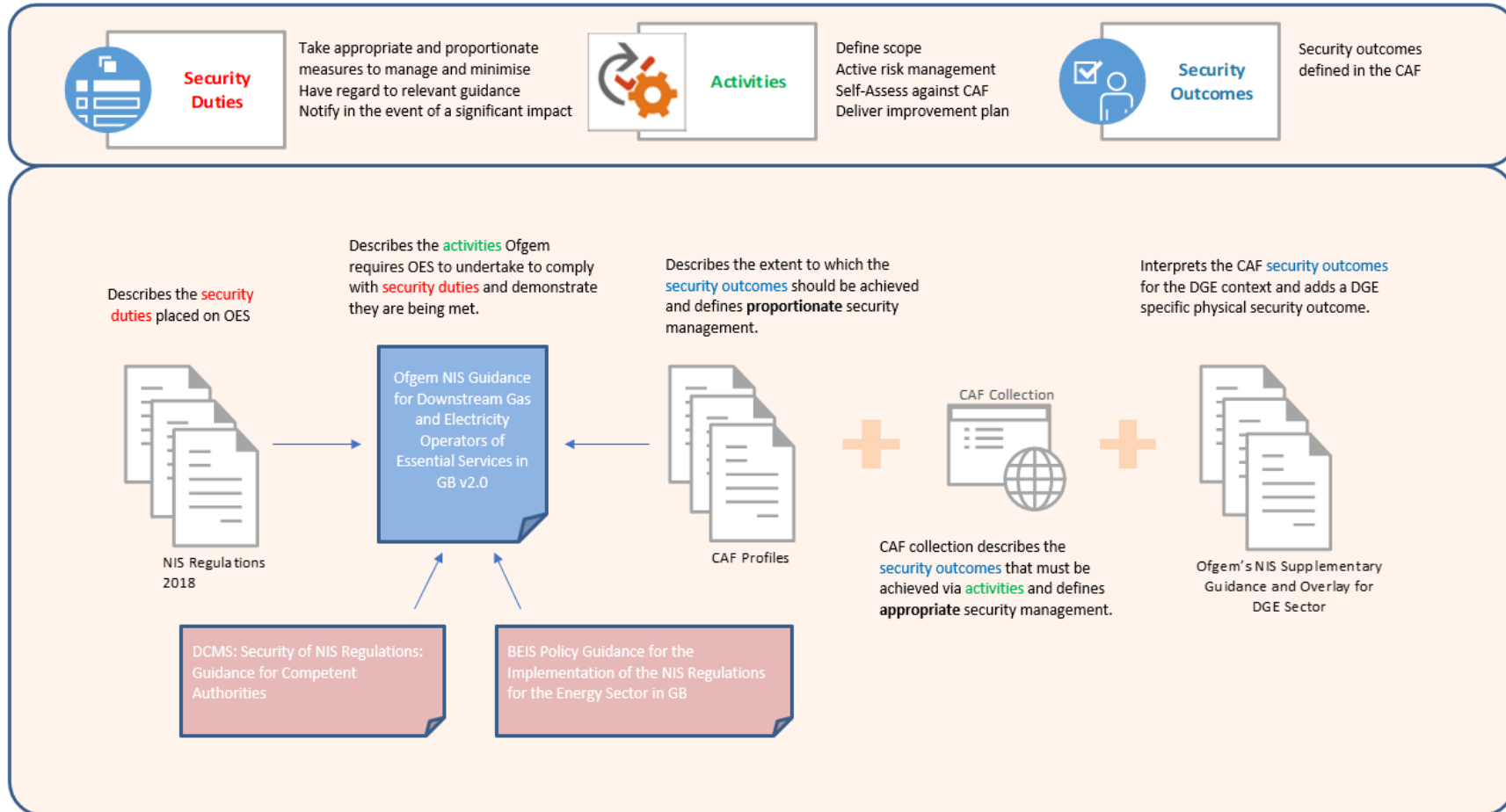
---

<sup>34</sup> Subject to para 1.18.

# Annex A

## Document Map

## Annex A - Document Map





# Annex B

## CAF Overlay

## **Annex B - CAF Overlay**

Annex B details Ofgem's interpretations of the CAF Indicators of Good Practice (IGPs). These interpretations are presented as a DGE Sector CAF Overlay. The interpretations describe the type and nature of security measures that Ofgem would typically expect to see implemented by an OES. These interpretations complement NCSC's CAF Guidance.

NCSC have produced the IGPs to describe the typical characteristics of an organisation that is achieving a contributing outcome. Use of the word 'typical' acknowledges that there are circumstances in which security outcomes may be better achieved via alternative means. Ofgem's CAF overlay has been produced on the same basis, meaning that the inclusion of an Ofgem interpretation of an IGP does not imply that it is mandatory. The interpretations are provided on a non-binding basis with the intention of guiding OES toward achieving and demonstrating attainment of the security outcomes.


The term 'network and information systems' is used repeatedly throughout the CAF tables and the overlays. In every instance, the term is being used to describe network and information systems that are in the OES' NIS scope.

# Objective A – Managing Security Risk

## Annex B.1 - Objective A - Managing Security Risk

*Appropriate organisational structures, policies, and processes in place to understand, assess and systematically manage security risks to the network and information systems supporting essential functions.*

### A1 Governance

A1 Governance		
<p><i>The organisation has appropriate management policies and processes in place to govern its approach to the security of network and information systems.</i></p>		
Related CAF Objective(s)	Ref	Contributing Outcome
A1 – Governance	A1.a	Board Direction
	A1.b	Roles and Responsibilities
	A1.c	Decision Making

#### A1.a Board Direction

A1.a – Board Direction	
<p><i>You have effective organisational security management led at board level and articulated clearly in corresponding policies.</i></p>	
	
Not achieved	Achieved
At least one of the following statements is true	All the following statements are true

<p>The security of network and information systems related to the operation of essential functions is not discussed or reported on regularly at board-level.</p> <p>Board-level discussions on the security of networks and information systems are based on partial or out-of-date information, without the benefit of expert guidance.</p> <p>The security of networks and information systems supporting your essential functions are not driven effectively by the direction set at board level.</p> <p>Senior management or other pockets of the organisation consider themselves exempt from some policies or expect special accommodations to be made.</p>	<ol style="list-style-type: none"> <li>1. Your organisation's <i>approach and policy</i> relating to the security of networks and information systems supporting the operation of essential functions are <i>owned and managed</i> at board level. These are communicated, in a meaningful way, to risk management decision-makers across the organisation.</li> <li>2. <i>Regular</i> board <i>discussions on the security</i> of network and information systems supporting the operation of your essential function take place, based on timely and accurate information and <i>informed by expert guidance</i>.</li> <li>3. There is a board-level individual who has overall accountability for the security of networks and information systems and drives regular discussion at board-level.</li> <li>4. Direction set at board level is translated into <i>effective organisational practices</i> that <i>direct and control</i> the security of the networks and information systems supporting your essential function.</li> </ol>
---	--

**Ofgem DGE CAF Interpretation**



<p>(Achieved)</p> <p>IGP 1 &amp; 4</p> <p>Management System</p>	<p>Ofgem interprets these IGPs as a requirement to maintain a comprehensive <b>security management system</b> relating to the security of networks and information systems that are within the scope of NIS-R. This requirement is further defined as follows:</p> <ol style="list-style-type: none"> <li>a) [<i>approach and policy</i>] A management system exists which clearly defines your approach to managing the security of networks and information systems that support your essential function.</li> <li>b) [<i>approach and policy</i>] [<i>effective organisational practices</i>] The management system consists of appropriate policies, standards, processes, procedures and/or practices which translate and embed the board's direction into business-as-usual activities. You are confident that these organisational practices deliver the intended security benefits and have a means of monitoring and demonstrating their effectiveness.</li> </ol>
---	---

	<ul style="list-style-type: none"> <li>c) <i>[owned and managed]</i> The management system clearly defines the governance roles, responsibilities and the chain of accountability.</li> <li>d) <i>[owned and managed]</i> The management system is reviewed in accordance with company policy and updated, as necessary, to ensure it is in line with the latest threats and the approved risk appetite.</li> <li>e) <i>[owned and managed]</i> <i>[direct and control]</i> The security management system is integrated into the company’s wider Corporate Management System (CMS), compliance structures and performance reporting processes.</li> </ul>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <ul style="list-style-type: none"> <li>a) A suite of policy documentation that combine to form a security management system. Ofgem have noted that many OES are using elements of internationally recognised standards and frameworks such as ISO 9001, ISO 27001 and ISO 55000 to contribute to their cyber security management system. In these instances, OES should be able to explain how these elements integrate with other security related organisational processes to form a complete security management system.</li> <li>b) Evidence (in the form of meeting minutes or reports) that the implementation of the security management system is monitored by your company’s compliance structures (e.g. company compliance committee or equivalent).</li> <li>c) Evidence (e.g. meeting minutes, directives) that the board is actively engaged in security management (e.g. provision of direction and guidance after the review of performance indicators).</li> </ul>

<p>(Achieved)</p> <p>IGP 2</p> <p>Reporting</p>	<p>IGP 2 – Ofgem interprets this IGP as follows:</p> <p>a) [<i>regular</i>] Senior management supply the board with scheduled (planned and periodic) feedback on the security of networks and information systems supporting the delivery of your essential function.</p> <p>b) [<i>informed by expert guidance</i>] This feedback should be prepared by suitably qualified and experienced personnel from within the organisation or by third parties.</p> <p>c) [<i>discussions on security</i>] Discussions and reports should include, but not be limited to:</p> <ul style="list-style-type: none"> <li>• cyber security risk status and trajectory</li> <li>• cyber security risks associated with the organisation’s supply chain</li> <li>• cyber security risks associated with the organisation’s interactions with upstream and downstream energy partners (e.g. transmission, distribution, retailers)</li> <li>• cyber security performance (supported by key performance indicators)</li> <li>• incidents experienced within the organisation</li> <li>• incidents experienced in the industry or similar industries</li> <li>• progress against NIS improvement plans</li> <li>• any changes to relevant cyber security threats.</li> </ul>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) Relevant status reports and meeting minutes.</p>

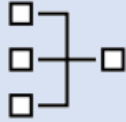
## References and Further Guidance



- [A.1 Governance - NCSC.GOV.UK](#)
- NIST 800-53 R4 – Appendix D: CA-1 Security Assessment and Authorisation Policies and Procedures, PL-1 Security Planning Policy, and Procedures



A1.b Roles and Responsibilities

<b>A1.b – Roles and Responsibilities</b>	
<p>Your organisation has established roles and responsibilities for the security of networks and information systems at all levels, with clear and well-understood channels for communicating and escalating risks.</p> 	
<b>Not achieved</b>	<b>Achieved</b>
<b>At least one of the following statements is true</b>	<b>All the following statements are true</b>
<p>Key roles are missing, left vacant, or fulfilled on an ad-hoc or informal basis.</p> <p>Staff are assigned security responsibilities but without adequate authority or resources to fulfil them.</p> <p>Staff are unsure what their responsibilities are for the security of the essential function.</p>	<ol style="list-style-type: none"> <li>1. <u>Necessary roles and responsibilities</u> for the security of networks and information systems supporting your essential function have been <u>identified</u>. These are reviewed periodically to ensure they remain <u>fit for purpose</u>.</li> <li>2. <u>Appropriately capable</u> and knowledgeable staff fill those roles and are given the <u>time, authority, and resources</u> to carry out their duties.</li> <li>3. There is <u>clarity</u> on who in your organisation has overall accountability for the security of the networks and information systems supporting your essential function.</li> </ol>
<b>Ofgem DGE CAF Interpretation</b>	
<p>(Achieved)</p> <p>IGP 1</p> <p>Roles and Responsibilities</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) [<i>necessary roles and responsibilities</i>] [<i>identified</i>] [<i>fit for purpose</i>]                      Being 'fit for purpose' means that you are confident that the roles and responsibilities that you have identified are sufficient to deliver the security management plan. This means that you must be able</p>

	<p>to associate all the activities and tasks listed in your security management plan with specific roles in your organisation.</p> <p>b) [<i>identified</i>] Key roles and assigned personnel are published internally and kept-up to-date. Individuals who are employed in roles with security responsibilities are fully aware of those responsibilities - this may be achieved by documenting these responsibilities in job specifications.</p> <p>c) [<i>necessary roles</i>] Roles can include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• Managers and senior leaders who are risk owners and who are responsible and accountable for elements of the security management system.</li> <li>• Operational Technology (OT) personnel who have responsibilities for securely maintaining and configuring OT devices</li> <li>• Operations personnel who have responsibilities for securely operating OT devices and networks</li> <li>• Information Technology (IT) personnel who have responsibilities for securing the enterprise IT networks that are connected to the OT environment and for maintaining and configuring gateways and boundary devices for OT networks.</li> <li>• Security personnel who have responsibilities for physical security at the site</li> <li>• Additional resources who may be in the legal, human resources and customer support and have responsibilities for implementing administrative controls.</li> </ul>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) A master list of security roles and responsibilities that is maintained as part of the security management system (this is often achieved in a RACI table format).</p> <p>b) The job specifications for each of the roles defined in the master list of security roles and responsibilities should clearly define the associated security responsibilities.</p>

<p>(Achieved)</p> <p>IGP 2</p> <p>Suitably Qualified and Experienced Personnel</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) [<i>appropriately capable</i>] You have baselined the minimum levels of qualification and experience required to effectively discharge the security responsibilities associated with each role. You are confident that the incumbents in each of your security roles exceeds this baseline, or there is a training plan in place to close the gap.</li> <li>b) [<i>time, authority and resources</i>] Personnel should be provided with sufficient information, financial, physical, and human resources to discharge their security responsibilities.</li> </ul> <p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <ul style="list-style-type: none"> <li>a) The baseline level of qualification and experience for each security role should be documented (possibly in the job specification).</li> <li>b) Evidence of the employment, or procurement, of a sufficient number of individuals to fill roles that have security responsibilities.</li> </ul>
<p>(Achieved)</p> <p>IGP 3</p> <p>Accountability</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) [<i>clarity</i>] A tool such as a responsible, accountable, consulted, and informed (RACI) matrix should be used to document and communicate responsibilities and accountabilities.</li> </ul>

	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) A clear chain of accountability which cascades down from board level and is documented in an appropriate format (such as a RACI matrix).</p>
--	---

## References and Further Guidance

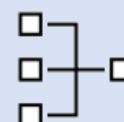


- [A.1 Governance - NCSC.GOV.UK](#)
- NIST SP800-82 R2 – Section 4.2
- IEC 62443/ISA99 2-1 – Sections A.3.2.2.2, A.3.2.3.4.2
- ISO 27019 – Sections 6.1.1, 6.1.2

A1.c Decision Making

**A1.c – Decision Making**

*You have senior-level accountability for the security of networks and information systems, and delegate decision-making authority appropriately and effectively. Risks to network and information systems related to the delivery of essential functions are considered in the context of other organisational risks.*



Not achieved	Achieved
<p><b>At least one of the following statements is true</b></p>	<p><b>All the following statements are true</b></p>
<p>What should be relatively straightforward risk decisions are constantly referred up the chain, or not made.</p> <p>Risks are resolved informally (or ignored) at a local level when the use of a more formal risk reporting mechanism would be more appropriate.</p> <p>Decision-makers are unsure of what senior management's risk appetite is, or only understand it in vague terms such as "averse" or "cautious".</p> <p>Organisational structure causes risk decisions to be made in isolation. (e.g. engineering and IT don't talk to each other about risk).</p> <p>Risk priorities are too vague to make meaningful distinctions between them. (e.g. almost all risks are rated 'medium' or 'amber').</p>	<ol style="list-style-type: none"> <li>1. Senior management have <u>visibility</u> of key risk decisions made throughout the organisation.</li> <li>2. Risk management decision-makers understand their responsibilities for making <u>effective and timely decisions</u> in the <u>context of the risk appetite</u> regarding the essential function, as set by senior management.</li> <li>3. Risk management decision-making is <u>delegated and escalated</u> where necessary, across the organisation, to people who have the skills, knowledge, tools, and authority they need.</li> <li>4. Risk management decisions are <u>periodically reviewed</u> to ensure their continued relevance and validity</li> </ol>

**Ofgem DGE CAF Interpretation**



<p>(Achieved)</p> <p>IGP 1</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) [<i>visibility</i>] Risk registers are maintained and are reviewed and approved on a scheduled basis (planned and periodic) by individuals</p>
--------------------------------	---

<p>Visibility</p>	<p>with sufficient authority to make the necessary risk management decisions.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <ul style="list-style-type: none"> <li>a) Risk registers that have been formally approved and accepted by those managers who are responsible and accountable for the risks.</li> </ul>
<p>(Achieved) IGP 2  Risk Appetite</p>	<p>Ofgem interprets this IGP as:</p> <ul style="list-style-type: none"> <li>a) [<i>context of risk appetite</i>] Your organisation’s risk appetite should be agreed by the board. The risk appetite should take account of the CAF profiles that are written by NCSC and issued by Ofgem.</li> </ul> <p>Note: The CAF profiles represent a cyber security attainment level that correspond to Ofgem’s initial view of appropriate and proportionate security for in-scope network and information systems. OES may deviate from the profile if they can demonstrate that a lower attainment level is appropriate and proportionate in the context of their essential function. Equally, OES may also be required to exceed the requirements of the profile if the OES’ own risk assessments indicate a requirement to do so.</p> <ul style="list-style-type: none"> <li>b) [<i>context of risk appetite</i>] Your risk appetite should be reviewed periodically, in accordance with company policy, or due to any significant change in threat level. Any changes should be promptly communicated to relevant personnel.</li> <li>c) [<i>effective and timely decisions</i>] The organisation’s policy and processes relating to the management of risk should be published as part of the organisation’s security management system. These policies and processes should be easily accessible and support effective decision making.</li> </ul>

	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) A documented risk appetite statement, and a process that explains how you manage situations where risk treatment decisions informed by your own risk appetites deviate from the relevant CAF profile.</p> <p>Note: This situation is described in more detail in the Ofgem’s NIS Supplementary Guidance document under the following sections:</p> <ul style="list-style-type: none"> <li>• How should OES assess the appropriateness of security measures?</li> <li>• How should OES assess the proportionality of security measures?</li> </ul>
<p>(Achieved)</p> <p>IGP 3</p> <p>Delegated and Escalated</p>	<p>Ofgem interprets this IGP as:</p> <p>a) [<i>delegated and escalated</i>] Suitable governance structures and scheduled activities (such as risk reviews) are in place to support the delegation and escalation of risk management decision making to the appropriate level.</p> <p>b) [<i>delegated and escalated</i>] Risk management decision-makers have the necessary authority and resources to make decisions and drive risk management activities in line with the guidance from the board.</p> <p>c) [<i>delegated and escalated</i>] Decision makers are given appropriate support by senior management.</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p>

	<p>a) A schedule of risk management activities (e.g. risk identification workshops, risk reviews, risk sentencing).</p> <p>b) Minutes of previously held risk management activities.</p> <p>c) Appropriate financial delegations/budgets have been delegated to allow timely and effective management of risk.</p>
<p>(Achieved)</p> <p>IGP 4</p> <p>Periodic review</p>	<p>Ofgem interprets this IGP as:</p> <p>a) [<i>periodically reviewed</i>] Suitable structures and scheduled activities (such as risk reviews) are in place to support the delegation and escalation of risk management decision making to the appropriate level.</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) A schedule of risk management activities (e.g. risk identification workshops, risk reviews, risk sentencing).</p> <p>b) Minutes from previously held risk management meetings/activities.</p>


## References and Further Guidance



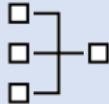
- [A.1 Governance - NCSC.GOV.UK](#)
- NIST 800-53 R4 – Appendix D: RA-1 Risk Assessment Policy and Procedures, RA-2 Security Categorization, RA-3 Risk Assessment



## A2 Risk management

A2 Risk Management		
<p>The organisation takes appropriate steps to identify, assess and understand security risks to the network and information systems supporting the operation of essential functions. This includes an overall organisational approach to risk management.</p>		
Related CAF Objective(s)	Ref	Contributing Outcome
A2 – Risk Management	A2.a	Risk Management Process
	A2.b	Assurance

### A2.a Risk Management Process

A2.a – Risk Management Process		
<p>Your organisation has effective internal processes for managing risks to the security of network and information systems related to the operation of essential functions and communicating associated activities.</p>		
Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
<p>Risk assessments are not based on a clearly defined set of threat assumptions.</p> <p>Risk assessment outputs are too complex or unwieldy to be consumed by decision-makers and are not effectively communicated in a clear and timely manner.</p>	<p>1. Your organisational process ensures that security risks to networks and information systems <u>relevant to essential functions are identified, analysed, prioritised, and managed.</u></p> <p>2. Your risk assessments are informed by an <u>understanding of the vulnerabilities</u> in the networks and information systems supporting your essential function.</p>	<p>7. Your organisational process ensures that security risks to networks and information systems <u>relevant to essential functions</u> are <u>identified, analysed, prioritised, and managed.</u></p> <p>8. Your approach to risk is focused on the <u>possibility of adverse impact</u> to your essential function, leading to a <u>detailed understanding</u> of how such impact might arise as a</p>

<p>Risk assessments for critical systems are a "one-off" activity (or not done at all).</p> <p>The security elements of projects or programmes are solely dependent on the completion of a risk management assessment without any regard to the outcomes.</p> <p>There is no systematic process in place to ensure that identified security risks are managed effectively.</p> <p>Systems are assessed in isolation, without consideration of dependencies and interactions with other systems. (e.g. interactions between IT and OT environments).</p> <p>Security requirements and mitigations are arbitrary or are applied from a control catalogue without consideration of how they contribute to the security of the essential function.</p> <p>Risks remain unresolved on a register for prolonged periods of time awaiting senior decision-making or resource allocation to resolve.</p>	<p>3. The output from your risk management process is a <u>clear set of security requirements</u> that will address the risks in line with your organisational approach to security.</p> <p>4. Significant conclusions reached during your risk management process are <u>communicated</u> to key security decision-makers and <u>accountable individuals</u>.</p> <p>5. You conduct risk assessments when significant events potentially affect the essential function, such as replacing a system or a change in the cyber security threat.</p> <p>6. You perform threat analysis and understand how generic threats apply to your organisation.</p>	<p>consequence of <u>possible attacker actions</u> and the <u>security properties</u> of your networks and information systems.</p> <p>9. Your risk assessments are based on a <u>clearly understood set of threat assumptions</u>, informed by an <u>up-to-date understanding</u> of security threats to your essential function and your sector.</p> <p>10. Your risk assessments are informed by an <u>understanding of the vulnerabilities</u> in the networks and information systems supporting your essential function.</p> <p>11. The output from your risk management process is a <u>clear set of security requirements</u> that will address the risks in line with your organisational approach to security.</p> <p>12. Significant conclusions reached during your risk management process are <u>communicated</u> to key security decision-makers and <u>accountable individuals</u>.</p> <p>13. Your risk assessments are dynamic and updated in the light of relevant changes which may include technical changes to networks and information systems, change of use and new threat information.</p> <p>14. The <u>effectiveness</u> of your risk management process is <u>reviewed</u> periodically, and improvements made as required.</p> <p>15. You perform <u>detailed threat</u> analysis and understand how this applies to your organisation in the context of the threat to your sector and the wider CNI.</p>
--	--	---

## Ofgem DGE CAF Interpretation



<p>(Partially Achieved)</p> <p>IGP 1</p> <p>(Achieved)</p> <p>IGP 7</p> <p>Risk Assessment Coverage</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) [<i>relevant to essential function</i>] You have fully captured and documented your NIS scope in accordance with the direction provided in the current version of Ofgem’s NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in Great Britain and the Supplementary Guidance. Your NIS scope takes account of the requirement for you to deliver the essential service in accordance with relevant licences, regulations and network codes. You have referred to these documents to help you define your NIS scope.</p> <p>b) [<i>identified, analysed, prioritised and managed</i>] You have had regard to the NCSC’s guidance on risk management and have selected a risk identification and assessment methodology that is appropriate to the systems in scope.</p> <p>c) [<i>identified, analysed, prioritised and managed</i>] You have recognised that, for those network architectures that include a conduit between the OT and IT networks, the systems on your OT network have a dependency on the security services (boundary protection, access control, SIEM etc) provided by your IT networks. You have included these IT security services within your NIS scope.</p> <p>d) [<i>identified, analysed, prioritised and managed</i>] You have taken account of common risks in your sub-sector (such as those associated with the use of particular equipment types and communications methods) and of context specific risks (such as those associated with your particular network topologies and equipment configurations). You have used multi-disciplinary teams to ensure a comprehensive capture of context specific organisational risks in accordance with your selected risk assessment methodology.</p>
---	---

	<p>e) [<i>identified, analysed, prioritised and managed</i>] Your risk management process is clearly explained in your security management system and the outputs of your risk management activities are documented.</p> <p>f) [<i>identified, analysed, prioritised and managed</i>] You have considered the risk of single cyber-attacks, multiple and coordinated near simultaneous attacks at the risk identification stage.</p> <p>g) [<i>identified, analysed, prioritised and managed</i>] You periodically review your risk assessments to consider changes in the cyber security landscape or scope.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) A documented risk management process.</p> <p>b) A comprehensive risk register that complies with the guidance provided in the current version of Ofgem’s NIS Guidance for Downstream Gas and Electricity Operators of Essential Services.</p>
<p>(Achieved)</p> <p>IGP 8</p> <p>Approach to Risk Assessment</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) [<i>possibility of adverse impact</i>] Your risk assessments take account of the potential for adverse impacts to the delivery of your essential service and for adverse impacts that may impact other Operators of Essential Services OES (typically referred to as cascading impacts) and have prioritised them accordingly.</p> <p>b) [<i>possibility of adverse impact</i>] You have identified risks originating on the systems of other OES on which you have dependencies. You have taken measures to control these risks where it is practical and feasible to do so.</p>

	<p>c) [<i>possibility of adverse impact</i>] Organisations in the electrical transmission, distribution and generation sectors understand which of its NIS assets contribute to, or could impact, the National Restoration Plan and has prioritised them accordingly.</p> <p>d) [<i>detailed understanding</i>] You have employed a system-driven risk assessment methodology to identify the possibility of adverse impacts to the essential function. The organisation has fully captured and documented this risk assessment and is able to explain it to Ofgem.</p> <p>e) [<i>detailed understanding</i>] The organisation’s cyber risk assessment panel is multi-disciplinary, such that the risk assessment is as complete as is feasible.</p> <p>f) [<i>possible attacker actions</i>] You understand the Tactics, Techniques and Procedures (TTPs) that attackers may employ against your systems. You conduct attack modelling (using a resource such as the MITRE ATT&amp;CK framework) to identify the specific techniques that an adversary could employ.</p> <p>g) [<i>security properties</i>] You have fully captured the existing security properties (the security function/capability provided by the controls) of your systems and understands how these properties contribute to controlling risk. You have considered the effectiveness of these security controls against the attack models you have developed and have identified where enhanced security controls will be required to match these threats.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) A comprehensive risk register that complies with the guidance provided in the current version of Ofgem’s NIS Guidance for Downstream Gas and Electricity Operators of Essential Services.</p>
(Achieved)	Ofgem interprets this IGP as follows:

<p>IGP 9</p> <p>Threat Analysis</p>	<p>a) [<i>clearly understood set of threat assumptions</i>] You have conducted and documented a threat assessment. Your assumptions include the possibility that your organisation is subject to attacks from threat actors ranging in capability from basic to advanced<sup>35</sup> (e.g. from commodity attacks to espionage and targeted attacks from malicious actors such as hostile states and criminals<sup>36</sup>).</p> <p>b) [<i>up to date understanding</i>] You review your threat assumptions, based on changes to the threat landscape. For example, in response to geo-political events, evidence of new cyber-attack campaigns that are relevant to your sector, or the disclosure of significant new vulnerabilities.</p> <p>c) [<i>up to date understanding</i>] You participate in cross-sector information sharing forums and draw on NCSC’s threat intelligence (e.g. through CiSP). You make use of all free services provided by NCSC (such as Early Warning<sup>37</sup>) and you are in receipt of an appropriate Threat Intelligence feed (e.g. MISP or a commercial equivalent). You have a means of prioritising new threat intelligence and updating risk assessments accordingly.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) a comprehensive risk register that has taken account of the risks posed by the full range of threat actors.</p> <p>b) Evidence of consideration (e.g. updates to risk assessments) of changes to the threat landscape.</p> <p>c) Evidence that the OES participates in cross sector information sharing initiatives and is in receipt of regular threat intelligence.</p>

<sup>35</sup> The OES’ threat and risk assessments should not be limited to the attacker capability levels referenced in the relevant CAF profile (the BP references a limited capability attacker, the EP references a moderate capability attacker). Para 1.13 of the Supplementary Guidance explains how, after considering the threat from the full range of attacker capabilities, OES can use the CAF Profiles to limit the implementation of their control set to that which is considered appropriate and proportionate.

<sup>36</sup> [CNI Hub - NCSC.GOV.UK](https://www.ncsc.gov.uk/cni-hub)

<sup>37</sup> [Early Warning - NCSC.GOV.UK](https://www.ncsc.gov.uk/early-warning)

<p>(Partially Achieved)</p> <p>IGP 2</p> <p>(Achieved)</p> <p>IGP 10</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) [<i>understanding of the vulnerabilities</i>] The organisation has a process that identifies and manages vulnerabilities at a component level (this is often achieved as part of an OES' asset management and/or configuration management processes).</p>
<p>Vulnerability Management</p>	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) demonstration that you are meeting the vulnerability management security outcome described at B4.d.</p>
<p>(Partially Achieved)</p> <p>IGP 3</p> <p>(Achieved)</p> <p>IGP 11 –</p> <p>Cyber Improvement Planning</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) [<i>clear set of security requirements</i>] Deficiencies in your security controls that are identified through your risk assessment and vulnerability management processes are assessed against your risk appetite. Those risks that required treatment are captured in the organisation's cyber improvement plan. The cyber improvement plan is produced according to Part D of Ofgem's NIS guidance for Downstream Gas and Electricity Operators of Essential Services in Great Britain v 2.0.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p>

	<p>a) A comprehensive cyber improvement plan that details the actions that will be undertaken to reduce cyber risks to within risk appetite.</p> <p>b) A clear linkage (in the form of a reference no. or similar) between the risks identified through vulnerability and risk assessments and the activities on the cyber improvement plan. These links are intended to make it simple for you, for external auditors and for Ofgem to confirm that outstanding risks are being treated.</p>
<p>(Partially Achieved) IGP 4</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) [<i>communicated</i>][<i>accountable individuals</i>] Residual risks (those risks that remain after risk treatment) are captured on the risk register and approved by accountable individuals. The means of approval is formal and documented.</p>
<p>(Achieved) IGP 12 - Residual Risk</p>	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) Evidence of acknowledgement and acceptance of residual risk by appropriate risk managers.</p>
<p>(Achieved) IGP 14 Process Monitoring</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) [<i>effectiveness</i>][<i>reviewed</i>] The organisation’s cyber risk management process is subject to an appropriate level of oversight. This may take the form of a formal Quality Assurance process, a regulatory compliance committee or another form of internal or external audit.</p> <p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p>



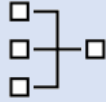
	<p>a) Documentary evidence of a relevant from of internal or external audit.</p>
<p>(Achieved)  IGP 15</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) [detailed threat analysis] You use the threat information detailed in the scenarios in the NCSC’s Enhanced CAF Profile for DGE document to inform your threat assessments.</p> <p>b) [<i>detailed threat analysis</i>] You employ organisation specific threat analysis (using a framework such as MITRE ATT&amp;CK) to develop threat models.</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) Evidence that organisation specific threat models have been used to inform the risk assessment process.</p>

## References and Further Guidance




- [A.2 Risk management - NCSC.GOV.UK](#)
- NIST 800-82 R2 – Appendix D: RA-1 Risk Assessment Policy and Procedures, RA-2 Security Categorization, RA-3 Risk Assessment, RA-5 Vulnerability Scanning
- IEC 62443-2-1 – 4.2.3 Risk identification, classification, and assessment, 4.3.4.2 Risk management and implementation
- IEC 62443-3-3 – SR 5.2 Zone boundary protection
- NIST 800-53 R4 – Appendix F: RA-1 Risk Assessment Policy and Procedures, RA-2 Security Categorization, RA-3 Risk Assessment, RA-5 Vulnerability Scanning
- ISO/IEC 27001 – 4.2.x Risk Assessment Approach
- NIST 800-53 R4 – Appendix D: RA-1 Risk Assessment Policy and Procedures, RA-2 Security Categorization, RA-3 Risk Assessment

A2.b Assurance

<b>A2.b – Assurance</b>	
<p><i>You have gained confidence in the effectiveness of the security of your technology, people, and processes relevant to essential functions.</i></p> 	
<b>Not achieved</b>	<b>Achieved</b>
<b>At least one of the following statements is true</b>	<b>All the following statements are true</b>
<p>A particular product or service is seen as a "silver bullet" and vendor claims are taken at face value.</p> <p>Assurance methods are applied without appreciation of their strengths and limitations, such as the risks of penetration testing in operational environments.</p> <p>Assurance is assumed because there have been no known problems to date.</p>	<ol style="list-style-type: none"> <li>1. You <u>validate</u> that the security measures in place to protect the networks and information systems are effective and remain effective for the lifetime over which they are needed.</li> <li>2. You understand the assurance methods available to you and choose appropriate methods to gain confidence in the security of essential functions.</li> <li>3. Your confidence in the security as it relates to your technology, people, and processes can be <u>justified to, and verified by, a third party</u>.</li> <li>4. <u>Security deficiencies uncovered</u> by assurance activities are assessed, prioritised and remedied when necessary, in a timely and effective way.</li> <li>5. The <u>methods used for assurance are reviewed</u> to ensure they are working as intended and remain the most appropriate method to use.</li> </ol>
<b>Ofgem DGE CAF Interpretation</b>	
<p>(Achieved)</p> <p>IGP 1 -</p>	<p>Ofgem interprets this IGP as follows:</p> <ol style="list-style-type: none"> <li>a) [<i>validate</i>] Validation of the technology, people and process that constitutes an OES' security measures requires:</li> </ol>


<p>Validation</p>	<p>a. <b>Technology</b> – You employ a mix of the following:</p> <ul style="list-style-type: none"> <li>○ maintenance of accurate configuration records and periodic documentation and system checks to ensure that devices are correctly configured in accordance with standard builds and physical security.</li> <li>○ vulnerability assessments (see contributing outcome A2.a)</li> <li>○ penetration testing.</li> </ul> <p>Your use of these validation techniques is cognisant of the risks associated with each and the relative importance of the security function provided by specific network element being validated. Meaning that devices and services with a high degree of security functionality – such as boundary protection devices – will be subject to the full range of techniques.</p> <p>b. <b>People</b> – The organisation:</p> <ul style="list-style-type: none"> <li>○ requires its people to undertake periodic cyber security training.</li> <li>○ may choose to employ human behavioural testing (e.g. simulated phishing emails) to reinforce training.</li> </ul> <p>c. <b>Process</b> – The organisation uses a mix of internal and external audits to validate the correct implementation of security processes.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <ul style="list-style-type: none"> <li>a) Asset registers in accordance with Contributing Outcome A3.</li> <li>b) Documented configuration management processes and records.</li> <li>c) Documented vulnerability management processes and records.</li> <li>d) Results of automated vulnerability scans (where appropriate).</li> <li>e) Results of penetration tests (where appropriate).</li> <li>f) Employee cyber security training plan and records.</li> <li>g) Results of any security relevant internal or external audits.</li> </ul>

<p>(Achieved)</p> <p>IGP 3</p> <p>Attestation of Controls</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) [<i>justified to, and verified by, a third party</i>] the organisation may choose to employ an independent auditor to verify the effectiveness of its security measures. Doing so may provide the organisation with confidence that the security measures are effective and may be taken into consideration during Ofgem inspections.</li> <li>b) [<i>justified to, and verified by, a third party</i>] The organisation must be prepared to justify the effectiveness of its security measures during an inspection. The organisation must collate and archive its assurance and verification documentation in such a way that they can be used as evidence during an inspection.</li> </ul>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <ul style="list-style-type: none"> <li>a) Copies of reports that an OES has commissioned from third parties (audit results, technical testing results).</li> <li>b) A suitable document repository, that is accessible by key members of OES staff, such that relevant NIS evidence can be easily presented on request.</li> </ul>
<p>(Achieved)</p> <p>IGP 4</p> <p>Response to Assurance Activity Findings</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) [<i>security deficiencies uncovered</i>] the organisation can provide evidence that recommendations made via assurance activities and findings made during validation activities have been recorded. These recommendations and findings have either been actioned, are in the process of being actioned, or have been refuted.</li> </ul>

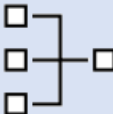
	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <ul style="list-style-type: none"> <li>a) Up to date configuration management records that demonstrate that recommendations and findings have been actioned.</li> <li>b) Up to date cyber improvement plans that demonstrate that those recommendations and findings with longer implementation timeframes have been programmed.</li> </ul>
<p>(Achieved)  IGP 5  Review of Practices</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) [<i>methods used for assurance are reviewed</i>] the organisation has evolved its assurance methods as its Security Management System has matured and become established. Initial assurance activity should be focused on ensuring that the processes employed are meeting their objectives. Later stage assurance activity should be focused on refining and optimising processes and checking that they are aligned to best practise.</li> </ul> <p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <ul style="list-style-type: none"> <li>a) Records (e.g. version records) demonstrating that the Security Management System is being periodically updated and improved.</li> </ul>
<p><b>References and Further Guidance</b></p> <div style="text-align: right;">  </div>	
Empty row for content	

- [A.2 Risk management - NCSC.GOV.UK](#)
- NIST SP800-82 R2 – Section 6.2.3
- ISO 27019: Sections 12.7, 14.2.8, 18.2

## A3 Asset Management

A3 Asset Management		
<p>Everything required to deliver, maintain, or support networks and information systems necessary for the operation of essential functions is determined and understood. This includes data, people, and systems, as well as any supporting infrastructure (such as power or cooling).</p>		
Related CAF Objective(s)	Ref	Contributing Outcome
A3 – Asset Management	A3.a	Asset Management

### A3.a Asset Management

A3.a – Asset Management	
<p>Everything required to deliver, maintain, or support networks and information systems necessary for the operation of essential functions is determined and understood. This includes data, people, and systems, as well as any supporting infrastructure (such as power or cooling).</p>	
	
Not achieved	Achieved
At least one of the following statements is true	All the following statements are true

<p>Inventories of assets relevant to the essential function are incomplete, non-existent, or inadequately detailed.</p> <p>Only certain domains or types of assets are documented and understood. Dependencies between assets are not understood (such as the dependencies between IT and OT).</p> <p>Information assets, which could include personally identifiable information or other sensitive information, are stored for long periods of time with no clear business need or retention policy.</p> <p>Knowledge critical to the management, operation, or recovery of essential functions is held by one or two key individuals with no succession plan.</p> <p>Asset inventories are neglected and out of date.</p>	<ol style="list-style-type: none"> <li>1. All assets <u>relevant to the secure operation</u> of essential functions are <u>identified and inventoried (at a suitable level of detail)</u>. The inventory is kept up to date.</li> <li>2. <u>Dependencies on supporting infrastructure</u> (e.g. power, cooling etc) are recognised and recorded.</li> <li>3. You have prioritised your assets according to their importance to the operation of the essential function.</li> <li>4. You have assigned responsibility for managing physical assets.</li> <li>5. Assets relevant to essential functions are <u>managed with cyber security in mind throughout their lifecycle</u>, from creation through to eventual decommissioning or disposal.</li> </ol>
--	--

## Ofgem DGE CAF Interpretation



<p>(Achieved)</p> <p>IGP 1</p> <p>Asset Register Coverage &amp; Management</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) [<i>relevant to the secure operation</i>] the asset inventory captures the following asset types:</p> <ul style="list-style-type: none"> <li>• the components of all systems and sub-systems named in your NIS scope.</li> <li>• the sources of data required to operate, maintain and restore these systems and sub-systems. These could include manuals, configuration management records, device images.</li> <li>• the people and contract services required operate, maintain and restore the systems. People should include those with niche (or possibly unique) knowledge of your systems who would be impossible to replace at short notice, e.g. developers of bespoke applications on which your essential services rely.</li> <li>• all ancillary systems that are necessary to support the secure and reliable operation of the network and information systems (e.g. UPS, backup generation, cooling).</li> </ul>
--	--



	<p>b) [<i>identified and inventoried</i>] the asset capture process is comprehensive, and you have a high degree of confidence that it is complete. You have used an appropriate range of tools and techniques to ensure completeness, these could include automated discovery tools and manual survey. The information is captured in a suitable format and is easily searchable, spreadsheets may prove to be adequate, however, larger organisations may wish to consider dedicated asset management solutions.</p> <p>c) [<i>suitable level of detail</i>] a suitable level of detail is that which allows the organisation to manage the assets through life. Information is expected to include, but is not limited to:</p> <ul style="list-style-type: none"><li>• the location of assets</li><li>• a unique identifier</li><li>• asset criticality relating to the assets' importance to the delivery of the essential function</li><li>• asset criticality relating to the assets' importance to the delivery of network security. You should be able to filter for devices that provide security enhancing functionality, and devices on the network boundary that are externally accessible. This will allow you to ensure that these devices are appropriately configured and patched.</li><li>• list of ancillary equipment required for maintenance and configuration</li><li>• list of firmware, operating systems and application software, including End of Life (EOL) dates</li><li>• details of known vulnerabilities/non-conformities against configuration management and patching policies. These vulnerabilities and non-conformities should be carried across to the risk register.</li></ul> <p>d) [<i>suitable level of detail</i>] for devices which are obsolete you have captured the following additional information (this information may be captured in the asset register, risk register, or vulnerabilities register – the choice of which will depend on your own processes):</p>
--	---

	<ul style="list-style-type: none"> <li>• list of the firmware, operating systems and application software that is obsolete</li> <li>• list of CVEs relevant to any software</li> <li>• risks of continued use of these devices</li> <li>• list of measures taken to reduce the likelihood and impact of compromise</li> <li>• details of the plans to upgrade obsolete devices.</li> </ul>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <ul style="list-style-type: none"> <li>a) comprehensive asset register.</li> <li>b) linkages between any vulnerabilities that are recorded/flagged in the asset register and the appropriate risk register and cyber improvement plan (if relevant).</li> </ul>
<p>(Achieved) IGP 2  Dependencies are Identified</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) [<i>dependencies on supporting infrastructure</i>] all dependencies are captured in the asset register and you can cross-reference these dependencies with risks you have identified under Principle E2 – Broader network and information systems resilience risks.</li> </ul> <p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <ul style="list-style-type: none"> <li>a) Risks relating to dependencies on supporting infrastructure have been recorded in the appropriate risk register.</li> </ul>

<p>(Achieved)</p> <p>IGP 5</p> <p>Life Cycle Management of Cyber Assets</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) [<i>managed with cyber security in mind throughout their life cycle</i>] You make full use of your asset registers and configuration management databases as part of your cyber security management system. You ensure that:</p> <ul style="list-style-type: none"> <li>• asset registers are up to date</li> <li>• asset registers are regularly reviewed and audited and obsolete devices are identified</li> <li>• Obsolete devices are appropriately managed</li> <li>• routine cross-reference new Common Vulnerabilities and Exposures (CVEs) and supplier security advisories with the devices and software employed on your networks. When relevant CVEs/advisories are identified you are able to quickly locate affected devices and schedule the necessary patches.</li> </ul> <p>b) [<i>managed with cyber security in mind throughout their life cycle</i>] You have policies which dictate:</p> <ul style="list-style-type: none"> <li>• the specification of security requirements for devices in the design and procurement processes (see B4.b)</li> <li>• the use of standardised secure device configurations, i.e. baseline/gold builds (see B4.b).</li> </ul>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) use of a method that allows for easy identification of devices that are obsolete (such as the use of date based conditional formatting in the asset).</p>


	<p>b) configuration management and patching records that demonstrate that the necessary patching is taking place.</p> <p>c) evidence that the risks identified through good asset management (e.g. the identification of obsolete devices and devices that remain unpatched) have been transferred to the appropriate risk registers.</p>
--	---

## References and Further Guidance

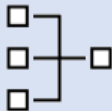


- [A.3 Asset management - NCSC.GOV.UK](#)
- NIST SP800-82 R2 – Section 6.2.3
- ISO 27019: Sections 12.7, 14.2.8, 18.2

## A4 Supply Chain

A4 Supply Chain		
<p><i>The organisation understands and manages security risks to networks and information systems supporting the operation of essential functions that arise because of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.</i></p>		
Related CAF Objective(s)	Ref	Contributing Outcome
A4 – Supply Chain	A4.a	Supply Chain

### A4.a Supply Chain

A4.a – Supply Chain		
<p><i>The organisation understands and manages security risks to networks and information systems supporting the operation of essential functions that arise because of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.</i></p>		
Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true

<p>You do not know what data belonging to you is held by suppliers, or how it is managed.</p> <p>Elements of the supply chain for essential functions are subcontracted and you have little or no visibility of the sub-contractors.</p> <p>You have no understanding of which contracts are relevant and / or relevant contracts do not specify appropriate security obligations.</p> <p>Suppliers have access to systems that provide your essential function that is unrestricted, not monitored or bypasses your own security controls.</p>	<p>1. You understand the <u>general risks</u> suppliers may pose to your essential functions.</p> <p>2. You know the <u>extent of your supply chain</u> for essential functions, including sub-contractors.</p> <p>3. You understand which contracts are relevant and you <u>include appropriate security obligations</u> in relevant contracts.</p> <p>4. You are aware of all third-party connections and have <u>assurance</u> that they meet your organisation's security requirements.</p> <p>5. Your approach to security incident management considers incidents that might arise in your supply chain.</p> <p>6. You <u>have confidence</u> that information shared with suppliers that is necessary for the operation of your essential function is <u>appropriately protected</u> from well-known attacks and known vulnerabilities.</p>	<p>7. You have a <u>deep understanding</u> of your supply chain, including sub-contractors and the <u>wider risks</u> it faces. You consider factors such as supplier's partnerships, competitors, nationality and other organisations with which they sub-contract. This informs your <u>risk assessment and procurement processes</u>.</p> <p>8. Your approach to supply chain risk management considers the risks to your essential functions arising from supply chain subversion by capable and well-resourced attackers.</p> <p>9. You have confidence that information shared with suppliers that is essential to the operation of your function is <u>appropriately protected from sophisticated attacks</u>.</p> <p>10. You understand which contracts are relevant and you include <u>appropriate security obligations</u> in relevant contracts. You have a <u>proactive approach to contract management</u> which may include a contract management plan for relevant contracts.</p> <p>11. Customer / supplier ownership of <u>responsibilities</u> are laid out in contracts.</p> <p>12. All network connections and <u>data sharing with third parties is managed effectively</u> and proportionately.</p> <p>13. When appropriate, your incident management process and that of your suppliers provide <u>mutual support</u> in the resolution of incidents.</p>
---	--	--

## Ofgem DGE CAF Interpretation



<p>(Partially Achieved)</p> <p>IGP 1</p> <p>Supplier Risk</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a. [<i>general risks</i>] You have conducted an assessment in which you have:</p> <ul style="list-style-type: none"> <li>• identified the suppliers whose products or services could have an impact on your essential service.</li> <li>• categorised your suppliers by type (e.g. OEM, Systems Integrator, Software Supplier, Cloud Service Provider) and considered the nature of the risks (e.g. introduction of malware, deliberate misconfiguration) associated with each type.</li> </ul> <p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) a register of suppliers, categorised by type and providing details of the nature of the risks associated with each.</p>
<p>(Partially Achieved)</p> <p>IGP 2</p> <p>Supply Chain Extent</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a. [<i>extent of your supply chain</i>] you have conducted an assessment in which you have:</p> <ul style="list-style-type: none"> <li>○ identified the suppliers whose products or services could have an impact on your essential service.</li> </ul>

	<p>Evidenced by:</p> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) register of suppliers, categorised by type and providing details of the nature of the risks associated with each.</p>
<p>(Partially Achieved)</p> <p>IGP 3</p> <p>Security Obligations</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) [<i>include appropriate security obligations</i>] you have created a standard set of security clauses for inclusion within contractual agreements. You select the appropriate security obligations for all new contracts and insert them as required.</p> <p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) a standard set of security clauses.</p> <p>b) evidence that these clauses have been included in recently issued contracts.</p> <p>c) an assessment of the contracts of all suppliers on your supplier register which identifies the contracts that are missing key security clauses, and opportunities to update them (e.g. for inclusion at contract re-let).</p>
	<p>Ofgem interprets this IGP as follows:</p>



<p>(Partially Achieved)</p> <p>IGP 4</p> <p>Assurance</p>	<p>a) [<i>assurance</i>] you recognise that third-party connections to your systems must be carefully managed and assured due to the risk that they pose. You are aware of the specific security controls that your suppliers have put in manage these risks and you have processes in place to ensure that your suppliers are maintaining these controls and abiding by all relevant processes.</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) your register of suppliers should clearly identify which suppliers have remote access to your systems. The register should also include the controls that your suppliers and your own organisation have put in place to mitigate the risks. You can demonstrate that you routinely liaise with these suppliers and have mechanisms in place (these may include audit checks, connection logs) to ensure that the remote connections are being managed in accordance with the agreement between your organisation and your supplier.</p>
<p>(Partially Achieved)</p> <p>IGP 6</p> <p>Supplier Confidence</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) [<i>have confidence</i>] you have agreements in place with all suppliers with which you share information. The agreements detail the measures that suppliers will take to secure your data. Ideally these agreements will be contractual, but they may also be best endeavours up until the point at which the contract is re-negotiated. The security measures that your suppliers are taking is appropriate for the nature of the information shared and you have assurances that the measures are being implemented in accordance with your agreement. These measures may include (but are not limited to), requirements for suppliers to have</p>

	<p>achieved an appropriate cyber security standard (such as cyber-essentials plus, ISO 27001 etc).</p> <p>b) [<i>appropriately protected</i>] the security measures that your suppliers are taking is appropriate for the nature of the information shared. You require those suppliers that hold your most sensitive data to meet more demanding cyber security requirements than those who hold less sensitive data sets.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) a standard set of security clauses that relate to custody of sensitive information.</p> <p>b) evidence that these clauses have been included in recently issued contracts.</p>
<p>(Achieved)</p> <p>IGP 7</p> <p>Knowledge of Supply Chain</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) [<i>deep understanding</i>] you have mapped and documented your supply chain, you update this documentation as new information becomes available (e.g. through contract documentation and supplier engagements) and can demonstrate that your understanding of your supply chain continually evolves. Your approach to understanding your supply chain is risk-based, meaning that you have a greater level of understanding regarding those elements of your supply chain that you assess as presenting the greatest risk.</p> <p>b) [<i>wider risks</i>] wider risks refer to risks other than cyber-security risks which could adversely impact the operation of your networks and prevent you from acquiring the devices and</p>

	<p>services you rely on. Examples include unavailability of stock, inability to export and insolvency.</p> <p>c) [<i>risk assessment and procurement process</i>] you can demonstrate that key procurement decisions have been informed by risk assessments that have considered supply chain security. Examples may include, risk assessing the use of software and hardware that has been procured from companies registered in countries known to be hostile to Great Britain.</p> <p>d) you fully comply with Stage 1 of the NCSC’s ‘How to assess and gain confidence in your supply chain cyber security’ webpage<sup>38</sup>.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) A comprehensive supply chain risk assessment which assesses the specific cyber risks associated with each of your suppliers.</p>
<p>(Achieved)</p> <p>IGP 9</p> <p>Awareness of Dependencies</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) [<i>appropriately protected from sophisticated attacks</i>] you maintain an Information Asset Register detailing what information is being held and processed by your suppliers.</p> <p>b) [<i>appropriately protected from sophisticated attacks</i>] you have ensured that suppliers store and process the information that you provide to them in a manner that is commensurate with the classification of that information. Typically, this will mean that your suppliers enforce a cyber security management system that provides a level of security that is equivalent to that of your own networks.</p>

<sup>38</sup> [How to assess and gain confidence in your supply chain... - NCSC.GOV.UK](https://www.ncsc.gov.uk/infrastructure/infrastructure-incident-response/infrastructure-incident-response-1)

	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <ul style="list-style-type: none"> <li>a) An information asset register detailing which suppliers are holding key information relating to your network and information systems.</li> <li>b) Measures to assure the cyber security of key suppliers. These measures may include use of questionnaires, mandating minimum security standards for suppliers (such as Cyber Essentials Plus), use of a supply chain cyber risk scoring service.</li> </ul>
<p>(Achieved)  IGP 10  Security Practices for Suppliers</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) [<i>appropriate security obligations</i>] you have created a standard set of security clauses for inclusion within contractual agreements. You select the appropriate security obligations for all new contracts and insert them as required</li> <li>b) [<i>proactive approach to contract management</i>] you monitor your suppliers to ensure that they are meeting their security obligations. This monitoring could take the form of engagement meetings or could extend to audits.</li> </ul> <p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <ul style="list-style-type: none"> <li>a) a standard set of security clauses.</li> <li>b) evidence that these clauses have been included in recently issued contracts.</li> </ul>

	<p>c) an assessment of the contracts of all suppliers on your supplier register which identifies the contracts that are missing key security clauses, and opportunities to update them (e.g. for inclusion at contract re-let).</p>
<p>(Achieved) IGP 11  Responsibilities</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) [<i>responsibilities</i>] you have clearly specified your requirements for security properties of devices and services in your procurement documentation. You have confirmed that your supplier understands the specification. Where necessary, the contract details which party is responsible for installing, configuring, testing and maintaining the security functionality of devices.</p> <p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) Supplier contracts with clearly specified security requirements.</p>
<p>(Achieved) IGP 12  Data Sharing with 3<sup>rd</sup> Parties</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a. [<i>data sharing with third parties is managed effectively</i>] you maintain Interface Control Documents (ICDs) which detail all network connections with third parties. Network connections could include, but are not limited to, vendor access for remote support and maintenance, customers, outsourced service providers, electricity companies.</p>

	<p>b. <i>[data sharing with third parties is managed effectively]</i> you have risk assessed each network connection with third parties and have employed appropriate controls.</p> <p>c. <i>[data sharing with third parties is managed effectively]</i> you share the minimum amount of data required for the third party to meet their obligations and maintain an Information Asset Register detailing which information is held by which suppliers.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) Network diagrams which clearly indicate information exchanges which cross the OES' network boundaries.</p> <p>b) Interface Control Documents (ICDs) which document the nature of the data that is being shared with third parties</p>
<p>(Achieved)</p> <p>IGP 13</p> <p>Mutual Support</p>	<p>Ofgem interprets this IGP as:</p> <p>a) <i>[mutual support]</i> you understand the circumstances in which breaches of your security will impact your suppliers and the circumstances in which breaches of your supplier's security will impact your essential service. You have agreements in place to inform each other in the event of these circumstances, and where necessary, will share resources with the aim of minimising the impact to all parties.</p> <p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p>

	a) Supplier contracts with clearly specified incident management responsibilities.
--	--

## References and Further Guidance



- [A.3 Asset management - NCSC.GOV.UK](#)
- [How to assess and gain confidence in your supply chain... - NCSC.GOV.UK](#)
- NIST 800-82 R2 – SA-9 External Information System Services, PS-7 Third-Party Personnel Security, SA-12 Supply Chain Protection
- IEC 62443 – Sections 7.4.1, SR 3.3 Security Functionality Verification, SR 3.4 Software and Information Integrity, SR 3.7 Error Handling
- NIST 800-53 R4 – Appendix F: SA-9 External Information System Services, PS-7 Third Party Personnel Security, SA-12 Supply Chain Protection
- ISO/IEC 27001 – A.15.2 Supplier service delivery management, A.15.2.1 Monitoring and review of supplier services, A.15.2.2 Managing changes to supplier services


# Objective B – Protecting against cyber attacks



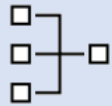
## Annex B.2 - Objective B – Protecting against cyber attacks

*Proportionate security measures are in place to protect the networks and information systems supporting essential functions from cyber-attack.*

### B1 Protection Policies and Processes

B1 Protection Policies and Processes		
<p><i>The organisation defines, implements, communicates, and enforces appropriate policies and processes that direct its overall approach to securing systems and data that support operation of essential functions.</i></p>		
Related CAF Objective(s)	Ref	Contributing Outcome
B1 – Service Protection Policies and Processes	B1.a	Policy and Processes Development
	B1.b	Policy and Processes Implementation

#### B1.a – Policy and Process Development

B1.a – Policy and Process Development		
<p><i>You have developed and continue to improve a set of cyber security and resilience policies and processes that manage and mitigate the risk of adverse impact on the essential function.</i></p>		
Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true

<p>Your policies and processes are absent or incomplete.</p> <p>Policies and processes are not applied universally or consistently.</p> <p>People often or routinely circumvent policies and processes to achieve business objectives.</p> <p>Your organisation’s security governance and risk management approach has no bearing on your policies and processes.</p> <p>System security is totally reliant on users' careful and consistent application of manual security processes.</p> <p>Policies and processes have not been reviewed in response to major changes (e.g. technology or regulatory framework), or within a suitable period.</p> <p>Policies and processes are not readily available to staff, too detailed to remember, or too hard to understand.</p>	<p>1. Your policies and processes document your <u>overarching security governance</u> and risk management approach, technical security practice and <u>specific regulatory compliance</u>.</p> <p>2. You review and update policies and processes in response to major cyber security incidents.</p>	<p>3. You <u>fully document</u> your <u>overarching security governance</u> and risk management approach, technical security practice and <u>specific regulatory compliance</u>. Cyber security is integrated and embedded throughout these policies and processes and key performance indicators are reported to your executive management.</p> <p>4. Your organisation’s policies and processes are developed to be <u>practical, usable and appropriate</u> for your essential function and your technologies.</p> <p>5. Policies and processes that <u>rely on user behaviour</u> are practical, appropriate and achievable.</p> <p>6. You review and update policies and processes at suitably regular intervals to ensure they remain relevant. This is in addition to reviews following a major cyber security incident.</p> <p>7. Any changes to the essential function or the threat it faces triggers a review of policies and processes.</p> <p>8. Your systems are designed so that they <u>remain secure</u> even when user security policies and processes are not always followed.</p>
---	---	---

### Ofgem DGE CAF Interpretation



<p>(Partially Achieved)</p> <p>IGP 1</p> <p>(Achieved)</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [<i>fully document</i>] you have a suite of documentation that describe the policies, processes and procedures you employ as part of your security management system. This documentation is easily accessible and is used by your security practitioners to guide their security related activities.</p>
--	---

<p>IGP 3</p> <p>Documented Practice</p>	<p>b) [<i>overarching security governance</i>] your suite of documentation covers cyber, physical and personnel security and describes how these 3 pillars integrate to implement a holistic security system.</p> <p>c) [<i>specific regulatory compliance</i>] you can map your policies and processes to specific CAF contributing outcomes. Your policies and processes include registers and logs that allow you to demonstrate that you are actively using them to deliver the relevant security outcomes. Relevant registers and logs are archived and provide the evidence you require to demonstrate that your security management is both appropriate and proportionate.</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) a suite of up-to-date policy, process and procedures that combine to form a security management system. This documentation should be owned by suitably qualified individuals and should be subject to periodic review and update.</p> <p>b) elements of this suite should address cyber, physical and personnel security.</p> <p>c) a complete set of up-to-date registers and logs that evidence the implementation of your policies and procedures (e.g. risk registers with records of amendments/updates).</p>
<p>(Achieved)</p> <p>IGP 4</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [<i>practical, usable and appropriate</i>] if you have used policy and process templates that you have found on-line, you have tailored them such that they are relevant to your operating context. Meaning that they consider the specific hardware, software, and support contracts that you employ.</p>

<p>Customised / Relevant</p>	<p>b) [<i>practical, usable and appropriate</i>] Your policies and processes are sufficiently thorough to meet the desired security outcome, without being so onerous as to make them unrealistic.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) a set of policy and processes that reference the specifics of your operating context.</p> <p>b) a set of logs and registers associated with each of your processes that evidence that they are being thoroughly implemented.</p>
<p>(Achieved) IGP 5  User Behaviour</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [<i>rely on user behaviour</i>] In instances where your processes are dependent on human behaviour, it must be reasonable to assume that those behaviours will be adhered to by staff. It is unreasonable to claim that security outcomes are being met through cumbersome processes that are easily circumvented.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) a set of logs and registers associated with each of your processes that evidence that they are being thoroughly implemented.</p>
<p>(Achieved) IGP 8</p>	<p>Ofgem’s interpretation is as follows:</p>

<p>Remain Secure</p>	<p>a) [<i>remain secure</i>] you have identified those policies and processes which could be circumvented or simply ignored, and you have taken additional measures to meet the relevant security outcome. Additional measures may include, but are not restricted to, management spot checks, automated reminders, additional training, layered controls (where there are specific controls intended to ‘back-stop’ against the risk of user non-compliance).</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) a set of logs and registers associated with each of your processes that evidence that they are being thoroughly implemented.</p>

## References and Further Guidance

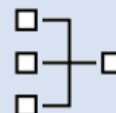


- [B.1 Service protection policies and processes - NCSC.GOV.UK](#)
- NIST SP800-82 R2 – Section 4.4
- IEC 62443 / ISA99 2-1 - Section 4.3.2.6
- ISO 27019 – Section 12.1.1

*B1.b – Policy and Process Implementation*

**B1.b – Policy and Process Implementation**

*You have successfully implemented your security policies and processes and can demonstrate the security benefits achieved.*



Not achieved	Partially achieved	Achieved
<p><b>At least one of the following statements is true</b></p>	<p><b>All the following statements are true</b></p>	<p><b>All the following statements are true</b></p>
<p>Policies and processes are ignored or only partially followed.</p> <p>The reliance on your policies and processes is not well understood.</p> <p>Staff are unaware of their responsibilities under your policies and processes.</p> <p>You do not attempt to detect breaches of policies and processes.</p> <p>Policies and processes lack integration with other organisational policies and processes.</p> <p>Your policies and processes are not well communicated across your organisation.</p>	<p>1. <u>Most of your policies and processes are followed and their application is monitored.</u></p> <p>2. Your <u>policies and processes are integrated with other organisational policies and processes, including HR assessments of individuals' trustworthiness.</u></p> <p>3. <u>All staff are aware of their responsibilities</u> under your policies and processes.</p> <p>4. All breaches of policies and processes with the potential to adversely impact the essential function are fully investigated. Other <u>breaches are tracked, assessed for trends</u> and action is taken to understand and address.</p>	<p>5. All your <u>policies and processes are followed</u>, their <u>correct application</u> and security <u>effectiveness</u> is evaluated.</p> <p>6. Your <u>policies and processes are integrated with other organisational policies and processes, including HR assessments of individuals' trustworthiness.</u></p> <p>7. Your policies and processes are effectively and appropriately communicated across all levels of the organisation resulting in good staff awareness of their responsibilities.</p> <p>8. <u>Appropriate action</u> is taken to address all breaches of policies and processes with potential to adversely impact the essential function including <u>aggregated breaches.</u></p>

## Ofgem DGE CAF Interpretation



<p>(Partially Achieved)</p> <p>IGP 1</p> <p>Following Policies and Processes</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [<i>Most of your policies and processes are followed</i>] you are confident that more than half of your policies and processes are being fully implemented. However, because many of your processes and policies are new, you are finding that they require more time to bed-in before you can be confident that they are being correctly applied and effective. You are actively taking steps to improve standards of application where necessary.</p> <p>b) [<i>application is monitored</i>] you can measure the extent to which your policies and processes are being followed and you maintain records of instances of policy violations.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) details of actions taken to improve levels of policy compliance.</p> <p>b) a register of policy and process violations the records of remedial actions.</p>
<p>(Partially Achieved)</p> <p>IGP 2</p> <p>(Achieved)</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [<i>policies and processes are integrated with other organisational policies</i>] you have identified instances where wider business processes can be integrated with security specific processes, thereby improving their effectiveness. This is particularly relevant for OT environments where Identity and Access Management</p>

<p>IGP 6</p> <p>Integrating Policies and Processes</p>	<p>(IdAM) controls are likely to be distinct from the enterprise IdAM enterprise controls. Examples include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• HR notify the appropriate IdAM system manager for all Joiner, Mover and Leaver (JML) events.</li> <li>• System permissions are reviewed in the event of disciplinary action.</li> </ul> <p>a) [<i>HR assessments of individual’s trustworthiness</i>] you follow the guidance in the following documentation:</p> <ul style="list-style-type: none"> <li>• DESNZ, Personnel Security for Critical National Infrastructure Operators and Operators of Essential Services (Energy): A Guidance Document for Security Managers on Personnel Security and National Security Vetting<sup>39</sup>.</li> </ul>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) a communication chain between the relevant department and IdAM administrators (for both IT and OT systems) detailing JML events.</p> <p>b) Details of the processes used to implement the DESNZ, Personnel Security for CNI OES (Energy) Guidance Document.</p>
<p>(Partially Achieved)</p> <p>IGP 3</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [<i>All staff are aware of their responsibilities</i>] you ensure that all your staff receive adequate training, such that they are aware of all security policies and processes that are relevant to their roles, and they have the skills to be able to implement those policies and processes.</p>

<sup>39</sup> At the time of writing, the DESNZ guidance remains in draft. It is scheduled for publication in 2023.



<p>Staff Awareness</p>	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <ul style="list-style-type: none"> <li>a) a security management system training plan.</li> <li>b) personnel records demonstrating that training has been satisfactorily completed.</li> </ul>
<p>(Partially Achieved)</p> <p>IGP 4</p> <p>Breaches</p>	<p>Ofgem’s interpretation is as follows:</p> <ul style="list-style-type: none"> <li>a) [<i>breaches are tracked and assessed for trends</i>] you can measure the extent to which your policies and processes are being followed and you maintain records of instances of policy violations.</li> </ul> <p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <ul style="list-style-type: none"> <li>a) details of actions taken to improve levels of policy compliance.</li> <li>b) a register of policy and process violations the records of remedial actions.</li> </ul>
<p>(Achieved)</p> <p>IGP 5</p>	<p>Ofgem’s interpretation is as follows:</p> <ul style="list-style-type: none"> <li>a) [<i>policies and processes are followed</i>] [<i>correct application</i>] You can measure the extent to which your policies and processes are being followed and you maintain records of instances of policy violations. For example, you maintain records of Acceptable Use Policy (AUP)</li> </ul>

<p>Policy Monitoring</p>	<p>violations (e.g. instances of shared passwords) and unauthorised use of removable media.</p> <p>b) [<i>effectiveness</i>] You review your policies and processes to ensure that they continue to contribute to the relevant security outcomes. For example, your patching status gives you a clear understanding of how effective your patching policy is being implemented.</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) A complete set of up-to-date logs and registers that evidence the implementation of your policies and procedures (e.g. risk registers with records of amendments/updates).</p> <p>b) A register of policy and process violations and records of remedial actions.</p> <p>c) A set of status reports/dashboards that are used to manage and monitor your key security processes.</p>
<p>(Achieved)</p> <p>IGP 8</p> <p>Management of Policy Application</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [<i>Appropriate action</i>] In the event of a security policy breach you consider the following actions:</p> <ul style="list-style-type: none"> <li>• completion of Post Incident Reviews</li> <li>• provision of additional training to prevent further breaches</li> <li>• commencement of disciplinary action where breaches are sufficiently serious, or repeated.</li> </ul> <p>b) [<i>aggregated breaches</i>] You periodically review the set of all breaches/policy violations with a view to identifying patterns</p>


	<p>and determining whether individual breaches may be indicators of a more sophisticated, longer-term, and multi-stage campaign.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <ul style="list-style-type: none"> <li>a) A central log of all process and policy violations and breaches.</li> <li>b) Any completed post incident reviews.</li> </ul>

## References and Further Guidance

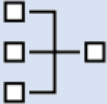


- [B.1 Service protection policies and processes - NCSC.GOV.UK](#)
- DESNZ, Personnel Security for Critical National Infrastructure Operators and Operators of Essential Services (Energy): A Guidance Document for Security Managers on Personnel Security and National Security Vetting.
- NIST SP800-82 R2 – Section 4.4
- IEC 62443 / ISA99 2-1 – Section 4.3.2.6
- ISO 27019 – Section 12.1.1

## B2 Identity and Access Control

B2 Identity and Access Control		
<p><i>The organisation understands, documents, and manages access to networks and information systems supporting the operation of essential functions. Users (or automated functions) that can access data or systems are appropriately verified, authenticated, and authorised.</i></p>		
Related CAF Objective(s)	Ref	Contributing Outcome
B2 – Identity and Access Control (IDAC)	B2.a	Identity Verification, Authentication and Authorisation
	B2.b	Device Management
	B2.c	Privileged User Management
	B2.d	Identity and Access Management (IdAM)

### B2.a – Identity Verification, Authentication and Authorisation

B2.a – Identity Verification, Authentication and Authorisation		
<p><i>You robustly verify, authenticate, and authorise access to the networks and information systems supporting your essential function.</i></p>		
Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true

<p>Initial identity verification is not robust enough to provide an acceptable level of confidence of a users' identity profile.</p> <p>Authorised users and systems with access to networks or information systems on which your essential function depends cannot be individually identified.</p> <p>Unauthorised individuals or devices can access your networks or information systems on which your essential function depends.</p> <p>The number of authorised users and systems that have access to your networks and information systems are not limited to the minimum necessary.</p>	<p>1. <u>Your process of initial identity verification</u> is robust enough to provide a reasonable level of confidence of a user's <u>identity profile</u> before allowing an authorised user access to networks and information systems that support your essential function.</p> <p>2. All authorised users and systems with access to networks or information systems on which your essential function depends are individually identified and authenticated.</p> <p>3. The number of authorised users and systems that have access to essential function networks and information systems <u>is limited to the minimum necessary</u>.</p> <p>4. You use <u>additional authentication mechanisms</u>, such as multi-factor (MFA), for <u>privileged access</u> to sensitive systems including Operational Technology where appropriate.</p> <p>5. You individually authenticate and authorise all remote access to all your networks and information systems that support your essential function.</p> <p>6. The list of users and systems with access to essential function networks and systems is reviewed on a regular basis at least annually.</p>	<p>7. Your <u>process of initial identity verification</u> is robust enough to provide a high level of confidence of a user's <u>identity profile</u> before allowing an authorised user access to networks and information systems that support your essential function.</p> <p>8. Only <u>authorised and individually authenticated users</u> can <u>physically access</u> and <u>logically connect</u> to your networks or information systems on which your essential function depends.</p> <p>9. The number of authorised users and systems that have access to all your networks and information systems supporting the essential function is <u>limited to the minimum necessary</u>.</p> <p>10. You use <u>additional authentication mechanisms</u>, such as multi-factor (MFA), for <u>privileged access</u> to all systems that operate or support your essential function.</p> <p>11. You use additional authentication mechanisms, such as multi-factor (MFA), when you individually authenticate and authorise <u>all remote user access</u> to all your networks and information systems that support your essential function.</p> <p>12. The list of users with access to networks and systems supporting and delivering the essential function is reviewed on a regular basis, at least every six months.</p>
--	---	---

**Ofgem DGE CAF Interpretation**



<p>(Partially Achieved) IGP 1</p>	<p>Ofgem's interpretation is as follows:</p> <p>a) [<i>process of initial identity verification</i>] your pre-employment checks are sufficient to establish the identity of your employees</p>
---------------------------------------	--

<p>(Achieved) IGP 7</p> <p>Identity Verification</p>	<p>and you follow DESNZ’s Personnel Security for CNI and OES (Energy) Guidance document (see B1.b).</p> <p>b) [<i>identity profile</i>] your pre-employment check policy specifies the identity profile required for each role. The identity profile relates to the level of confidence you require in an individual’s declared identity, for example Government’s identify profile guidance<sup>40</sup>. You are not required to follow the Government’s identity profile guidance prescriptively, however, you should be able to demonstrate that the identity profiles you use are appropriate to the level of access that you are granting to your systems.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) an identity and access management policy that details the process of initial identity verification.</p> <p>b) a documented pre-employment check process that follows DESNZ’s Personnel Security for CNI and OES (Energy) Guidance document (see B1.b).</p> <p>c) you have confirmed that any 3<sup>rd</sup> party organisations with access to your systems employ suitably robust identity verification processes.</p>
<p>(Partially Achieved) IGP 3</p> <p>(Achieved) IGP 9</p> <p>Least Privilege</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a. [<i>limited to the minimum necessary</i>] you enforce the principle of least privilege, and you actively manage your Access Control Lists in response to Joiner, Mover and Leaver events (see B1.b)</p> <p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) an identity and access management policy that details how you implement the principle of least privilege on your networks and</p>

<sup>40</sup> [Identity profiles - GOV.UK \(www.gov.uk\)](http://www.gov.uk)

	<p>information systems. Examples may include Roles Based or Attribute Based Access Control schemes (RBAC, ABAC). In instances where you rely on system specific IdAM mechanisms your access management policy should detail the processes you employ for each separate system.</p>
<p>(Partially Achieved) IGP 4</p> <p>(Achieved) IGP 10</p> <p>Additional Authentication</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [<i>Additional Authentication, for privileged access</i>] additional authentication refers to mechanisms that are in addition to the password or pass-numbers that should be employed on all devices.</p> <p>In an OT environment almost all physical and logical access to devices can be defined as privileged, however, it is also the case that many devices will not natively support additional authentication methods (such as MFA).</p> <p>Ofgem expects OES to risk assess all interactive devices (e.g. OT workstations and HMIs) and apply additional authentication to control local access where it is appropriate and proportionate to do so. It is accepted that the inability of many obsolete devices to natively support additional authentication methods, and the implementation of compensating controls, will mean there are instances where it is neither appropriate nor proportionate.</p> <p>Ofgem does expect OES to apply additional authentication to networks and information systems that are hosted in the enterprise domain.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) a register of the mechanisms providing authentication services for all network and information systems supporting your essential function (this may be recorded as a field in your asset registers).</p>

<p>(Achieved) IGP 8</p> <p>Access Control</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [<i>authorised and individually authenticated</i>] You understand, and have documented, which roles (and associated individuals) are authorised to access each system. Wherever feasible, your systems require that users are individually authenticated.</p> <p>Where it is not feasible to individually authenticate, you have limited the use of shared credentials to those situations where there is a clear safety or operational justification to do so (e.g. speed of response).</p> <p>In instances where shared credentials are in use, you use compensating controls to enhance access control (such as enhanced physical access controls) and you have taken measures to reduce the number of individuals using shared credentials. For example, each control room shift is issued with a set of shared credentials, rather than all shifts using the same shared credentials.</p> <p>b) [<i>physically access</i>] your physical security management system has been designed to restrict physical access to your networks and information systems. Your physical security measures have been designed to complement your logical access controls. For example, enhanced physical access controls are employed to limit access to your most sensitive systems.</p> <p>c) [<i>logically connect</i>] your network and information systems all have an appropriate authentication mechanism for both local and remote access. If there are instances where this is not possible - due to obsolete hardware and software - you have logged this as a risk in your risk register and you are enforcing compensating controls.</p> <p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p>
---	--



	<ul style="list-style-type: none"> <li>a) an identity and access management policy that details the process for approving authorisations and detailing the process for maintaining access control lists.</li> <li>b) a register of the mechanisms providing authentication services for all network and information systems supporting your essential function (this may be recorded as a field in your asset registers).</li> <li>c) where domain level authentication services are being employed, the service on the OT/CNI networks and enterprise networks should be separate. OT systems should not rely on services from the IT domain for authentication and authorisation.</li> <li>d) A physical security management system that meets the security outcomes detailed in CAF Objective E (DGE Supplement) and complements your network zoning policy. E.g. your most critical networks are housed within buildings/facilities that have enhanced physical security measures.</li> <li>e) In cases where logical and physical access controls do not meet best practice, the risks should be recorded in your risk register with evidence of compensating controls.</li> </ul>
<p>(Achieved) IGP 11</p> <p>Remote Access Authentication</p>	<p>Ofgem’s interpretation is as follows:</p> <ul style="list-style-type: none"> <li>a) [<i>all remote user access</i>] any user requiring a remote connection to your network and information systems must do so via a mechanism that enforces additional authentication mechanisms.</li> </ul> <p>Additional authentication refers to mechanisms that are in addition to passwords or numbers.</p> <p>Where users require remote access to your OT networks, they will be required to pass through a minimum of two discrete authentication mechanisms. The first to gain access to the corporate network and the second to gain access from the corporate network to the OT/CNI network.</p>

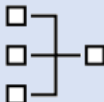
	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) network diagrams clearly showing the IdAM services that control remote access.</p>
--	---

## References and Further Guidance



- [B.2 Identity and access control - NCSC.GOV.UK](#)
- NIST SP800-82 R2 – Sections 5.15 & 6.2.7, AC-3 Access Enforcement, AC-17 Remote Access, IA-2 Identification and Authentication (Organizational Users), IA-8 Identification and Authentication (Non-Organisational Users), PE-3 Physical Access Control
- IEC 62443 / ISA99 3-3, SR 1.1 Human User Identification and Authentication, SR 1.2 Software Process and Device Identification and Authentication, SR 1.5 Authenticator Management, SR 1.7 Strength of Password-based Authentication
- ISA 99 (Part 4) - I&AM Requirement 10
- ISO 27002 Clause 9

B2.b – Device Management

<b>B2.b – Device Management</b>		
<p><i>You fully know and have trust in the devices that are used to access your networks, information systems and data that support your essential function.</i></p>		
<b>Not achieved</b>	<b>Partially achieved</b>	<b>Achieved</b>
<b>At least one of the following statements is true</b>	<b>All the following statements are true</b>	<b>All the following statements are true</b>
<p>Users can connect to your essential function's networks using devices that are not corporately managed.</p> <p>Privileged users can perform administrative functions from devices that are not corporately managed.</p> <p>You have not gained assurance in the security of any third-party devices or networks connected to your systems.</p> <p>Physically connecting a device to your network gives that device access without device or user authentication.</p>	<ol style="list-style-type: none"> <li>1. Only <u>corporately owned and managed devices</u> can access your essential function's networks and information systems.</li> <li>2. All privileged access occurs from corporately management devices <u>dedicated to management functions</u>.</li> <li>3. You have <u>sought to understand</u> the security properties of third-party devices and networks before they can be connected to your systems. You have taken appropriate steps to mitigate any risks identified.</li> <li>4. The act of connecting to a network port or cable does not grant access to any systems.</li> <li>5. You are able to detect unknown devices being connected to your network and investigate such incidents.</li> </ol>	<ol style="list-style-type: none"> <li>6. <u>Dedicated devices</u> are used for <u>privileged actions</u> (such as administration or accessing the essential function's network and information systems). These devices are not used for directly browsing the web or accessing email.</li> <li>7. You either <u>obtain independent and professional assurance</u> of the security of third-party devices or networks before they connect to your systems, or you only allow <u>third-party devices or networks dedicated to supporting your systems</u> to connect.</li> <li>8. <u>You perform certificate-based device identity management</u> and only allow known devices to access systems necessary for the operation of your essential function.</li> <li>9. You perform regular scans to detect unknown devices and investigate any findings.</li> </ol>

## Ofgem DGE CAF Interpretation



<p>(Partially Achieved)</p> <p>IGP 1</p> <p>Managed Devices</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [corporately owned and managed devices] these devices may belong to your own organisation, or, to a third-party supplier. However, in both cases the devices must be governed by a formalised IT policy. This precludes the use of any privately owned devices (e.g. Bring Your Own Devices) and the use of any corporate devices to which an employee has administrative rights.</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) a corporate mobile device management policy (which will typically be owned by your IT department).</p> <p>b) a policy document describing the use of PAWs on the OT and IT environments and how you control the use of these devices.</p>
<p>(Partially Achieved)</p> <p>IGP 2</p> <p>Privileged Access</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [<i>dedicated to management functions</i>] you have a process to ensure that the Privileged Access Workstations (PAWs) that temporarily connect to your OT systems for the purpose of system management (e.g. commissioning, configuring and maintaining) are <b>only</b> used for these purposes. This process extends to third party suppliers as well as your own staff.</p>

	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <ul style="list-style-type: none"> <li>a) a policy document describing the use of PAWs on the OT and IT environments and how you control the use of these devices.</li> <li>b) Work instructions or Maintenance Task Procedures that specify the use of PAWS.</li> <li>c) a register of all your PAWs and their permitted use (this information is likely to be captured in your asset register).</li> </ul>
<p>(Partially Achieved)  IGP 3</p>	<p>Ofgem’s interpretation is as follows:</p> <ul style="list-style-type: none"> <li>a) [<i>sought to understand</i>] Ofgem’s expects OES to demonstrate the IGP described at IGP 7.</li> </ul>
<p>(Achieved)  IGP 6  Dedicated Devices</p>	<p>Ofgem’s interpretation is as follows:</p> <ul style="list-style-type: none"> <li>a) [<i>Dedicated devices</i>] you have a process to ensure that the devices that temporarily connect to your OT systems for the purposes of commissioning, configuring and maintaining are <b>only</b> used for these purposes. This process extends to third party suppliers as well as your own staff.</li> <li>b) [<i>Dedicated devices</i>] you class any device, including removable media, that is temporarily connecting to your OT environment as a privileged access device and manage it accordingly.</li> </ul> <p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <ul style="list-style-type: none"> <li>a) a policy document describing the use of PAWs on the OT and IT environments and how you control the use of these devices.</li> <li>b) Work instructions or Maintenance Task Procedures that specify the use of PAWS.</li> </ul>

	<ul style="list-style-type: none"> <li>c) evidence that third party suppliers are contractually bound to comply with your PAW policy.</li> <li>d) a register of all your PAWs and their permitted use (this information is likely to captured in your asset register).</li> </ul>
<p>(Achieved)</p> <p>IGP 7 –</p> <p>Awareness of Risks posed by Third Party Assets</p>	<p>Ofgem’s interpretation is as follows:</p> <ul style="list-style-type: none"> <li>a) [<i>independent and professional assurance</i>] your default policy is that no 3<sup>rd</sup> party devices connect to your network or systems. Wherever possible, you supply 3<sup>rd</sup> parties with the devices and software that they need to enable them to complete their tasks and these devices remain under your supervision.</li> </ul> <p>However, in cases where it is essential for 3<sup>rd</sup> parties to use their own devices, you have a process to minimise the risk they present to your network. This process may include, but is not limited to, scanning for malware and limiting the software installed to only that which is necessary for the task.</p> <p>You do not accept the assurances of the 3<sup>rd</sup> party that their devices are secure. Where it is necessary for 3<sup>rd</sup> parties to connect their own devices to your systems, you subject those devices to a minimum set of checks which are conducted by your own staff prior to allowing connection.</p> <p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <ul style="list-style-type: none"> <li>a) a policy document describing the use of PAWs on the OT and IT environments and how you control the use of these devices.</li> <li>b) evidence that third party suppliers are contractually bound to comply with your PAW and network connection policies.</li> </ul>

<p>(Achieved)</p> <p>IGP 8 –</p> <p>IdAM</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [<i>You perform certificate-based device identity management</i>] You perform certificate-based device identity management where practicable. However, it may not be feasible to perform certificate-based device identity management on all your OT networks. This is due to the number of discrete OT networks that you operate and the number of OT devices that will not support the technique. In these cases, you compensate by enforcing strict physical security controls to reduce the risk of connection of unauthorised devices. You employ physical and logical port security wherever possible.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice to have been generated:</p> <p>a) details of any certificate-based device identity management schemes that you employ.</p> <p>b) evidence of physical and logical port security.</p>

## References and Further Guidance

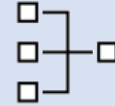


- [B.2 Identity and access control - NCSC.GOV.UK](#)
- NIST SP800-82 R2 – IA-3 Device Identification and Authentication
- IEC 62443/ISA99 3-3 – SR 5.4 Application Partitioning, SR 1.2 Software Process and Device Identification and Authentication

*B2.c – Privileged User Management*

**B2.c – Privileged User Management**

*You closely manage privileged user access to networks and information systems supporting the essential function.*



Not achieved	Partially achieved	Achieved
<p><b>At least one of the following statements is true</b></p>	<p><b>All of the following statements are true</b></p>	<p><b>All the following statements are true</b></p>
<p>The identities of the individuals with privileged access to your essential function systems (infrastructure, platforms, software, configuration, etc) are not known or not managed.</p> <p>Privileged user access to your essential function systems is via weak authentication mechanisms (e.g. only simple passwords).</p> <p>The list of privileged users has not been reviewed recently (e.g. within the last 12 months).</p> <p>Privileged user access is granted on a system-wide basis rather than by role or function.</p> <p>Privileged user access to your essential function is via generic, shared or default name accounts.</p> <p>Where there are “always on” terminals which can perform privileged actions (such as in a control room), there are no additional controls (e.g. physical controls) to ensure access is appropriately restricted.</p> <p>There is no logical separation between roles that an individual may have and hence the actions they perform. (e.g. access to corporate email and privilege user actions).</p>	<ol style="list-style-type: none"> <li>Privileged user access requires additional validation, but this does not use a strong form of authentication (e.g. multi-factor (MFA) or additional real-time security monitoring).</li> <li>The identities of the individuals with privileged access to your essential function systems (infrastructure, platforms, software, configuration, etc) are known and managed. This includes third parties.</li> <li>Activity by privileged users is routinely reviewed and validated. (e.g. at least annually).</li> <li>Privileged users are only granted specific privileged permissions which are essential to their business role or function.</li> </ol>	<ol style="list-style-type: none"> <li>Privileged user access to your essential function systems is carried out from <u>dedicated separate accounts that are closely monitored and managed</u>.</li> <li>The issuing of <u>temporary, time-bound rights</u> for privileged user access and external third-party support access is in place.</li> <li>Privileged user access rights are regularly reviewed and always updated as part of your joiners, movers and leavers process.</li> <li>All privileged user access to your networks and information systems requires <u>strong authentication, such as multi-factor (MFA) or additional real-time security monitoring</u>.</li> <li>All privileged user activity is routinely <u>reviewed, validated and recorded</u> for offline analysis and investigation.</li> </ol>




## Ofgem DGE CAF Interpretation



<p>(Achieved)</p> <p>IGP 5 –</p> <p>Dedicated Accounts</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [<i>dedicated separate accounts that are closely monitored and managed</i>] This amounts to:</p> <ul style="list-style-type: none"> <li>• privileged user access is conducted from dedicated privileged user accounts and devices which are not used for typical day-to-day functions (e.g. email, web browsing).</li> <li>• all privileged user actions are logged and you have defined SIEM rules that will detect suspicious and potentially damaging events. The rules that you have defined are system specific (for example you are monitoring for changes to safety and process critical set points and alarms).</li> </ul> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) a privileged user access policy.</p> <p>b) a logging and monitoring policy which specifically addresses privileged user monitoring.</p>
<p>(Achieved)</p> <p>IGP 6 –</p> <p>Time Bound Provisioning</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [<i>temporary, time-bound rights</i>] You have processes in place which enforce ‘<i>just in time administration</i>’. Just in time administration ensures that the privileged user is only permitted to access a system after they have been approved to do so for a specific purpose. Ideally, just in time administration should be enforced via</p>

	<p>technical means such as a Privileged Access Management (PAM) Service.</p> <p>It may not be possible to implement a PAM on your OT networks, where this is the case you should enforce just in time administration through alternative processes, such as a documented works request/permit to work. In certain circumstances, just in time administration can also be enforced by securing PAWs or required hardware in locked storage, release from storage would form part of the works request/permit to work process.</p> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Details of any PAM service that is being employed.</li> <li>b) Privileged user access policy and processes.</li> </ul>
<p>(Achieved)</p> <p>IGP 8 –</p> <p>Authentication</p>	<p>Ofgem’s interpretation is as follow:</p> <ul style="list-style-type: none"> <li>a) [<i>strong authentication, such as multi-factor (MFA) or additional real-time security monitoring</i>] Strong local authentication, such as MFA, is achievable in the IT environment and Ofgem expects to see such measures implemented.</li> </ul> <p>Strong local authentication in the OT environment is more difficult to achieve, but OES are expected to work towards it. OES should risk assess each OT workstation and HMI and determine the degree of authentication that it is appropriate and proportionate. OT workstations and HMIs serving critical systems that are outside of an access-controlled building (but within the site perimeter) should be prioritised for upgrade to a type that does support MFA (where safety considerations allow). In cases where strong local authentication is not yet possible, it is reasonable for OES to elect to use strong physical security controls (such as Automatic Access Control Systems) or electronic key cabinets as a compensating control.</p>

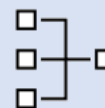
	<p>OES should consider changing procurement guides to ensure that any new OT workstations or HMIs are supplied with the functionality to support strong authentication.</p> <p>Ofgem expects that all remote access is subject to MFA as described at B2.a.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>• A register of all OT workstations and HMIs, detailing the local access controls that are being enforced (your asset register should provide these details).</li> </ul>
<p>(Achieved)</p> <p>IGP 9 –</p> <p>Tracking of Privileged Access</p>	<p>Ofgem’s interpretation is as follows:</p> <ul style="list-style-type: none"> <li>a) [reviewed, validated and recorded] You have tools and/or manual processes in place to ensure that logs of all privileged user actions in the IT and OT environments are checked to confirm that they correspond to legitimate activity. All remote 3rd party connections are recorded and audit events are passed to a SIEM.</li> </ul> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) A logging and monitoring policy which specifically addresses privileged user monitoring.</li> </ul>
<p><b>References and Further Guidance</b></p> <div style="text-align: right;">  </div>	

- [B.2 Identity and access control - NCSC.GOV.UK](#)
- [Introduction to identity and access management - NCSC.GOV.UK](#)
- IEC 62443-2-1 – Section A.3.3.2.2
- IEC 62443 / ISA99 3-3 – SR 1.4 Identifier Management, SR 2.1 Authorisation Enforcement, RE 2 Password Lifetime Enforcement for All Users
- ISO 27019 – Section 9.2.3

*B2.d – Identity and Access Management (IdAM)*

**B2.d – Identity and Access Management (IdAM)**

*You assure good management and maintenance of identity and access control for your networks and information systems supporting the essential function.*



Not achieved	Partially achieved	Achieved
<b>At least one of the following statements is true</b>	<b>All of the following statements are true</b>	<b>All the following statements are true</b>
<p>Greater rights are granted than necessary.</p> <p>Identity validation and requirement for access of a user, device or systems is not carried out.</p> <p>User rights are not reviewed when users change roles.</p> <p>User rights remain active when users leave your organisation.</p> <p>Access rights granted to devices or systems to access other devices and systems are not reviewed on a regular basis (at least annually).</p>	<p>1. You follow a <u>robust procedure</u> to verify each user and issue the <u>minimum required access rights</u>.</p> <p>2. You regularly review access rights and those no longer needed are revoked.</p> <p>3. User access rights are reviewed when users change roles via your joiners, leavers and movers process.</p> <p>4. All user, device and system access to the systems supporting the essential function is <u>logged and monitored</u>, but it is not compared to other log data or access records.</p>	<p>5. You follow a <u>robust procedure</u> to verify each user and issue the <u>minimum required access rights</u>, and the application of the procedure is regularly audited.</p> <p>6. User permissions are reviewed both when people change roles via your joiners, leavers and movers process and at regular intervals - at least annually.</p> <p>7. All user, device and systems access to the systems supporting the essential function is <u>logged and monitored</u>.</p> <p>8. You <u>regularly review access logs</u> and correlate this data with other access records and expected activity.</p> <p>9. Attempts by unauthorised users, devices or systems to connect to the systems supporting the essential function are alerted, promptly assessed and investigated.</p>

## Ofgem DGE CAF Interpretation



<p>(Partially Achieved)</p> <p>IGP 1</p> <p>(Achieved)</p> <p>IGP 5</p> <p>Procedure</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [robust procedure] You meet the IGPs at B2.a</p> <p>b) [minimum required access rights] You ensure that staff only have access to the systems that they require to carry out their roles. You avoid providing ‘blanket-access’ to all systems for all staff.</p> <p>You make full use of the functionality on all of your devices and, where the device allows, you issue permissions on the basis of the principal of least privilege and distinguish between standard and administrative users. This requires that you fully understand the user administration functionality on your devices and that you have correctly configured it so as to provide access protection to critical functions.</p>
	<p>Where appropriate, Ofgem would expect to see the following as evidence of good practice being applied.</p> <p>For b) above</p> <p>a) Relevant IDAM policies and proof, in the form of your critical systems.</p> <p>b) Your IdAM policies clearly define the degree to which you are able to limit permissions on each of your devices and demonstrates that you’re making full use of this functionality.</p>
<p>(Partially Achieved)</p>	<p>Ofgem’s interpretation is as follows:</p>

<p>IGP 4</p> <p>(Achieved)</p> <p>IGP 7</p> <p>Logging and Monitoring</p>	<p>a) [logged and monitored] You have a process to monitor user access to all your systems. Ideally this process will be automated, and you will be able to monitor logs from a central SIEM. However, this may not be possible for stand-alone systems, such as packaged plant. In these instances, you have a process of copying access event logs from HMIs and reviewing them manually at appropriate interval. This form of monitoring would be considered appropriate and proportionate for systems for which operator access to the HMIs is infrequent and the number of log entries is correspondingly small.</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) SIEM tooling covering essential systems.</li> <li>b) demonstration of a process to manually check logs on systems that are not integrated with a SIEM tool.</li> </ul>
<p>(Achieved)</p> <p>IGP 8</p> <p>Review of Activity</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [regularly review access logs] In cases where you have implemented SIEM tooling, and have configured alerts, this would typically be considered as reviewing access logs in real-time. In cases where you are reliant on copying access event logs from HMIs, and are reviewing them manually, you have a scheduled (planned and periodic) process to complete this activity.</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) SIEM tooling covering essential systems.</li> <li>b) demonstration of a process to manually check logs on systems that are not integrated with a SIEM tool.</li> </ul>


## References and Further Guidance



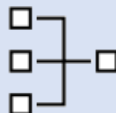
- [B.2 Identity and access control - NCSC.GOV.UK](#)
- [Introduction to identity and access management - NCSC.GOV.UK](#)
- NIST 800-82 R2 – Section 6.2.1, Appendix G AC-1 Access Control Policy and Procedures, AC-2 Account Management, AC-3 Access Enforcement, AC-4 Information Flow Enforcement, AC-5 Separation of Duties, AC-6 Least Privilege, AC-7 Unsuccessful Logon Attempts, AC-8 System Use Notification, IA-1 Identification and Authentication Policy and Procedures, IA-2 Identification and Authentication (Organizational Users), IA-5 Authenticator Management, IA-6 Authenticator Feedback, IA-8 Identification and Authentication (Non-Organizational Users)
- IEC 62443-2-1 – Section A.3.3.2.2
- ISO 27001 – Sections 7.1.1, 7.1.2, 9.2, 12.4
- ISO 27019 – Sections 9.1, 9.2, 9.3, 9.4
- HMG GPG 44 – Authentication of claimed identity



## B3 Data security

B3 Data security		
<p><i>Data stored or transmitted electronically is protected from actions such as unauthorised access, modification, or deletion that may cause an adverse impact on essential functions. Such protection extends to the means by which authorised users, devices and systems access critical data necessary for the operation of essential functions. It also covers information that would assist an attacker, such as design details of networks and information systems.</i></p>		
Related CAF Objective(s)	Ref	Contributing Outcome
B3 - Data Security	B3.a	Understanding Data
	B3.b	Data in Transit
	B3.c	Stored Data
	B3.d	Mobile Data
	B3.e	Media / Equipment Sanitisation

### B3.a – Understanding Data

B3.a – Understanding Data		
<p><i>You have a good understanding of data important to the operation of the essential function, where it is stored, where it travels and how unavailability or unauthorised access, modification or deletion would adversely impact the essential function. This also applies to third parties storing or accessing data important to the operation of essential functions.</i></p>		
Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All the following statements are true

<p>You have incomplete knowledge of what data is used by and produced in the operation of the essential function.</p> <p>You have not identified the important data on which your essential function relies.</p> <p>You have not identified who has access to data important to the operation of the essential function.</p> <p>You have not clearly articulated the impact of data compromise or inaccessibility.</p>	<ol style="list-style-type: none"> <li>1. You have identified and catalogued all the data <u>important to the operation of the essential function</u>, or that would <u>assist an attacker</u>.</li> <li>2. You have identified and catalogued who has access to the data important to the operation of the essential function.</li> <li>3. You periodically review location, transmission, quantity and quality of data important to the operation of the essential function.</li> <li>4. You have identified all mobile devices and media that hold data important to the operation of the essential function.</li> <li>5. You <u>understand and document</u> the impact on your essential function of all relevant scenarios, including unauthorised access, modification or deletion, or when authorised users are unable to appropriately access this data.</li> <li>6. You <u>occasionally validate</u> these documented impact statements.</li> </ol>	<ol style="list-style-type: none"> <li>7. You have identified and catalogued all the data <u>important to the operation of the essential function</u>, or that would <u>assist an attacker</u>.</li> <li>8. You have identified and catalogued who has access to the data important to the operation of the essential function.</li> <li>9. You maintain a current understanding of the location, quantity and quality of data important to the operation of the essential function.</li> <li>10. You take steps to remove or minimise unnecessary copies or unneeded historic data.</li> <li>11. You have identified all mobile devices and media that may hold data important to the operation of the essential function.</li> <li>12. You maintain a current <u>understanding of the data links used to transmit data</u> that is important to your essential function.</li> <li>13. You understand the context, limitations and dependencies of your important data.</li> <li>14. You <u>understand and document</u> the impact on your essential function of all relevant scenarios, including unauthorised data access, modification or deletion, or when authorised users are unable to appropriately access this data.</li> <li>15. You validate these documented impact statements regularly, at least annually.</li> </ol>
--	--	--

## Ofgem DGE CAF Interpretation



<p>(Partially Achieved)</p> <p>IGP 1</p> <p>(Achieved)</p> <p>IGP 7</p> <p>Data Context</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [<i>important to the operation of the essential function</i>] the operation and management of your essential service will rely on multiple data sources. This data may include, but will not be restricted to, telemetry data required to maintain ‘view’ and ‘control’ of the system, historical plant historian data<sup>41</sup>, system design and configuration data and system back-ups.</p> <p>b) [assist an attacker] Implementing a cyber security management system creates several documents that would be especially useful to an attacker. These documents include, but are not limited to, network diagrams, asset registers, configuration management databases, vulnerability registers and attack path maps. Once these documents are created it is vital that they are adequately protected. Protection is achieved by understanding the types of data that could assist an attacker, marking all such documentation as sensitive (in accordance with your company policy) and ensuring that the data is stored and secured in a manner that is commensurate with the security marking.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) A completed NIS Information Asset Register (IAR). The Information Asset Register may be part of your main NIS asset register, or it may be a discrete document. The IAR should include details of:</p> <ul style="list-style-type: none"> <li>• Data and information held</li> </ul>

<sup>41</sup> The type and nature of this data will vary considerably between OES and it is the responsibility of individual OES to identify important data sources.

	<ul style="list-style-type: none"> <li>• Volume</li> <li>• Classification and/or sensitivity</li> <li>• System(s) which use it, both organisational and third party</li> <li>• Location where the data is stored (e.g. onsite, offsite, third-party location)</li> <li>• Format data is stored in (e.g. physical (paper copies) or digital (server storage/tape drives), mobile media)</li> <li>• Technical security controls that have been applied to data stored on mobile devices (e.g. encryption)</li> <li>• Access control restrictions</li> <li>• Data backup requirements.</li> </ul> <p>b) Meeting minutes demonstrating that the IAR has been reviewed and revised where necessary.</p>
<p>(Partially Achieved)</p> <p>IGP 5 &amp; 6</p> <p>(Achieved)</p> <p>IGP 14</p> <p>Documented Risks</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) [understand and document] your NIS risk register should include risks associated with loss of Confidentiality, Integrity and Availability (CIA) of data important to the operation of the essential service.</p> <p>b) [occasionally validate] You review your risk register in accordance with guidance issued at A1.c.</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) A risk register with entries that related to loss of CIA of critical data streams and where appropriate, historic data.</p>
<p>(Achieved)</p>	<p>Ofgem interprets this IGP as follows:</p>

<p>IGP 12</p> <p>Data Flow</p>	<p>a) [understanding of the data links used to transmit data] You maintain Interface Control Documents (ICD) for each system. These ICDs detail all the information that is shared between systems, across network boundaries (particularly between OT and enterprise networks) and outside of the organisation. You have used this ICD to help inform your risk register (see IGP 5). Your ICD captures the following information:</p> <ul style="list-style-type: none"> <li>• Data/fields transmitted</li> <li>• Data recipient (system or organisation)</li> <li>• Data link (e.g. internal network, leased line, public network)</li> <li>• Transmission protocol including descriptions of protocol breaks used at boundaries</li> <li>• Criticality of data transmission, including an assessment of whether the essential service relies on the transmission</li> <li>• Security controls applied to the transmission, including details of any boundary devices that are traversed by the data.</li> </ul>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Interface Control Documents (ICDs) for all your systems.</p>

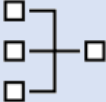

## References and Further Guidance



- [B.3 Data security - NCSC.GOV.UK](#)
- NIST 800-82 R2 – SI-12 Information Handling and Retention, SI-10 Information Input Validation
- IEC 62443-2-1 – Sections 4.3.4.3 System Development and Maintenance, 4.3.4.4 Information and Document Management, 4.3.3.3 Physical and Environmental Security
- NIST 800-53 R4 – Appendix F: SI-12 Information Handling and Retention, AC-16 Security Attributes, ZI-10 Information Input Validation

- ISO 27001 – A.12.1 Security Requirements of Information Systems, A.12.2 Correct Processing in Applications, 4.3.1 General Document Requirements, 4.3.2 Control of Documents, 4.3.3 Control of Records
- ISO 27019 – 8.2 Information classification

B3.b – Data in Transit

<h2 style="margin: 0;">B3.b – Data in Transit</h2>		
<p><i>You securely configure the network and information systems that support the operation of essential functions.</i></p>		
Not achieved	Partially achieved	Achieved
<p><b>At least one of the following statements is true</b></p>	<p><b>All of the following statements are true</b></p>	<p><b>All the following statements are true</b></p>
<p>You do not know what all your data links are, or which carry data important to the operation of the essential function.</p> <p>Data important to the operation of the essential function travels without technical protection over non-trusted or openly accessible carriers.</p> <p>Critical data paths that could fail, be jammed, be overloaded, etc. have no alternative path.</p>	<p>1. You have identified and <u>protected (effectively and proportionately)</u> all the <u>data links</u> that carry data important to the operation of your essential function.</p> <p>2. You apply appropriate technical means (e.g. cryptography) to protect data that travels over non-trusted or openly accessible carriers, but you have limited or no confidence in the robustness of the protection applied.</p>	<p>3. You have identified and protected (effectively and proportionately) all the data links that carry data important to the operation of your essential function.</p> <p>4. You apply appropriate physical and / or technical means to protect data that travels over non-trusted or openly accessible carriers, with <u>justified confidence</u> in the robustness of the protection applied.</p> <p>5. Suitable <u>alternative transmission paths</u> are available where there is a significant risk of impact on the operation of the essential function due to resource limitation (e.g. transmission equipment or function failure, or important data being blocked or jammed).</p>
<h3 style="margin: 0;">Ofgem DGE CAF Interpretation</h3>		
		
	<p>Ofgem’s interpretation is as follows:</p>	

<p>(Partially achieved)</p> <p>IGP 1 –</p> <p>Data Protection</p>	<p>a) [<i>protected (effectively and proportionately)</i>] you have taken measures to protect your data that is commensurate with the consequence of compromise. For example, you have taken measures to assure the integrity of data flows that are critical to the safe operation of your plant, and you have taken measures to ensure the confidentiality of data that could assist and attacker.</p> <p>b) [data links] you have taken account of all data links that carry important data, this includes networked transmission of data, use of removable media and the physical carriage of hard copy data.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) a set of data flow diagrams (or similar) of sufficient detail to show individual data links and the means of protection (e.g. VPN, radio link encryption).</p> <p>b) interface Control Documents that specify the nature of the data links used for each interface.</p>
<p>(Achieved)</p> <p>IGP 4 –</p> <p>Assurance</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [justified confidence] You have tested and validated the means you are using to protect your data. Ofgem would expect an OES to have conducted technical testing of their networks to confirm that the encryption function on all data flows across non-trusted (e.g. public internet) or openly accessible carriers (e.g. wi-fi, radio links) have been correctly configured.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) penetration test results.</p>




<p>(Achieved)</p> <p>IGP 5 –</p> <p>Alternate Solutions</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [alternative transmission paths] All data transmissions that have been identified as critical to the provision of the essential service have been recorded in the relevant Interface Control Documents (ICD) and the NIS risk register. You have assessed whether these transmission paths are sufficiently resilient. Where your assessments indicate that that there is significant risk of the failure or compromise you have considered the provision of multi-path and or modular redundant communication links.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) the provision of resilient communication designs where they are required.</p> <p>b) business resilience or business continuity plans that address the need for maintenance and stand up of alternative solutions.</p>

## References and Further Guidance



- [B.3 Data security - NCSC.GOV.UK](#)
- NIST SP800-82 R2 – Sections 5.14, 6.2.16, Appendix G MP-5 Media Transport
- IEC 62443-3-3 – SR 3.1 Communication Integrity
- ISO 27019 – Section 13.1.4
- NCSC NIS Guidance B5

B3.c – Stored Data

<b>B3.c – Stored Data</b>		
<p><i>You have protected stored data important to the operation of the essential function.</i></p>		
<b>Not achieved</b>	<b>Partially achieved</b>	<b>Achieved</b>
<b>At least one of the following statements is true</b>	<b>All of the following statements are true</b>	<b>All the following statements are true</b>
<p>You have no, or limited, knowledge of where data important to the operation of the essential function is stored.</p> <p>You have not protected vulnerable stored data important to the operation of the essential function in a suitable way.</p> <p>Backups are incomplete, untested, not adequately secured or could be inaccessible in a disaster recovery or business continuity situation.</p>	<ol style="list-style-type: none"> <li>1. All copies of <u>data important to the operation of your essential function</u> are necessary. Where this important data is transferred to less secure systems, the data is provided with limited detail and / or as a read-only copy.</li> <li>2. You have applied suitable physical and / or technical means to protect this important stored data from unauthorised access, modification or deletion.</li> <li>3. If cryptographic protections are used, you apply suitable technical and procedural means, but you have limited or no confidence in the robustness of the protection applied.</li> <li>4. You have suitable, <u>secured backups of data</u> to allow the operation of the essential function to continue should the original data not be available. This may include off-line or segregated backups, or appropriate alternative forms such as paper copies.</li> </ol>	<ol style="list-style-type: none"> <li>5. You have only necessary copies of this data. Where data is transferred to less secure systems, the data is provided with limited detail and / or as a read-only copy.</li> <li>6. You have applied suitable physical or technical means to protect this important stored data from unauthorised access, modification or deletion.</li> <li>7. If cryptographic protections are used you apply suitable technical and procedural means, and you have justified confidence in the robustness of the protection applied.</li> <li>8. You have suitable, secured backups of data to allow the operation of the essential function to continue should the original data not be available. This may include off-line or segregated backups, or appropriate alternative forms such as paper copies.</li> <li>9. Necessary historic or archive data is suitably secured in storage.</li> </ol>

## Ofgem DGE CAF Interpretation



<p>(Partially Achieved)</p> <p>IGP 1 –</p> <p>Data Propagation</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [<i>important to the operation of the essential function</i>] the operation and management of your essential service will rely on multiple data sources. This data may include, but will not be restricted to, may be telemetry data required to maintain ‘view’ and ‘control’ of the system, it may be historic plant historian data<sup>42</sup>, system design and configuration data, system back-ups.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) An Information Asset Register (IAR), as detailed at Ofgem’s interpretation of IGP1, of B3.a.</p>
<p>(Partially Achieved)</p> <p>IGP 4 –</p> <p>Backups</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [secured backups of data] You have taken account of principle B5.c.</p>

## References and Further Guidance

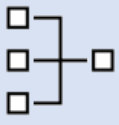


- [B.3 Data security - NCSC.GOV.UK](https://www.ncsc.gov.uk/section/102/b3)

<sup>42</sup> The type and nature of this data will vary considerably between OES and it is the responsibility of individual OES to identify important data sources.

- NIST 800-82 R2 – Appendix G AC-4 Information Flow Enforcement, IA-1 Identification and Authentication Policy and Procedures, IA-5 Authenticator Management, IA-6 Authenticator Feedback, IA-7 Cryptographic Module Authentication, SC-28 Protection of Information at Rest
- IEC 62443-3-3 – Sections 5.7.2 & 11.5, SR 4.1 Information Confidentiality
- NIST 800-53 R4 – Appendix D: AU-9 Protection of Audit Information, CP-9 Information System Backup, MP-1 Media Protection Policy and Procedures, MP-4 Media Storage
- ISO 270019 – Section 10.1 NIST FIPS 140-2

B3.d – Mobile Data

<b>B3.d – Mobile Data</b>		
<p><i>You have protected data important to the operation of the essential function on mobile devices.</i></p>		
<b>Not achieved</b>	<b>Partially achieved</b>	<b>Achieved</b>
<b>At least one of the following statements is true</b>	<b>All of the following statements are true</b>	<b>All the following statements are true</b>
<p>You don't know which mobile devices may hold data important to the operation of the essential function.</p> <p>You allow data important to the operation of the essential function to be stored on devices not managed by your organisation, or to at least equivalent standard.</p> <p>Data on mobile devices is not technically secured, or only some is secured.</p>	<p>1. You know <u>which mobile devices hold data</u> important to the operation of the essential function.</p> <p>2. Data important to the operation of the essential function is only stored on mobile devices with at least equivalent security standard to your organisation.</p> <p>3. Data on mobile devices is <u>technically secured</u>.</p>	<p>4. <i>Mobile devices</i> that hold data that is important to the operation of the essential function are <i>catalogued</i>, are under your organisation's control and configured according to best practice for the platform, with appropriate technical and procedural policies in place.</p> <p>5. Your organisation can remotely wipe all mobile devices holding data important to the operation of essential function.</p> <p>6. You have minimised this data on these mobile devices. Some data may be automatically deleted off mobile devices after a certain period.</p>
<b>Ofgem DGE CAF Interpretation</b>		
	<p>Ofgem's interpretation is as follows:</p>	



<p>(Partially Achieved)</p> <p>IGP 1</p> <p>Information Asset Register</p>	<p>a) [<i>you know which mobile devices hold data</i>] you understand which mobile devices (e.g. laptops, removable media) host important data and you have records of these devices. Your records and management processes enable you to manage them through life and assure the data that they host.</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) an asset register, as detailed at Ofgem’s interpretation of IGP 1 of A3.a, which clearly identifies mobile devices.</p> <p>b) an Information Asset Register (IAR), as detailed at Ofgem’s interpretation of IGP 1, of B3.a., which clearly identifies when important information is being hosted on mobile devices.</p>
<p>(Partially Achieved)</p> <p>IGP 3 –</p> <p>Technically Secured</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [<i>technically secured</i>] You do not rely solely on people and processes to secure mobile devices. You have also implemented appropriate and proportionate technical measures to secure the data on your mobile devices. The technical measures employed will depend on the purpose for which the mobile device is employed and will need to be selected after risk assessment. Further guidance can be found at: <a href="#">Device Security Guidance - NCSC.GOV.UK</a></p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) A mobile device management policy covering all relevant mobile devices. This may amount to more than one policy if mobile devices are managed by separate departments (e.g. IT and OT teams).</p>


<p>(Achieved)</p> <p>IGP 4 –</p> <p>Mobile Data Assets</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [<i>mobile devices, catalogued</i>] you understand which mobile devices (e.g. laptops, removable media) host important data and you have records of these devices. Your records and management processes enable you to manage them through life and assure the data that they host.</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>b) an asset register, as detailed at Ofgem’s interpretation of IGP 1 of A3.a, which clearly identifies mobile devices.</p> <p>c) an Information Asset Register (IAR), as detailed at Ofgem’s interpretation of IGP 1, of B3.a., which clearly identifies when important information is being hosted on mobile devices.</p>
--	--

**References and Further Guidance**



- [B.3 Data security - NCSC.GOV.UK](#)
- IEC 62443 / ISA 99 3-3 – SR 2.3 Use Control for Portable and Mobile Devices
- ISO 27019 – Sections 6.2.1 & 10.1
- ISA 99 Part 4 Protection of data at rest
- NCSC End user device (EUD security guidance)
- NIST FIPS 140-2

B3.e – Media / Equipment Sanitisation

<b>B3.e – Media / Equipment Sanitisation</b>		
<p><i>You appropriately sanitise media and equipment holding data important to the operation of the essential function.</i></p>		
<b>Not achieved</b>	<b>Partially achieved</b>	<b>Achieved</b>
<b>At least one of the following statements is true</b>	<b>All of the following statements are true</b>	<b>All the following statements are true</b>
<p>Some or all devices, equipment or removable media that hold data important to the operation of the essential function are disposed of without sanitisation of that data.</p>	<p>1. Data important to the operation of the essential function is removed from all devices, equipment and removable media before reuse and / or disposal.</p>	<p>2. You catalogue and track all devices that contain data important to the operation of the essential function (whether a specific storage device or one with integral storage).</p> <p>3. All data important to the operation of the essential function is sanitised from all devices, equipment or removable media before reuse and / or disposal using an assured product or service.</p>
<b>Ofgem DGE CAF Interpretation</b>		
General	Ofgem does not have any DGE sector specific interpretation for this security outcome.	




## References and Further Guidance

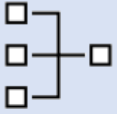


- [B.3 Data security - NCSC.GOV.UK](#)
- NIST SP800-53 R2 – Section 3.10, Media Protection, MP-6 Media Sanitization
- ISO 27019 – Section 8.3

## B4 System Security

B4 System Security		
<p><i>Network and information systems and technology critical for the operation of essential functions are protected from cyber-attack. An organisational understanding of risk to essential functions informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.</i></p>		
Related CAF Objective(s)	Ref	Contributing Outcome
B4 - System Security	B4.a	Secure by Design
	B4.b	Secure Configuration
	B4.c	Secure Management
	B4.d	Vulnerability Management

### B4.a – Secure by Design

B4.a – Secure by Design		
<p><i>You design security into the network and information systems that support the operation of essential functions. You minimise their attack surface and ensure that the operation of the essential function should not be impacted by the exploitation of any single vulnerability.</i></p>		
Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All the following statements are true

<p>Systems essential to the operation of the essential function are not appropriately segregated from other systems.</p> <p>Internet access is available from operational systems.</p> <p>Data flows between the essential function's operational systems and other systems are complex, making it hard to discriminate between legitimate and illegitimate/malicious traffic.</p> <p>Remote or third-party accesses circumvent some network controls to gain more direct access to operational systems of the essential function.</p>	<ol style="list-style-type: none"> <li>1. You employ appropriate expertise to design network and information systems</li> <li>2. You design <u>strong boundary defences where your networks and information systems interface with other organisations</u> or the world at large.</li> <li>3. You design <u>simple data flows</u> between your networks and information systems and any <u>external interface to enable effective monitoring</u>.</li> <li>4. You design to make network and information system recovery simple.</li> <li>5. All inputs to operational systems are checked and validated at the network boundary where possible, or additional monitoring is in place for content-based attacks.</li> </ol>	<ol style="list-style-type: none"> <li>6. You employ appropriate expertise to design network and information systems.</li> <li>7. Your networks and information systems are <u>segregated into appropriate security zones</u>, e.g. <u>operational systems</u> for the essential function are segregated in a highly trusted, more secure zone.</li> <li>8. The networks and information systems supporting your essential function are designed to have <u>simple data flows</u> between components <u>to support effective security monitoring</u>.</li> <li>9. The networks and information systems supporting your essential function are <u>designed to be easy to recover</u>.</li> <li>10. <u>Content-based attacks are mitigated for all inputs</u> to operational systems that affect the essential function (e.g. via transformation and inspection).</li> </ol>
--	---	--

## Ofgem DGE CAF Interpretation



<p>(Partially Achieved)</p> <p>IGP 2</p> <p>Boundary Defence Interface</p>	<p>Ofgem interprets this IGP as follows:</p> <ol style="list-style-type: none"> <li>a) [<i>strong boundary defences where your networks and information systems interface with other organisations</i>] you have clearly identified all of the points of interconnection between your network and information systems and external organisations/third parties. These points of interconnection are equipped with a method of validating message format and content.</li> </ol>
--	---

	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a. Network diagrams that show points of interconnection between network and information systems and external organisations/third parties.</li> </ul>
<p>(Partially Achieved)</p> <p>IGP 3</p> <p>Effective Monitoring</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a. [<i>simple data flows, to enable effective monitoring</i>] your data flows have been designed such that you are able to easily validate message format and content. Where necessary, you employ protocol breaks at network boundaries to transform data into the simplest format and perform validation of message format and content.</li> </ul> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) A set of Interface Control Documents (ICDs) for your in-scope systems that conform with the interpretation provided by Ofgem at IGP 12, B3a.</li> <li>b) a set of data flow diagrams (or similar) of sufficient detail to show data flows between network segments, and the means of validating message format and content.</li> <li>c) details of a logging and monitoring strategy that details how data flows between network segments are monitored and that conforms with the guidance provided at C1.a.</li> </ul>
<p>(Achieved)</p> <p>IGP 7</p>	<p>Ofgem interprets this IGP as follows:</p>

<p>Security Zones</p>	<p>a) [<i>segregated into appropriate security zones</i>] your network design is based around the segregation principle. You have grouped your services and systems into network segments that take account of their criticality. This approach corresponds with the concept of zones and conduits described in the IEC 62443 reference model. You have ensured that your OT networks, and any other systems that you have identified as being critical<sup>43</sup>, are segregated from your enterprise systems.</p> <p>b) [<i>operational systems</i>] the term operational systems is synonymous with Operational Technology (OT) and refers to any technology that interfaces with the physical world. It includes Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS). As OES in the DGE sector it is likely that much of your NIS scope will be classed as operational systems.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Network diagrams that clearly show all the OES' networks and information systems that are in-scope, the zones that they are part of and DMZs.</p> <p>b) Evidence that physical security zones map to network zones such that they are mutually supporting. Meaning that, wherever possible, the components of critical OT networks are afforded a level of physical security that exceeds that provided to less critical systems.</p>
<p>(Achieved)</p>	<p>Ofgem interprets this IGP as follows:</p>

<sup>43</sup> This does not preclude systems that are in NIS scope from being hosted on enterprise networks, so long as those systems and networks are appropriately and proportionately secured. However, it does require those OES who operate non-OT systems that they class as Critical National Infrastructure (CNI), such as the System Operators, to segregate according to criticality.

<p>IGP 8</p> <p>Simple Data Flows</p>	<p>a) [<i>simple data flows, support effective security monitoring</i>] your data flows have been designed such that you are able to easily validate message format and content. Where necessary, you employ protocol breaks at network boundaries to transform data into the simplest format and perform validation of message format and content.</p> <p>b) [<i>simple data flows, support effective security monitoring</i>] you have considered the risks associated with importing data from various sources and have applied boundary protection that is commensurate with the risk. For example, you have applied higher levels of boundary protection and monitoring to data that is being imported from outside of your organisation.</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) A set of Interface Control Documents (ICDs) for your in-scope systems that conform with the interpretation provided by Ofgem at IGP 12, B3a.</p> <p>b) a set of data flow diagrams (or similar) of sufficient detail to show data flows between network segments, and the means of validating message format and content.</p> <p>c) details of a logging and monitoring strategy that details how data flows between network segments are monitored and that conforms with the guidance provided at C1.a.</p>
<p>(Achieved)</p> <p>IGP 9</p> <p>Recovery</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a. [<i>designed to be easy to recover</i>] you have taken account of principle B5.</p>

<p>(Achieved)</p> <p>IGP 10</p> <p>Mitigation</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a. [<i>Content-based attacks are mitigated for all inputs</i>] you understand all of the possible paths/inputs by which data can be imported onto your networks and systems, these include network connections and removable media.</p> <p>You are aware that content-based attacks are likely to originate from less trusted networks (either outside of your organisation, or from less trusted network segments within your organisation) and, as a result, you have employed appropriate defensive measures at the boundaries of your network segments.</p> <p>You employ appropriate defensive techniques to reduce the likelihood of content-based attacks, these may include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• rapid patching</li> <li>• uni-directional flow control</li> <li>• use of a simple transfer protocol with a protocol break</li> <li>• message content verification</li> <li>• message transformation</li> </ul>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) a set of Interface Control Documents (ICDs) for your in-scope systems that conform with the interpretation provided by Ofgem at IGP 12, B3a.</p> <p>b) a set of data flow diagrams (or similar) of sufficient detail to show data flows between network segments and between systems, and the means of validating message format and content (where this has been applied).</p>


## References and Further Guidance



- [B.4 System security - NCSC.GOV.UK](#)
- [Pattern: Safely Importing Data - NCSC.GOV.UK](#)
- NIST 800-82 R2 – Appendix G: PL-7 Security Concept of Operations, PL-8 Information Security Architecture, SA-8 Security Engineering Principles, SA-17 Developer Security Architecture and Design
- IEC 62443-1-1 – Sections 5.2, 5.5, 5.9, 6.4, 6.5
- IEC 62443-3-3 – SR 5.2 Zone Boundary Protection
- NIST 800-53 R4 – Section 2.6, Appendix D: AU-9 Protection of Audit Information, CP-9 Information System Backup, MP-1 Media Protection Policy and Procedures, MP-4 Media Storage
- ISO 27001 – Sections 14.1 & 14.2



B4.b – Secure Configuration

<h2 style="margin: 0;">B4.b – Secure Configuration</h2>		
<p><i>You securely configure the network and information systems that support the operation of essential functions.</i></p>		
Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All the following statements are true
<p>You haven't identified the assets that need to be carefully configured to maintain the security of the essential function.</p> <p>Policies relating to the security of operating system builds or configuration are not applied consistently across your network and information systems relating to your essential function.</p> <p>Configuration details are not recorded or lack enough information to be able to rebuild the system or device.</p> <p>The recording of security changes or adjustments that effect your essential function is lacking or inconsistent.</p>	<ol style="list-style-type: none"> <li>1. You have identified and documented the <u>assets that need to be carefully configured</u> to maintain the security of the essential function.</li> <li>2. <u>Secure platform and device builds</u> are used across the estate.</li> <li>3. Consistent, secure and minimal system and device configurations are applied across the same types of environment.</li> <li>4. Changes and adjustments to security configuration at security boundaries with the networks and information systems supporting your essential function <u>are approved and documented.</u></li> <li>5. You verify software before installation is permitted.</li> </ol>	<ol style="list-style-type: none"> <li>6. You have identified, documented and <u>actively manage</u> (e.g. maintain security configurations, patching, updating according to good practice) the <u>assets that need to be carefully configured</u> to maintain the security of the essential function.</li> <li>7. <u>All platforms conform</u> to your secure, defined baseline build, or the latest known good configuration version for that environment.</li> <li>8. You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.</li> <li>9. You regularly review and validate that your network and information systems have the expected, secured settings and configuration.</li> <li>10. Only permitted software can be installed.</li> <li>11. Standard users are not able to change settings that would impact security or the business operation.</li> <li>12. If <u>automated decision-making technologies</u> are in use,</li> </ol>

		<p><u>their operation is well understood</u>, and decisions can be replicated.</p>
--	--	--

## Ofgem DGE CAF Interpretation




<p>(Partially Achieved)</p> <p>IGP 1</p> <p>Asset Configuration</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [<i>assets that need to be carefully configured</i>] assets include the in-scope systems themselves and the network devices that provide network functionality and security (e.g. switches, firewalls, VPN software, etc). Any assets that form part of a network boundary are prioritised.</p> <p>b) [<i>assets that need to be carefully configured</i>] your device management policies and processes take account of the risks associated with making changes in an OT environment.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) a configuration management and patching policy, with associated processes. These processes describe how:</p> <ul style="list-style-type: none"> <li>• a case of misconfiguration or out of date patching is identified.</li> <li>• tickets are raised to complete any re-configuration or patching that is required.</li> <li>• your configuration register/database is updated to reflect the completion of the tickets.</li> </ul> <p>b) a configuration management register/database that captures all configurable devices and their configuration status. This register/database may be a component your asset-register or may be a stand-alone document.</p>

	<p>c) documented baseline builds and build images.</p> <p>d) an asset register that conforms to Ofgem’s interpretation at IGP 1, A3.a.</p>
<p>(Partially Achieved)</p> <p>IGP 2</p> <p>Secure Platform and Device Builds</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [<i>secure platform and device builds</i>] you use well understood, consistent and secured baseline/gold builds across your environments. These builds are suitably hardened.</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) a configuration management register/database that captures all configurable devices and their configuration status. This register/database may be a component of your asset-register or may be a stand-alone document.</p>
<p>(Partially Achieved)</p> <p>IGP 4</p> <p>Configuration Management</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [<i>approved and documented</i>] you implement configuration management policies that govern configuration changes. Technical documentation of the networks and information systems is up to date.</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) a configuration management and patching policy, with associated processes. These processes describe how:</p> <ul style="list-style-type: none"> <li>• a case of misconfiguration or out of date patching is identified.</li> <li>• tickets are raised to complete any re-configuration or patching that is required.</li> <li>• Your configuration register/database is updated to reflect the completion of the tickets.</li> </ul> <p>b) a configuration management register/database that captures all configurable devices and their configuration status. This</p>

	<p>register/database may be a component your asset-register or may be a stand-alone document.</p>
<p>(Achieved)  IGP 6  Proactive Device Management</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [<i>actively manage</i>] You have documented policies and processes that describe how you manage device configuration. These policies and processes include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• baseline (‘gold’) builds for commonly used devices/platforms.</li> <li>• a means of ensuring that only permitted software is installed on devices.</li> <li>• maintenance of patch and configuration files</li> </ul> <p>You follow these processes and ensure that your assets are correctly configured and updated with the latest approved patches in a timely manner. Where it is not possible to update devices to the latest approved patch level (for reasons of down-time or safety) you:</p> <ul style="list-style-type: none"> <li>• maintain a register of missed patches (as part of configuration management register/database)</li> <li>• monitor the risks associated with lack of patching as part of your routine risk assessment updates</li> <li>• have a documented plan to install missing patches as soon as is reasonably practicable or,</li> <li>• adopt additional risk reduction measures to minimise any residual risk where patching cannot be carried out.</li> <li>• maintain a register of obsolete platforms/devices (as part of configuration management register/database).</li> </ul> <p>b) [<i>assets that need to be carefully configured</i>] assets include the in-scope systems themselves and the network devices that e.g. provide network functionality and security (e.g. switches, firewalls, VPN software, etc). Any assets that form part of a network boundary are prioritised.</p>

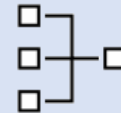
	<p>c) [<i>assets that need to be carefully configured</i>] your device management policies and processes take account of the risks associated with making changes in an OT environment.</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) a configuration management and patching policy, with associated processes. These processes describe how:</p> <ul style="list-style-type: none"> <li>• a case of misconfiguration or out of date patching is identified.</li> <li>• tickets are raised to complete any re-configuration or patching that is required.</li> <li>• your configuration register/database is updated to reflect the completion of the tickets.</li> </ul> <p>b) a configuration management register/database that captures all configurable devices and their configuration status. This register/database may be a component your asset-register or may be a stand-alone document.</p> <p>c) documented baseline builds and build images.</p> <p>d) an asset register that conforms to Ofgem’s interpretation at IGP 1, A3.a.</p>
<p>(Achieved)</p> <p>IGP 7</p> <p>Known Good Build</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [All platforms conform] all in scope network and information systems, and the wider network devices that provide network functionality and security are appropriately configuration managed.</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) An asset register that conforms to Ofgem’s interpretation at IGP 1, A3.a.</p>

	<p>b) A configuration management register/database that captures configurable devices and their configuration status. This register/database may be a component your asset-register or may be a stand-alone document.</p>
<p>(Achieved)</p> <p>IGP 12 -</p> <p>Automated Decision Making</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [<i>automated decision making, their operation is well understood</i>] you understand where you employ logic in your system and process controls (e.g. in PLCs and relays) and you understand the logic that is being implemented (i.e., the programs/logic). You would be able to detect if any malicious changes were made to these programs.</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Backups of all current ‘known good’ configurations of devices which includes the programs/OT ladder logic that is being implemented.</p>
<p><b>References and Further Guidance</b></p> <div style="text-align: right;">  </div>	
<ul style="list-style-type: none"> <li>• <a href="#">B.4 System security - NCSC.GOV.UK</a></li> <li>• NIST SP800-82 R2 – Sections 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9</li> <li>• NIST SP800-82 R2 – Appendix G: CM-2 Baseline Configuration, PL-7 Security Concept of Operations, PL-8 Information Security Architecture, SA-8 Security Engineering Principles,</li> <li>• IEC 62443 / ISA99 3-3 – SR 7.6 Network and Security Configuration Settings, SR 7.7 Least Functionality</li> </ul>	

*B4.c – Secure Management*

**B4.c – Secure Management**

*You manage your organisation's network and information systems that support the operation of essential functions to enable and maintain security.*



Not achieved	Partially achieved	Achieved
<b>At least one of the following statements is true</b>	<b>All of the following statements are true</b>	<b>All the following statements are true</b>
<p>Essential function networks and systems are administered or maintained using non-dedicated devices.</p> <p>You do not have good or current technical documentation of your networks and information systems.</p>	<p>1. Your systems and devices supporting the operation of the essential function are only administered or maintained by authorised privileged users from dedicated devices.</p> <p>2. Technical knowledge about networks and information systems, such as documentation and network diagrams, is regularly reviewed and updated.</p> <p>3. You prevent, detect and remove malware or unauthorised software. You use technical, procedural and physical measures as necessary.</p>	<p>4. Your systems and devices supporting the operation of the essential function are only administered or maintained by authorised privileged users from dedicated devices that are technically segregated and secured to the same level as the networks and systems being maintained.</p> <p>5. You regularly review and update technical knowledge about networks and information systems, such as documentation and network diagrams, and ensure they are securely stored.</p> <p>6. You prevent, detect and remove malware or unauthorised software. You use technical, procedural and physical measures as necessary.</p>

**Ofgem DGE CAF Interpretation**



Ofgem does not have any DGE sector specific interpretation for this security outcome.

## References and Further Guidance



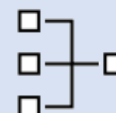
- [B.4 System security - NCSC.GOV.UK](#)
- NIST SP800-82 R2 – Section 6.2.5
- NIST 800-53 R4 – Appendix D: AC-5 Separation of Duties, SC-1 System and Communications Protection Policy and Procedures, SC-3 Security Function Isolation, MA-1 System Maintenance Policy, and Procedures
- ISO27001 – Sections 12.1.2, 14.2.2



B4.d – Vulnerability Management

## B4.d – Vulnerability Management

*You manage known vulnerabilities in your network and information systems to prevent adverse impact on the essential function.*



Not achieved	Partially achieved	Achieved
<b>At least one of the following statements is true</b>	<b>All of the following statements are true</b>	<b>All the following statements are true</b>
<p>You do not understand the exposure of your essential function to publicly known vulnerabilities.</p> <p>You do not mitigate externally exposed vulnerabilities promptly.</p> <p>You have not recently tested to verify your understanding of the vulnerabilities of the networks and information systems that support your essential function.</p> <p>You have not suitably mitigated systems or software that is no longer supported.</p> <p>You are not pursuing replacement for unsupported systems or software.</p>	<ol style="list-style-type: none"> <li>1. You <u>maintain a current understanding of the exposure</u> of your essential function to publicly known vulnerabilities.</li> <li>2. Announced vulnerabilities for all software packages, network equipment and operating systems used to support your essential function are tracked, <u>prioritised</u> and externally exposed vulnerabilities are mitigated (e.g. by patching) promptly.</li> <li>3. Some vulnerabilities that are not externally exposed have <u>temporary mitigations</u> for an extended period.</li> <li>4. You have temporary mitigations for unsupported systems and software while <u>pursuing migration to supported technology</u>.</li> <li>5. You <u>regularly test</u> to fully understand the vulnerabilities of the networks and information systems that support the operation of your essential function.</li> </ol>	<ol style="list-style-type: none"> <li>6. You maintain a current understanding of the exposure of your essential function to publicly known vulnerabilities.</li> <li>7. Announced vulnerabilities for all software packages, network equipment and operating systems used to support the operation of your essential function are tracked, prioritised and mitigated (e.g. by patching) promptly.</li> <li>8. You regularly test to fully understand the vulnerabilities of the networks and information systems that support the operation of your essential function and verify this understanding with third-party testing.</li> <li>9. You maximise the use of supported software, firmware and hardware in your networks and information systems supporting your essential function.</li> </ol>

## Ofgem DGE CAF Interpretation



<p>(Partially achieved)</p> <p>IGP 1</p> <p>Understanding Vulnerabilities</p>	<p>Ofgem’s interpretation is as follow:</p> <p>a) [<i>maintain a current understanding of the exposure</i>] you have a process of identifying known vulnerabilities for your network and information systems. You use all a range of sources including subscribing to vendor security notices, monitoring threat intelligence sources and websites hosting common vulnerabilities and exposures data. You are able to quickly identify the network and information systems that are affected by these vulnerabilities and exposures.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Your configuration management registers/databases are being regularly updated with applicable vulnerabilities and exposures (i.e., those that affect your network and information systems).</p> <p>b) Your configuration management registers/databases are built such that you can use filters to identify the networks and information systems that may be exposed to new vulnerabilities (meaning you can filter for all platforms that are running particular specific software versions).</p> <p>c) Your configuration management registers/databases contain details of networks and information systems that remain exposed to vulnerabilities and provide details of any compensating controls/temporary mitigations that you have implemented.</p>
<p>(Partially Achieved)</p>	<p>Ofgem’s interpretation is as follows:</p>

<p>IGP 2</p> <p>Awareness and Prioritisation</p>	<p>a) [<i>prioritised</i>] The means by which you record vulnerabilities allow you to prioritise them according to risk. You use this prioritised vulnerability data to inform your risk management process and your system management and patching process.</p> <p>b) [<i>externally exposed</i>] You do not accept temporary mitigations and/or risk acceptance to vulnerabilities and exposures that are exposed to the OT/IT network boundary, or the IT/internet boundary. All such vulnerabilities and exposures at your network boundaries are patched in accordance with targets stipulated in your patching policy.</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) your configuration management registers/databases are built such that you can use filters to identify which assets are exposed to external network segments. Your records show that all such devices are fully patched.</p>
<p>(Partially Achieved)</p> <p>IGP 3</p> <p>Temporary mitigations</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [<i>temporary mitigations</i>] you understand which of your assets cannot be patched to remove vulnerabilities and, where they remain in use, you have made a risk-based decision to do so. Your risk-based decision has taken account of the criticality of the system and any temporary mitigations that are in place. The residual risk is being owned at the appropriate level. (Note: this does not apply to devices exposed to external network segments).</p> <p>b) [<i>temporary mitigations</i>] the mitigations chosen will depend on circumstances, however they may include further network segregation and/or measures to ensure that the vulnerable system only receives trusted data. In circumstances where the risk is demonstrably low it may be reasonable to accept rather than mitigate/treat the residual risk.</p>

	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) your configuration management registers/databases contain details of networks and information systems that remain exposed to vulnerabilities and provide details of any compensating controls/temporary mitigations that you have implemented.</li> </ul>
<p>(Partially Achieved)</p> <p>IGP 4 –  Migration</p>	<p>Ofgem’s interpretation is as follows:</p> <ul style="list-style-type: none"> <li>a) [<i>pursuing migration to supported technology</i>] You understand how long you are likely to continue to carry the risk of unsupported systems and your security improvement plan identifies when the unsupported technology will be replaced.</li> </ul> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) A security improvement plan detailing the improvement activity that will provide a full mitigation for the identified vulnerabilities.</li> </ul>
<p>(Partially Achieved)</p> <p>IGP 5 –  Migration</p>	<p>Ofgem’s interpretation is as follows:</p> <ul style="list-style-type: none"> <li>a) [<i>regularly test</i>] You undertake scheduled (planned and periodic) test activity for your IT and OT environments. Test activity includes penetration testing and vulnerability scans. You schedule your testing according to risk and you prioritise your networks’ boundary devices.</li> </ul> <p>Your approach to OT testing takes account of the risk of testing in a live environment and you have considered approaches such as testing your baseline builds/gold builds in a lab environment.</p>

Where appropriate, Ofgem would expect the following evidence of good practice:

- a) A security testing policy that details how you test IT and OT environments. This policy will describe how you intend to use internal and/or third-party resources to conduct testing and will define the scope of tests and the interval at which they occur.
- b) Copies of all test results from the point at which your security testing policy was introduced.

## References and Further Guidance



- [B.4 System security - NCSC.GOV.UK](#)
- References and Further Guidance:
- NIST SP 800-82 R2 – CA-8 Penetration Testing, RA-5 Vulnerability Scanning, SI-7 Software, Firmware, and Information Integrity
- ISO 27019 – Section 12.6
- NCSC – “Vulnerability Management” from guidance repository

## B5 Resilient networks and systems

### B5 Resilient Networks and Systems

*The organisation builds resilience against cyber-attack and system failure into the design, implementation, operation, and management of systems that support the operation of essential functions.*

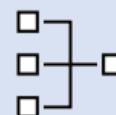


Related CAF Objective(s)	Ref	Contributing Outcome
B5 - Resilient Networks and Systems	B5.a	Resilience Preparation
	B5.b	Design for Resilience
	B5.c	Backups

#### B5.a – Resilience Preparation

### B5.a – Resilience Preparation

*You are prepared to restore the operation of your essential function following adverse impact.*



Not achieved	Partially achieved	Achieved
<b>At least one of the following statements is true</b>	<b>All of the following statements are true</b>	<b>All the following statements are true</b>
<p>You have limited understanding of all the elements that are required to restore operation of the essential function.</p> <p>You have not completed business continuity and / or disaster recovery plans for your essential function's networks, information systems and their dependencies.</p>	<p>1. You know all networks, information systems and underlying technologies that are necessary to restore the operation of the essential function; and understand their interdependence.</p> <p>2. You know the order in which systems need to be recovered to efficiently and effectively restore</p>	<p>3. You have business continuity and disaster recovery plans that have been tested for practicality, effectiveness and completeness. Appropriate use is made of different test methods, e.g. manual fail-over, table-top exercises, or red-teaming.</p> <p>4. You use your security awareness and threat</p>

<p>You have not fully assessed the practical implementation of your disaster recovery plans.</p>	<p>the operation of the essential function.</p>	<p>intelligence sources, to make immediate and potentially temporary security changes in response to new threats, e.g. a widespread outbreak of very damaging malware.</p>
--	---	--

### Ofgem DGE CAF Interpretation



<p>General</p>	<p>Ofgem does not have a DGE sector specific interpretation for this security outcome.</p>
----------------	--

### References and Further Guidance



- [B.5 Resilient networks and systems - NCSC.GOV.UK](#)
- NIST 800-82 R2 – Section 6.2.6, Appendix G: CM-8 Information System Component Inventory, CP-1 Contingency Planning Policy and Procedures, CP-2 Contingency Plan, CP-4 Contingency Plan Testing, CP-10 Information System Recovery and Reconstitution
- IEC 62443 / ISA99 2-1 – Section A.3.4.3.8
- IEC 62443-3-3 – SR 7.3 Control System Backup, SR 7.4 Control System Recovery and Reconstitution, SR 7.5 Emergency Power, SR 7.8 Control System Component Inventory
- ISO 27001 – Sections 17.1, 17.2
- NIST 800-82 R2 – Appendix G: PL-7 Security Concept of Operations, PL-8 Information Security Architecture, SA-8 Security Engineering Principles, SA-17 Developer Security Architecture and Design
- IEC 62443-1-1 – Sections 5.2, 5.5, 5.9, 6.4, 6.5
- IEC 62443-3-3 – SR 5.2 Zone Boundary Protection
- NIST 800-53 R4 – Section 2.6, Appendix D: AU-9 Protection of Audit Information, CP-9 Information System Backup, MP-1 Media Protection Policy and Procedures, MP-4 Media Storage
- ISO 27001 – Sections 14.1 & 14.2

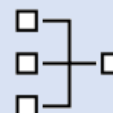
- NCSC Cyber security design principles
- NCSC 6 security architecture 'anti-patterns'



B5.b – Design for Resilience

**B5.b – Design for Resilience**

*You design the network and information systems supporting your essential function to be resilient to cyber security incidents. Systems are appropriately segregated, and resource limitations are mitigated.*



Not achieved	Partially achieved	Achieved
<p><b>At least one of the following statements is true</b></p>	<p><b>All of the following statements are true</b></p>	<p><b>All the following statements are true</b></p>
<p>Operational networks and systems are not appropriately segregated.</p> <p>Internet services, such as browsing and email, are accessible from essential operational systems supporting the essential function.</p> <p>You do not understand or lack plans to mitigate all resource limitations that could adversely affect your essential function.</p>	<p>1. <u>Operational systems</u> that support the operation of the essential function are <u>logically separated from your business systems</u>, e.g. they reside on the same network as the rest of the organisation, but within a DMZ. Internet access is not available from operational systems.</p> <p>2. <u>Resource limitations</u> (e.g. network bandwidth, single network paths) have been identified but not fully mitigated.</p>	<p>3. Operational systems that support the operation of the essential function are segregated from other business and external systems by appropriate technical and physical means, e.g. separate network and system infrastructure with independent user administration. Internet services are not accessible from operational systems.</p> <p>4. You have identified and mitigated all resource limitations, e.g. bandwidth limitations and single network paths.</p> <p>5. You have identified and mitigated any geographical constraints or weaknesses. (e.g. systems that your essential function depends upon are replicated in another location, important network connectivity has alternative physical paths and service providers).</p> <p>6. You review and update assessments of dependencies, resource and geographical limitations and mitigation's when necessary.</p>

## Ofgem DGE CAF Interpretation



<p>(Partially Achieved)</p> <p>IGP 1</p> <p>Network Architecture</p>	<p>Ofgem’s interpretation is as per IGP 2 of B4.a follows:</p> <p>a) [<i>operational systems</i>] the term operational system is synonymous with Operational Technology (OT) and refers to any technology that interfaces with the physical world. It includes Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS). As OES in the DGE sector it is likely that much of your NIS scope will be classed as operational systems.</p> <p>b) [<i>logically separated from your business systems</i>] your network design is based around the segregation principle. You have grouped your services and systems into network segments that take account of their criticality. This approach corresponds with the concept of zones and conduits described in the IEC 62443 reference model. You have ensured that your OT networks, and any other systems that you have identified as being critical<sup>44</sup>, are segregated from your enterprise systems.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Network diagrams that clearly show all the OES’ networks and information systems that are in-scope, the zones that they are part of, and DMZs.</p>
	<p>Ofgem’s interpretation is as follows:</p>

<sup>44</sup> This does not preclude systems that are in NIS scope from being hosted on enterprise networks, so long as those systems and networks are appropriately and proportionately secured. However, it does require those OES who operate non-OT systems that they class as Critical National Infrastructure (CNI), such as the System Operators, to segregate according to criticality.


(Partially Achieved)  IGP 2  Resource limitations	a) You have analysed your network infrastructure and identified single points of failure and choke points. You are planning upgrades to resolve these issues where the risk they pose exceeds your risk appetite.
	Where appropriate, Ofgem would expect the following evidence of good practice:  a) Entries in risk registers where lack of network and information system resilience presents a risk to the essential service in the event of a loss of connectivity.

## References and Further Guidance



- [B.5 Resilient networks and systems - NCSC.GOV.UK](#)
- NIST SP800-82 R2 – Sections 5.1, 5.5, 5.13
- IEC 62443 / ISA99 3-3 – Section 7.1
- IEC 62443-3-3 - Section 9.1
- ISO 27019 – Section 13.1.3

B5.c – Backups

<h2 style="margin: 0;">B5.c – Backups</h2>		
<p><i>You hold accessible and secured current backups of data and information needed to recover operation of your essential function.</i></p>		
Not achieved	Partially achieved	Achieved
<b>At least one of the following statements is true</b>	<b>All of the following statements are true</b>	<b>All the following statements are true</b>
<p>Backup coverage is incomplete and does not include all relevant data and information needed to restore the operation of your essential function.</p> <p>Backups are not frequent enough for the operation of your essential function to be restored within a suitable timeframe.</p>	<p>1. You have <u>appropriately secured backups</u> (including data, configuration information, software, equipment, processes and knowledge). These backups will be accessible to recover from an extreme event.</p> <p>2. You <u>routinely test backups</u> to ensure that the backup process functions correctly and the backups are usable.</p>	<p>3. Your <u>comprehensive, automatic and tested</u> technical and procedural backups are secured at centrally accessible or secondary sites to recover from an extreme event.</p> <p>4. Backups of all important data and information needed to recover the essential function; are made, <u>tested, documented and routinely reviewed</u>.</p>
<h3 style="margin: 0;">Ofgem DGE CAF Interpretation</h3>		
<p>(Partially Achieved)</p> <p>IGP 1</p> <p>Secured Backups</p>	<p>Ofgem’s interpretation is as follows:</p> <p style="margin-left: 20px;">a. [<i>appropriately secured backups</i>] you maintain a set of backups that are secured off-line.</p>	
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p>	

	<p>a. A back-up policy detailing processes for the OT and enterprise environments.</p>
<p>(Partially Achieved)</p> <p>IGP 2</p> <p>Testing Backups</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a. [routinely test backups] You follow a documented process for confirming that your set of backups is complete and that you are able to efficiently use these backups to restore your systems.</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Records of back-up activity.</p> <p>b) Records of back-up testing activity.</p>
<p>(Achieved)</p> <p>IGP 3 &amp; 4 – Backup Policy</p>	<p>Ofgem’s interpretation is as follows:</p> <p>a) [<i>comprehensive, automatic and tested</i>] Your backup policy details how backups of all of the software, configurations, data and other relevant information for your network and information systems are maintained.</p> <p>You have employed automatic backup procedures wherever it is appropriate and safe to do so. In cases where it is not appropriate or safe it would be acceptable for back-ups to be taken manually after configuration changes have been made. The creation of back-ups should be part of your engineering change management process and scheduled through any computerised maintenance management system (CMMS) established for work scheduling.</p> <p>b) [<i>tested, documented and routinely reviewed</i>] You follow a documented process for confirming that your set of backups is complete and that you are able to efficiently use these backups to restore your systems.</p>


	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"><li>a) a back-up policy detailing processes for the OT and enterprise environments.</li><li>b) records of back-up activity.</li><li>c) records of back-up testing activity.</li></ul>
--	---

## References and Further Guidance

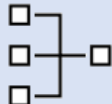


- [B.5 Resilient networks and systems - NCSC.GOV.UK](#)
- NIST 800-82 R2 – CP-9 Information System Backup, CP-10 - Information System Recovery and Reconstitution, CM-8 - Information System Component Inventory
- IEC 62443-3-3 – SR 7.3, Control System Backup, SR 7.4 Control System Recovery and Reconstitution
- ISO/IEC 27001 – Sections A.10.5, A.14.1
- ISO/IEC 27019 – Section 12.3

## B6 Staff awareness and training

B6 Staff awareness and training		
<p><i>Staff have appropriate awareness, knowledge, and skills to carry out their organisational roles effectively in relation to the security of network and information systems supporting the operation of essential functions.</i></p>		
Related CAF Objective(s)	Ref	Contributing Outcome
B6 – Staff Awareness and Training	B6.a	Cyber Security Culture
	B6.b	Cyber Security Training

### B6.a – Cyber Security Culture

B6.a – Cyber Security Culture		
<p><i>You develop and pursue a positive cyber security culture.</i></p>		
Not achieved	Partially achieved	Achieved
<p><b>At least one of the following statements is true</b></p>	<p><b>All of the following statements are true</b></p>	<p><b>All the following statements are true</b></p>
<p>People in your organisation don't understand what they contribute to the cyber security of the essential function.</p> <p>People in your organisation don't know how to raise a concern about cyber security.</p> <p>People believe that reporting issues may get them into trouble.</p>	<p>1. Your executive management understand and widely communicate the importance of a positive cyber security culture. Positive attitudes, behaviours and expectations are described for your organisation.</p> <p>2. All people in your organisation understand the contribution they</p>	<p>4. Your executive management clearly and effectively communicates the organisation's cyber security priorities and objectives to all staff. Your organisation displays positive cyber security attitudes, behaviours and expectations.</p>

<p>Your organisation's approach to cyber security is perceived by staff as hindering the business of the organisation.</p>	<p>make to the essential function's cyber security.</p> <p>3. All individuals in your organisation know who to contact and where to access more information about cyber security. They know how to raise a cyber security issue.</p>	<p>5. People in your organisation raising potential cyber security incidents and issues are treated positively.</p> <p>6. Individuals at all levels in your organisation routinely report concerns or issues about cyber security and are recognised for their contribution to keeping the organisation secure.</p> <p>7. Your management is seen to be committed to and actively involved in cyber security.</p> <p>8. Your organisation communicates openly about cyber security, with any concern being taken seriously.</p> <p>9. People across your organisation participate in cyber security activities and improvements, building joint ownership and bringing knowledge of their area of expertise.</p>
--	--	--

**Ofgem DGE CAF Interpretation**



<p>General</p>	<p>Ofgem does not have any DGE sector specific interpretation for this security outcome.</p>
----------------	--

**References and Further Guidance**



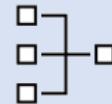
- NIST SP800-82 R2 – Section 6.2.2
- ISO 27001 – Clause 7
- ISO 27019 – Section 7.2.2
- NCSC Growing positive security cultures
- CPNI SeCuRE 4 Assessing security culture



*B6.b – Cyber Security Training*

**B6.b – Cyber Security Training**

*The people who support the operation of your essential function are appropriately trained in cyber security. A range of approaches to cyber security training, awareness and communications are employed.*



Not achieved	Partially achieved	Achieved
<b>At least one of the following statements is true</b>	<b>All of the following statements are true</b>	<b>All the following statements are true</b>
<p>There are teams who operate and support your essential function that lack any cyber security training.</p> <p>Cyber security training is restricted to specific roles in your organisation.</p> <p>Cyber security training records for your organisation are lacking or incomplete.</p>	<ol style="list-style-type: none"> <li>1. You have defined appropriate cyber security training and awareness activities for all roles in your organisation, from executives to the most junior roles.</li> <li>2. You use a range of teaching and communication techniques for cyber security training and awareness to reach the widest audience effectively.</li> <li>3. Cyber security information is easily available.</li> </ol>	<ol style="list-style-type: none"> <li>4. All people in your organisation, from the most senior to the most junior, follow appropriate cyber security training paths.</li> <li>5. Each individual's cyber security training is tracked and refreshed at suitable intervals.</li> <li>6. You routinely evaluate your cyber security training and awareness activities to ensure they reach the widest audience and are effective.</li> <li>7. You make cyber security information and good practice guidance easily accessible, widely available and you know it is referenced and used within your organisation.</li> </ol>

## Ofgem DGE CAF Interpretation



General

Ofgem does not have any DGE sector specific interpretation for this security outcome.

Where appropriate, Ofgem would expect the following evidence of good practice:

- a) Details of all cyber security training provided by your organisation. Ideally this would take the form of an organisational cyber security training plan.
- b) Records of completed training.

## References and Further Guidance




- NIST SP800-82 R2 – Section 6.2.2
- ISO 27019 – Section 7.2.2

# Objective C – Detecting cyber security events


## Annex B.3 - Objective C. Detecting cyber security events

Capabilities exist to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential functions.

### C1 Security monitoring

C1 Security Monitoring		
<p>The organisation monitors the security status of the networks and systems supporting the operation of essential functions to detect potential security problems and to track the ongoing effectiveness of protective security measures.</p>		
Related CAF Objective(s)	Ref	Contributing Outcome
C1 – Security Monitoring	C1.a	Monitoring Coverage
	C1.b	Securing Logs
	C1.c	Generating Alerts
	C1.d	Identifying Security Incidents
	C1.e	Monitoring Tools and Skills

#### C1.a – Monitoring Coverage

C1.a - Monitoring Coverage	
<p>The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function.</p>	

Not achieved	Partially achieved	Achieved
<p><b>At least one of the following statements is true</b></p>	<p><b>All of the following statements are true</b></p>	<p><b>All the following statements are true</b></p>
<p>Data relating to the security and operation of your essential functions is not collected.</p> <p>You do not confidently detect the presence or absence of Indicators of Compromise (IoCs) on your essential functions, such as known malicious command and control signatures (e.g. because applying the indicator is difficult or your logging data is not sufficiently detailed).</p> <p>You are not able to audit the activities of users in relation to your essential function.</p> <p>You do not capture any traffic crossing your network boundary including as a minimum IP connections.</p>	<p>1. <u>Data</u> relating to the security and operation of some areas of your essential functions is collected but coverage is <u>not comprehensive</u>.</p> <p>2. You easily detect the <u>presence or absence of IoCs</u> on your essential function, such as known malicious command and control signatures.</p> <p>3. Some user monitoring is done, but not covering a fully <u>agreed list</u> of <u>suspicious or undesirable behaviour</u>.</p> <p>4. You <u>monitor</u> traffic crossing your <u>network boundary</u> (including IP address connections as a minimum).</p>	<p>5. Monitoring is based on an <u>understanding</u> of your networks, common <u>cyber-attack methods</u> and what you need <u>awareness of</u> in order to <u>detect</u> potential security incidents that could <u>affect the operation</u> of your essential function (e.g. presence of malware, malicious emails, user policy violations).</p> <p>6. Your <u>monitoring data</u> provides enough <u>detail</u> to <u>reliably detect security incidents</u> that could affect the operation of your essential function.</p> <p>7. You easily detect the <u>presence or absence of IoCs</u> on your essential functions, such as known malicious command and control signatures.</p> <p>8. Extensive monitoring of <u>user activity</u> in relation to the operation of essential functions enables you to detect policy violations and an agreed list of suspicious or undesirable behaviour.</p> <p>9. You have <u>extensive</u> monitoring coverage that includes <u>host-based monitoring</u> and <u>network gateways</u>.</p> <p>10. All <u>new systems</u> are considered as potential monitoring data sources to <u>maintain a comprehensive monitoring capability</u>.</p>

**Ofgem DGE CAF Interpretation**



Ofgem interprets this IGP as follows:

<p>(Partially Achieved)</p> <p>IGP 1</p> <p>Monitoring Coverage</p>	<p>a) In contrast to the practices detailed against IGP 9, monitoring requirements and capability, while understood and prioritised, is [not comprehensive] and information relating to network security status omits some lower priority data.</p> <hr/> <p>Ofgem would expect to see the following evidence of good practice as follows relating to monitoring coverage:</p> <p>a) See evidence of good practice detailed against IGPs 5-10.</p> <p>b) Monitoring strategy programme of improvement prioritises integration of data sources into your monitoring programme, which is time bound and actively being managed. Resulting in a well communicated and clearly defined (prioritised) work programme for onward development of capability for monitoring coverage in line with risk assessment requirements.</p>
<p>(Partially Achieved)</p> <p>IGP 3</p> <p>User Monitoring</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) You should understand user behaviours and the impact they may have on the systems they interact with carrying out business as usual activities to provide your essential service.</p> <p>b) You differentiate between legitimate user activities required to carry out essential tasks and those behaviours that are suspicious or undesirable requires an understanding of required activity relating to users and their defined roles and responsibilities.</p> <p>c) You should use this understanding to develop an agreed list (prioritised) within your monitoring regime to identify [suspicious or undesirable behaviour] when it occurs, prioritising monitoring of privileges users who have greater ability to impact your essential service, raising alerts when necessary (see C1.c).</p> <p>Examples may include, but are not limited to:</p> <ul style="list-style-type: none"> <li>Monitoring for configuration changes to programmable systems e.g. safety related systems.</li> </ul>

	<ul style="list-style-type: none"> <li>• addition or removal of applications and system services from operating systems.</li> <li>• changes to important system files and data records</li> <li>• attempted escalation of privileges and or attempted unauthorised use of resources.</li> </ul> <p>(See IGP 8 for further detail)</p> <p>d) When assessing your capability against the indicative use case above for user monitoring and the requirements outlined in IGP 8 your monitoring of user activity has yet to extend to cover suspicious or undesirable behaviour.</p>
	<p>Ofgem would expect to see the following evidence of good practice as follows:</p> <ul style="list-style-type: none"> <li>a. Examples of analysis (or requirements gathering) undertaken against known and well-understood attacks have been completed (see C1.d) to derive monitoring techniques for suspicious or undesirable behaviours. This analysis has led to the creation of requirements ([agreed list]) which are captured and used to shape your monitoring programme.</li> <li>b. You have baselined your systems such that understanding of normal behaviour has been gained and this is then used in conjunction with understanding of TTPs to establish detection capabilities and identify and assess deviations from baseline (see C2) in accordance with your requirements ([agreed list]).</li> <li>c. These aspects above should be available within lifecycle documentation created to support the design and implementation of your monitoring capability.</li> <li>d. See evidence of good practice detailed against IGPs 5-10.</li> </ul>
	<p>Ofgem interprets this IGP as follows:</p>

<p>(Partially Achieved)</p> <p>IGP 4</p> <p>Network Boundaries</p>	<p>a. Within your security design NIS assets should be segregated and segmented from less critical assets applying secure design principles outlined in objective B (protecting against cyber-attacks) to implement a secure architecture that reduces the number of defined access and egress points creating network gateways and choke points on your network which are actively monitored to understand traffic flows across your network boundaries.</p> <p>b. Important gateways and network interfaces include but are not limited to:</p> <ul style="list-style-type: none"> <li>• connections between your network and the Internet</li> <li>• connections between zones in OT (Operational Technology) and IT networks</li> <li>• external gateways to third party networks.</li> </ul> <p>Monitoring of IP traffic should include capture of 5-tuple metadata from critical zone boundaries such as the IT/OT interface.</p> <hr/> <p>Ofgem would expect to see the following evidence of good practice:</p> <p>a. See evidence of good practice detailed against IGPs 5-10.</p>
<p>(Achieved)</p> <p>IGP 5</p> <p>Informed Monitoring Strategy</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) You should apply learning gained during risk assessment (see A2) about the probable events that could impact on the correct operation of their network and information systems, intentional or otherwise, to devise appropriate and proportional defensive architectural controls (see CAF objective B). Seeking to minimise the likelihood of disruption or loss.</p> <p>[Understanding] of Networks and Assets</p> <p>b) You should establish and maintain a security monitoring programme that defines the operators logging and monitoring</p>



	<p>requirements. At a minimum, addressing the collection, review, and retention of audit logs for IT assets. And where practical to do so for OT assets similarly. Any programme should address requirements for suitable qualified and experienced personnel (see C1.e) as a key component to support the activity from design and capture through to action “in the event of”. Covering people, processes and systems holistically.</p> <p>c) Once established you should ensure that the programme is regularly reviewed and update lifecycle documentation routinely (at least annually), or when significant changes occur that could impact this control.</p> <p>[Detecting] potential cyber incidents through Situational Awareness</p> <p>d) Implementing a successful security monitoring programme requires organisations to establish and maintain activities and technologies to collect, analyse, prioritise, alarm and present actionable intelligence to responsible persons within the organisation. Enabling reporting on the overall health of networks and information systems that may [could affect operation]. Identifying potential risks to their continued availability or performance.</p> <p>This situational awareness can support organisations to proactively respond to security events, minimising the potential for disruptive incidents (see objective D) resulting in actual impacts on overall availability or performance of any essential functions provided.</p> <p>e) Enabling appropriate response in the event that disruption occurs thereby supporting any response and restorative activities necessary to reinstate operational effectiveness and maintain business continuity.</p> <p>Situational [awareness] has four main objectives:</p> <ul style="list-style-type: none"><li>• Perform Logging</li><li>• Perform Monitoring</li><li>• Establish and maintain a common operating picture</li><li>• Management Activities to act.</li></ul>
--	---

	<p>f) The organisation should develop, document, and maintain a strategy for monitoring, which should cover, but not be limited to:</p> <ul style="list-style-type: none"><li>• Monitoring objectives</li><li>• Scope</li><li>• Rationale</li><li>• Event logging approach and requirements</li><li>• Event analysis approach and requirements</li><li>• Approach to aligning threat intelligence with monitoring</li><li>• Approach to aligning incident response with monitoring</li><li>• Approach to aligning vulnerability management with monitoring.</li></ul> <p>g) Building situational awareness requires the application of a cohesive monitoring strategy which defines the objectives and requirements for monitoring, the content of which is informed by a detailed understanding of both network architecture, and components.</p> <p>h) Use of common techniques, tactics and procedures [cyber-attack methods] used to gain access to and exploit vulnerabilities within an environment should be inbuilt into detection capabilities.</p> <p>For example through adoption of a framework such as MITRE or similar approach to understand coverage required. In doing so a clear prioritisation order for monitoring can defined based on system vulnerability (see vulnerability management) and the overall criticality of components within the individual networks and information systems supporting your essential function is made. Enabling deployment of monitoring to detect such activities.</p> <p>i) Monitoring provides an additional layer of defence to work alongside these control measures, in part to audit their effectiveness and supporting assurance activities. As well as flagging any unwanted activity based on observable techniques, tactics and procedures, indicators of compromise, behavioural indicators or other detectable events that may represent an increased risk to the operating environment.</p> <p>Unlike vulnerability assessment however, which looks to identify and manage ongoing flaws or weakness within the design of</p>
--	---

	<p>network and information systems, detection is specifically looking for signs of vulnerability exploit or a worsening of the vulnerability situation through intentional or accidental activity across the assets base.</p> <p>j) While a major focus of CAF objective C is the detection of cyber security events, the security of network and information systems covers security in general which may include non-cyber related incidents. Any monitoring programme devised should extend to general health and availability of network and information system assets and supporting infrastructure, for example combining the following to support the essential service provided: -</p> <ul style="list-style-type: none"> <li>• UPS availability</li> <li>• emergency power supplies failover systems</li> <li>• fire detection and suppression systems for server rooms</li> <li>• HVAC</li> <li>• condition of spares</li> <li>• Access control systems</li> <li>• Maintenance laptops and portable programming devices</li> <li>• Functioning of physical security controls.</li> </ul>
	<p>Ofgem would expect to see the following evidence of good practice as follows.</p> <p>a) Development and maintenance of lifecycle documentation to detail the organisational aims and objectives for monitoring across critical network and information systems.</p> <p>b) Production of detailed technical design documents covering functional requirements for monitoring activities and their application.</p> <p>c) Detailed network architecture overlays to document and visualise data collection capabilities and coverage of logging and monitoring programme.</p>

	<p>d) Discovery and consideration of assessment in coverage against common TTPs detailed within recognised frameworks e.g. MITRE attack framework.</p> <p>e) Demonstration of maintenance activities to sustain monitoring programmes e.g. application of change control or programme enhancements and version control.</p> <p>f) Performing of documented internal review and audit of any security monitoring programme established.</p> <p>g) Demonstrable evidence of referential linking to vulnerability management studies / threat intelligence gathering activities and reporting.</p>
<p>(Achieved)</p> <p>IGP 6</p> <p>Detection Capabilities</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) The use case and technical requirements for monitoring coverage to support and enable incident response are defined by the OES. Appropriate tools and techniques have been identified to reliably detect and support incident response and recovery activities for critical assets.</p> <p>b) Monitoring of both IT and OT systems can be achieved through a variety of tools and techniques that could include but not be limited to:</p> <ul style="list-style-type: none"> <li>• Intrusion Detection Systems (IDS) &amp; Intrusion Prevention Systems (IPS), which should be tailored and customised to the operating environment (e.g. covering all necessary proprietary and custom IT &amp; OT protocols, performing passive monitoring to avoid potential performance issues within sensitive OT networks);</li> <li>• Malicious code protection monitoring (e.g. endpoint protection, anti-malware &amp; antivirus);</li> <li>• Networks &amp; boundary protection monitoring;</li> <li>• Identity &amp; Access Management monitoring tools (e.g. including session monitoring/recording, privileged, shared, and critical user IDs tracking);</li> </ul>

	<ul style="list-style-type: none"><li>• Establish tools to monitor systems supporting critical services (e.g. Active directory, historians, databases, third party access).</li> <li>c) Monitoring devices should be strategically deployed within the control system (e.g. at selected perimeter locations and near systems supporting critical applications) to collect essential information according to the organisational monitoring coverage strategy.</li> <li>d) Monitoring mechanisms may also be deployed at ad hoc locations within the control system to track specific transactions and events.</li> <li>e) Monitoring tools should make use of all logging data collected to pinpoint activity within an incident to facilitate effective monitoring of the networks and information systems supporting your essential function.</li> <li>f) Where possible all logging sources should be enabled, and the logs collected in order (or accurately time-stamped) to better inform the investigation and incident response process.</li> <li>g) Monitoring tools should include appropriate reporting mechanisms to allow for a timely response to events and security incidents according to organisational incident response processes.</li> <li>h) To keep the reporting focused and the amount of information to a level that could be processed by the recipients, mechanisms such as integration and monitoring through Security Operation Centres (SOC) and Security Information and Event Management (SIEM) systems should be applied to correlate individual events into aggregate reports, which establish a larger context in which the raw events occurred to support incident response activities.</li> <li>i) Additionally, these mechanisms could be used to track the effect of security changes to the control system. Having forensic tools pre-installed could facilitate incident analysis and response.</li> <li>j) Monitoring covers both IT and OT systems and where practical to do so extends down through the Purdue architecture to industrial control system devices. Monitoring and logging for activities at</li></ul>
--	---

	<p>these lower layers may be possible to do and is largely dependent upon technology.</p> <p>k) You should ensure that the use of security monitoring tools and scanning techniques does not adversely impact the operational performance of the essential function (e.g. performing passive monitoring with custom industrial controls systems (ICS) and OT systems). This may limit capabilities deployed on OT systems in particular.</p> <p>l) OES should always consider deploying technology where practical to do so unless the operational risk (availability and network integrity) outweighs the benefit (evidence-based assessment) in providing coverage.</p> <p>m) Where monitoring is not provided the asset should be protected from inference through a combination of physical and procedural measures.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) As above. OES have a defined process and is following procedures set out to enable security monitoring including technical requirement and malicious code detection (complimented by objective D).</p> <p>b) Identification of critical components and locations to gather understanding of network traffic and general systems health.</p> <p>c) Assessment process to support deployment of logging and monitoring capabilities across the network with clear objectives and goals established.</p>
<p>(Achieved)  IGP 7</p>	<p>Ofgem interprets this IGP as follows:</p> <p>There is justified confidence that monitoring should detect the presence of known indicators of compromise on the networks and systems supporting your essential function.</p>

<p>Validation of Monitoring Capability</p>	<ul style="list-style-type: none"> <li>a) You should assure and document testing and validation of monitoring systems.</li> <li>b) Monitoring could include integration with Security Operation Centres (SOCs) for continuous analysis and incident response capabilities.</li> <li>c) You should employ automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks.</li> <li>d) The monitoring systems should be updated regularly to maintain their effectiveness.</li> </ul>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Routine testing and commissioning or acceptance tests for monitoring and detection programmes;</li> <li>b) Commissioning of internal / external compliance audits;</li> <li>c) Documented SOC (Security Operation Centres) integration &amp; testing;</li> <li>d) Documented penetration tests;</li> <li>e) Review of incident response and recovery testing and exercising (see D1.x).</li> </ul>
<p>(Achieved)  IGP 8  Privileged Users</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) Monitoring is conducted of privileged user activity in relation to the administration of network and information system assets supporting your essential function for suspicious or undesirable activity where practical to do so. For IT based systems this should be comprehensive. For OT systems this is not likely to be achievable on obsolete systems and privileged user activity should be managed procedurally to restrict unauthorised change.</li> <li>b) You should design and implement additional logging requirements for privileged users, such as System Administrators and</li> </ul>

	<p>Operators, in the networks and information systems supporting your essential function.</p> <p>Privileged users have access to more sensitive information, including security-related information, than the general user population. Access to such information means that privileged users can potentially do greater damage to systems and organisations than non-privileged users. Therefore, implementing additional monitoring on privileged users helps to ensure that organisations can identify malicious activity at the earliest possible time and take appropriate actions.</p> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Control of work procedures established and actively being followed.</li> <li>b) Physical and Technical controls to prevent access to systems without authorisation.</li> <li>c) Development and implementation of a comprehensive monitoring strategy evidence through technical capability review.</li> </ul>
<p>(Partially Achieved) IGP 2</p> <p>(Achieved) IGP 9</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) Monitoring data is collected from, at least, the critical networks and systems supporting your essential function (note – system capability is covered by 6).</li> <li>b) It may not be possible to monitor all parts of all systems due to limitations in technology, communications, etc. However, monitoring should be in place for critical elements of the networks and information systems supporting your essential functions.</li> <li>c) Monitoring scope could include, but not be limited to:</li> </ul>



<p>Monitoring Coverage (1)</p>	<ul style="list-style-type: none"> <li>• Control centres;</li> <li>• Supporting enterprise systems, networks &amp; databases;</li> <li>• Engineering workstations &amp; data historians;</li> <li>• Critical PLCs;</li> <li>• Supervisory Control and Data Acquisition (SCADA) systems;</li> <li>• Distributed Control Systems (DCS);</li> <li>• Firewalls &amp; network switches;</li> <li>• Energy Management Systems (EMS);</li> <li>• Single points of failure systems;</li> <li>• Critical network zones or conduits;</li> <li>• Egress or ingress zones (inbound and outbound communications traffic);</li> <li>• Safety instrumented systems (SIS);</li> <li>• Unauthorised assets connected to the SCADA &amp; ICS network;</li> <li>• IT &amp; OT specific protocols &amp; ports;</li> <li>• Specific monitoring of key assets (e.g. domain controllers, engineering workstations, assets accessed from non-ICS networks, assets used for file transfer by portable media, perimeter devices, etc.);</li> <li>• Unexpected shutdowns or reboots;</li> <li>• For perimeter devices – repeated denied connections, configuration changes, management console access.</li> </ul>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ol style="list-style-type: none"> <li>a) Logging and monitoring system design has been comprehensively assessed for system types and can evidenced as such through lifecycle documentation.</li> <li>b) Suitable architecture and monitoring tools have been implemented to allow the interrogation and identification of IoCs, see C1.e for further details.</li> <li>c) Information, instruction and guidance provided to support personnel responsible for system design, management and use.</li> </ol>

	<p>d) For systems that are not practical to integrate into an active logging and monitoring scheme (e.g. systems that are intermittently connected, or cases where the risk of connection outweighs the benefit of coverage), there has been consideration of alternate methods of system review, such as periodic health checking and review of local systems, or PCAP capture for offline review.</p>
<p>(Partially (Achieved) IGP 2  (Achieved) IGP 9  Monitoring Coverage (2)</p>	<p>Ofgem interprets this IGP as follows:  Prioritising monitoring of network gateways and critical devices –</p> <p>a) Extensive monitoring is performed of network gateways and host-based monitoring for critical devices, where possible.</p> <ul style="list-style-type: none"> <li>• You should implement extensive monitoring of all network gateways, particularly between the networks and systems supporting your essential function and other networks and systems e.g. corporate IT and external.</li> <li>• You should also consider implementing extensive monitoring of conduits between different security zones within the networks and information systems supporting your essential function.</li> <li>• You should implement, where possible, host-based monitoring on critical devices such as, but not limited to, the core devices of the control systems e.g. engineering workstations, operator stations, SCADA master servers, etc.</li> </ul> <p>b) Monitoring of devices at lower levels of the Purdue architecture may need to be managed procedurally to regularly review the status of isolated devices or those systems which do not have any native capability to log and report upon activity.</p>

	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Monitoring strategy and design documentation tied to use case for NIS assets.</li> <li>b) Development of, application and adherence to architecture design practices to enable and support monitoring activities.</li> <li>c) Personnel with the pre-requisite skills and understanding of IT and OT estates have been involved in systems design and approval.</li> <li>d) Monitoring coverage and detection capability has been cross referenced to industry frameworks such as MITRE defend to establish use cases vs attack surface and threat.</li> </ul>
<p>(Partially Achieved)</p> <p>IGP 2</p> <p>(Achieved)</p> <p>IGP 9</p> <p>Monitoring Coverage (3)</p>	<p>Ofgem interprets this IGP as follows:</p> <p>Identifying and understanding common communications traffic and event patterns provides useful information to system monitoring devices to better identify suspicious or anomalous traffic and events when they occur. Such information can help reduce the number of false positives and false negatives during system monitoring.</p> <ul style="list-style-type: none"> <li>a) Provide visibility into network traffic at external and key internal system interfaces to optimize the effectiveness of monitoring devices.</li> <li>b) Analyse outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information.</li> <li>c) Analysing communications traffic and event patterns for the system monitored.</li> </ul>

	<ul style="list-style-type: none"> <li>d) Development of profiles representing common traffic and event patterns.</li> <li>e) Use the traffic and event profiles in tuning system-monitoring devices (see C1.c).</li> </ul>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Monitoring strategy / design documentation.</li> <li>b) Application and adherence to architecture design practices.</li> </ul>
<p>(Achieved)</p> <p>IGP 10</p> <p>Maintaining and Extending Coverage</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) The organisation should ensure that monitoring requirements are included in the design and development of new systems or significant modifications.</li> <li>b) Monitoring should be included as part of the asset management lifecycle and security requirements for critical systems.</li> <li>c) Monitoring coverage provided should be kept under review to support continuous improvement of monitoring coverage improving both technical capabilities of systems employed and analytical techniques to provide actionable intelligence associated with operational event data and logs.</li> </ul> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Artefacts relating to operation and enhancement of monitoring requirements are documented and available to personnel responsible for system design, operation and maintenance.</li> </ul>


- b) A gated change management process exists with roles and responsibilities for change management to suitably qualified individuals having been defined.
- c) Update of logging and monitoring capabilities are appraised within change management activities when updating, modifying or introducing new technologies across network and information systems.

## References and Further Guidance



- [C.1 Security monitoring - NCSC.GOV.UK](#)
- NIST 800-82 R2 – CA-7 Continuous Monitoring, MA-1 System Maintenance Policy and Procedures, SC-3 Security Function Isolation, SI-3 Malicious Code Protection, SI-4 Information System Monitoring
- IEC 62443-2-1 – Sections 4.3.4.3 System Development and maintenance, 4.3.3.3 Physical and environmental security
- ISO/IEC 27001 – Section A.10.10 Monitoring
- ISO/IEC 27019 – Section 12.4 Logging and monitoring

C1.b – Securing Logs

<h2 style="margin: 0;">C1.b – Securing Logs</h2>		
<p><i>You hold logging data securely and grant read access only to accounts with business need. No employee should ever need to modify or delete logging data within an agreed retention period, after which it should be deleted.</i></p>		
Not achieved	Partially achieved	Achieved
<b>At least one of the following statements is true</b>	<b>All of the following statements are true</b>	<b>All the following statements are true</b>
<p>It is possible for logging data to be easily edited or deleted by unauthorised users or malicious attackers.</p> <p>There is no controlled list of who can view and query logging information.</p> <p>There is no monitoring of the access to logging data.</p> <p>There is no policy for accessing logging data.</p> <p>Logging is not synchronised, using an accurate common time source.</p>	<ol style="list-style-type: none"> <li>1. Only authorised staff can <u>view logging data for investigations</u>.</li> <li>2. Privileged users can view logging information.</li> <li>3. There is some monitoring of access to logging data (e.g. copying, deleting or modification, or even viewing.)</li> </ol>	<ol style="list-style-type: none"> <li>4. The <u>integrity</u> of logging data is <u>protected</u>, or any <u>modification is detected and attributed</u>.</li> <li>5. The logging architecture has mechanisms, processes and procedures to ensure that it can protect itself from threats comparable to those it is trying to identify. This includes protecting the function itself, and the data within it.</li> <li>6. Log data analysis and normalisation is only performed on copies of the data keeping the master copy unaltered.</li> <li>7. Logging <u>datasets are synchronised</u>, using an <u>accurate common time source</u>, so separate datasets can be correlated in different ways.</li> <li>8. <u>Access</u> to logging data is <u>limited</u> to those with <u>business need</u> and no others.</li> <li>9. All actions involving all logging data (e.g. copying, deleting or modification, or even viewing) can be traced back to a unique user.</li> </ol>

		10. Legitimate reasons for accessing logging data are given in use policies.
--	--	--


**Ofgem DGE CAF Interpretation**



<p>(Partially Achieved)</p> <p>IGP 1</p> <p>(Achieved)</p> <p>IGP 4</p> <p>Protecting Log Data</p>	<p>Ofgem interprets this IGP as follows:</p> <p>Protecting Log Data</p> <ul style="list-style-type: none"> <li>a) You hold logging data securely and grant read access only to [privileged users] with business need. No employee should ever need to modify or delete logging data within an agreed retention period, after which it should be deleted.</li> </ul> <p>Monitored Access –</p> <ul style="list-style-type: none"> <li>b) Access to logging data is monitored and backed up appropriately.</li> <li>c) There should be a policy and procedures defined and implemented to monitor logging data.</li> <li>d) Security monitoring of logging data should identify unauthorised attempts to access, modify or delete logging data, where practical to do so.</li> <li>e) Security monitoring of logging data should be reviewed in accordance with established policy.</li> </ul>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Documented evidence of practices implemented to achieve this security outcome are available and form part of BAU activities.</li> </ul>


<p>(Achieved)</p> <p>IGP 7</p> <p>Time Sync</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) Infrastructure devices such as routers, switches, and firewalls, servers, endpoints should use centralised time services.</li> </ul> <p>Many of these devices do not have onboard real-time clocks and will revert to a default date and time after a reboot. Devices such as these log critical event data to an internal or external syslog. Proper time stamps on these log entries are important for identifying and resolving faults in the device. Furthermore, synchronized clocks allow for system wide fault analysis involving multiple infrastructure devices.</p> <ul style="list-style-type: none"> <li>b) Where utilised devices should standardise / adopt UTC to support data alignment from multiple sources without the need to provide compensation of time offsets across data sets. Standardising to UTC simplifies log correlation within the organisation and with external parties no matter what time zone the device being synchronised is located in.</li> <li>c) Time service infrastructure within the environment and the method for distribution and synchronisation of devices should be designed with the same security controls as the network segment in which the service is provided.</li> <li>d) Failover options should be considered for network time services to allow for planned degradation of the service provided and minimise impact of any loss or failure upon the network.</li> <li>e) The impact of loss of time services are understood and restoration plans are designed and implemented to enable effective recovery of the service within the required period.</li> <li>f) Monitoring schemes should check the availability and overall health of time services provided via a watchdog or equivalent indicator to detect service interruption within the operational environment and communicate this as part of the overall monitoring programme.</li> </ul>
---	---



	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Documented evidence of practices implemented to achieve this security outcome are available and form part of BAU activities.</li> </ul>
<p>(Achieved) IGP 8  Restricted Access</p>	<p>Ofgem interprets this IGP as follows:</p> <p>Only authorised personnel can view aggregated logging information.</p> <ul style="list-style-type: none"> <li>a) There should be a policy and procedures defined and implemented to ensure only authorised users are permitted to view or copy logging data.</li> <li>b) Where practical to do so users should be prevented from deleting or modify logging data within the defined and documented data retention period. For example remote devices and hardware with localised caching of alert and or event data should be password protected to prevent viewing, alternation, deletion accidental or otherwise, by personnel other than those tasked with responsibility for system administration or upkeep.</li> </ul> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Documented evidence of practices implemented to achieve this security outcome are available and form part of BAU activities.</li> </ul>
<p><b>References and Further Guidance</b></p> <div style="text-align: right;">  </div>	
<ul style="list-style-type: none"> <li>• <a href="#">C.1 Security monitoring - NCSC.GOV.UK</a></li> </ul>	

- 
- NIST SP800-82 R2 – Section 5.16
  - OG86 - Appendix 2 C1 Security Monitoring
  - IEC 62443/ISA99 3-3 – SR 3.9 Protection of Audit Information, SR 6.1 Audit Log  
Accessibility
  - ISO 27019 – Section 12.4.2

C1.c – Generating Alerts

<b>C1.c – Generating Alerts</b>		
<i>Evidence of potential security incidents contained in your monitoring data is reliably identified and triggers alerts.</i>		
<b>Not achieved</b>	<b>Partially achieved</b>	<b>Achieved</b>
<b>At least one of the following statements is true</b>	<b>All of the following statements are true</b>	<b>All the following statements are true</b>
<p>Alerts from third party security software is not investigated e.g. Anti-Virus (AV) providers.</p> <p>Logs are distributed across devices with no easy way to access them other than manual login or physical action.</p> <p>The resolution of alerts to a network asset or system is not performed.</p> <p>Security alerts relating to essential functions are not prioritised.</p> <p>Logs are reviewed infrequently.</p>	<p>1. Alerts from third party security software are <u>investigated</u>, and action taken.</p> <p>2. Some, but not all, logging datasets can be easily <u>queried</u> with search tools to aid investigations.</p> <p>3. The <u>resolution</u> of alerts to a network asset or system is performed regularly.</p> <p>4. Security alerts relating to some essential functions are <u>prioritised</u>.</p> <p>5. Logs are <u>reviewed</u> at regular intervals.</p>	<p>6. Logging data is enriched with other network knowledge and data when investigating certain suspicious activity or alerts.</p> <p>7. A wide range of signatures and indicators of compromise is used for investigations of suspicious activity and alerts.</p> <p>8. <u>Alerts</u> can be easily <u>resolved to network assets</u> using knowledge of networks and systems. The <u>resolution</u> of these alerts is <u>performed in almost real time</u>.</p> <p>9. Security <u>alerts</u> relating to all essential functions are <u>prioritised</u> and this information is used to support incident management.</p> <p>10. <u>Logs are reviewed</u> almost continuously, in real time.</p> <p>11. Alerts are tested to ensure that they are generated reliably and that it is possible to distinguish genuine security incidents from false alarms.</p>

## Ofgem DGE CAF Interpretation



<p>(Partially Achieved)</p> <p>IGP 1</p> <p>Investigating alerts</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) Where alerts are generated (i.e. malware detection or suspicious behaviour) there is a requirement to prioritise action to [investigate] the root cause of the alert. Resulting in either modification and/or fine tuning of alerts to reduce false positives, or to take risk informed remediation action for assets impacted.</li> <li>b) Common tactics, techniques and procedures used by threat actors (external or internal) should be utilised when you investigate alerts (further information relating to incident investigation is detailed C1.d).</li> </ul>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Documented evidence of practices implemented to achieve this security outcome are available and form part of BAU activities.</li> </ul>
<p>(Partially Achieved)</p> <p>IGP 2</p> <p>Querying logs</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) You have prioritised the aggregation of specific data sets through a central security event and alerting system across the enterprise to enable this capability, but coverage is not comprehensive (see C1.a).</li> <li>b) For systems yet to be integrated into the centralised security and event system, capability of local systems to acquire and store log data has been investigated. Where practical to do so this is configured to capture security event information locally to allow [querying] of the data set during investigation, using either native toolsets and/or third-party software as necessary to easily obtain</li> </ul>

	<p>information within the raw log data collected (see C1.e). This is based on search criteria established within incident response procedures.</p> <p>c) System capability has been explored with OEMs and relevant third parties to ensure understanding of system functionality (art of the possible) has been obtained and considered when establishing your ongoing security monitoring programme for NIS critical assets (see B4).</p> <p>d) Personnel are familiar with and competent to use the systems employed to query log data collected when carry out incident investigation (see C1.e) and routine operation of NIS assets.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Documented evidence of practices implemented to achieve this security outcome are available and form part of BAU activities.</p>
<p>(Partially Achieved)  IGP 3  Alert resolution</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) Where alerts are generated the origin of the alerts are identifiable (linked to an asset register) such that IP address and or unique identifier can easily be [resolved] to a physical asset on the network or determined as untrusted and responded to accordingly.</p> <p>b) Monitoring and detection is performed in (near) real time to provide actionable intelligence which can be dealt with promptly based on a prioritised order (risk based) of response.</p> <p>c) Where asset information is not automatically linked to monitoring toolsets to provide an accurate view of assets being managed, manual updates are routinely conducted to maintain its efficacy. The frequency of which should minimise the need to manually resolve alerts to assets outside of the tooling provided to ensure timely response to alerts as when they are triggered.</p>

	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Documented evidence of practices implemented to achieve this security outcome are available and form part of BAU activities.</li> </ul>
<p>(Partially Achieved) IGP 4 Alert Prioritisation</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) Alerts should be assigned a priority which is determined based on, the relative importance of assets functions and systems, an understanding of vulnerability exposure, and exploitability based on probable threat. Allowing monitoring personnel to triage and respond to the most important alerts efficiently. However, some deficiencies exist within the tooling itself or practical limitations exist which prevent or limit your ability to prioritise alerts for all essential functions.</li> </ul> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Use of centralised security event and incident monitoring tooling to support analysis and comparison of alerts to improve efficiency (see C1.a)</li> <li>b) You have incorporated risk understanding into the design and realisation of your monitoring programme. You have prioritised improvements to fine tune alerts using related intelligence to improve differentiation and support personnel make decisions based on actionable intelligence.</li> <li>c) Were limitations exist e.g. monitoring coverage and / or system capability, you have taken a prioritised approach to address any deficiency and/or resolve practical limitations.</li> </ul>

	<ul style="list-style-type: none"> <li>d) Information learned from previous incidents informs the prioritisation of alerts and is actively used to differentiate alerts raised.</li> <li>e) You are actively seeking to improve use of threat intelligence to improve prioritisation of events, automating this where practical to improve efficiency.</li> </ul>
<p>(Partially Achieved)</p> <p>IGP 5</p> <p>Log Review</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) The acquisition of logging and monitoring data is actively reviewed by operational personnel, at a suitable frequency which is informed by system / function criticality, exploitable vulnerability exposure and threat.</li> </ul> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Establishment of a logging and monitoring strategy defining requirements for review.</li> <li>b) Documented evidence of practices implemented to achieve this security outcome are available and form part of BAU activities.</li> </ul>
<p>(Achieved)</p> <p>IGP 6</p> <p>Log Enrichment</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) Wherever practical OES should aim to centralise security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this requirement.</li> <li>b) Aggregating data provides an opportunity to carry out detailed log analysis and supports the more advanced detection techniques beyond standardised tooling. It can be key to analysing sequential</li> </ul>

	<p>activities related to cyber intrusion that stand alone systems would fail to identify in isolation.</p> <p>Useful information reference providing further information on the log enrichment forms one of the topics of interest from the NCSC guidance note on “Building a Security Operations Centre (SOC)” - <a href="https://www.ncsc.gov.uk/collection/building-a-security-operations-centre">https://www.ncsc.gov.uk/collection/building-a-security-operations-centre</a></p> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Development and documenting of security monitoring strategy and use cases for systems monitored.</li> <li>b) Architectural design of security monitoring solution.</li> <li>c) Alignment of security monitoring technique to threat intelligence (see objective D).</li> </ul>
<p>(Achieved)</p> <p>IGP 7</p> <p>Security Alerts</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) OES should select and adopt a detection technique that is based on the probable threat profile faced by the organisation providing coverage across the estate that is matched to attacker sophistication.</li> <li>b) Detection techniques available range from the use of commercial off the shelf (COTS) security tooling from various security vendors; the creation of custom use cases and data mining techniques through to proactive threat hunting (see C2) and many graduations in-between.</li> <li>c) Each detection technique has its own benefits and limitations and may carry a significant overhead to deploy effectively. And are therefore not suitable for all cases where limitations and resource</li> </ul>



	<p>demands change the probability of success for a given environment.</p> <p>d) You have established a security monitoring strategy across your estate. Providing a use case for security monitoring that considers threat to devise a strategy for security monitoring and detection, and is measured and appropriate for the asset being protected. In-line with the security monitoring strategy, you should design and implement an appropriate monitoring capability consisting of appropriate tools, processes, and personnel to satisfy this use case, focussing on probable attacker sophistication and threat intelligence.</p> <p>e) Your capability should use a wide range of signatures and indicators of compromise to help identify and analyse suspicious activity, at least in the critical areas of the networks and systems supporting your essential functions.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Adoption of security monitoring programme that is tailored to the operating environment adopting an appropriate detection approach aligned to the organisations risk profile.</p> <p>b) For low threat sites, use of COTs security tooling is likely to be sufficient to enable detection of frequent, untargeted common attacks. With increasing intelligence being built into any detection technique as the probability of more advanced actors targeting any specific asset owned and operated increases.</p> <p>c) For NIS critical assets security alerts and logs should be generated for all systems supporting essential functions typically. The scope for OT systems for example could include, but not be limited to:</p> <ul style="list-style-type: none"> <li>• Engineering and operator workstations;</li> <li>• Critical Programmable Logical Controllers (PLCs);</li> </ul>

	<ul style="list-style-type: none"> <li>• Supervisory Control and Data Acquisition (SCADA) systems;</li> <li>• Distributed Control Systems (DCS);</li> <li>• Firewalls &amp; network switches;</li> <li>• Data historians and databases;</li> <li>• Energy Management Systems (EMS);</li> <li>• Single points of failure systems;</li> <li>• Safety instrumented systems (SIS);</li> <li>• All unauthorised assets connected to the SCADA and Industrial Control Systems (ICS) network;</li> <li>• Key assets (e.g. domain controllers, assets accessed from non-ICS networks, assets used for file transfer by portable media, perimeter devices, gateways, etc.);</li> <li>• Endpoint protection, antivirus, or anti malware services;</li> <li>• Supporting enterprise systems.</li> <li>• Use of wireless intrusion detection systems (WIDS) for sensitive networks to detect and alert on unauthorized wireless access points.</li> </ul> <p>d) At minimum the configuration of detection systems and tooling should use a wide range of signatures and indicators of compromise to help identify and analyse suspicious activity, at least in the critical areas of the networks and systems supporting your essential functions.</p> <p>e) For OT assets, monitoring could include the security alerts / events from the assets deployed that would indicate that a countermeasure has failed or been compromised – based upon a review of the countermeasures deployed. This could include, for example:</p> <ul style="list-style-type: none"> <li>• unauthorised assets connected to the OT network login failures and locked accounts etc.</li> <li>• access attempts from remote connections.</li> <li>• unauthorised activities by privileged (e.g. administrator) accounts such as, security policy changes, new / modified user accounts, access to security logs, alerts from security software, e.g. AV, IDS, whitelisting etc.</li> <li>• For key assets (e.g. domain controllers, engineering workstations, assets accessed from non-OT networks, assets used for file transfer by portable media, perimeter devices):</li> </ul>
--	---

	<ul style="list-style-type: none"> <li>○ high network traffic (at key points)</li> <li>○ high CPU usage (key assets)</li> <li>○ low disk space</li> <li>○ large numbers of events generated in security logs</li> <li>○ unexpected shutdowns or reboots</li> <li>○ For perimeter devices – repeated denied connections, configuration</li> <li>○ changes, management console access.</li> </ul>
<p>(Achieved)</p> <p>IGP 8</p> <p>Mapping of Alerts to Assets</p>	<p>Map alerts to assets in scope –</p> <ul style="list-style-type: none"> <li>a) Alerts should be resolved to assets in the networks and systems supporting your essential function.</li> <li>b) The monitoring and alerting systems should be designed and implemented such that it is possible to trace alerts to individual assets impacted to aid investigation and response.</li> <li>c) Assets should be mapped, updated, and aligned according to organisational asset management processes.</li> </ul> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) See IGP 6 – System documentation has been produced, detailing design, implementation and testing of alerting systems, specifically data flows between detection engines and reporting tools. Where this covers OT assets this may cover operational alarms and event data sets and historical data from the available process historians or alarm annunciation systems where this may enrich the data stream.</li> </ul>
<p>(Achieved)</p>	<p>Ofgem interprets this IGP as follows:</p>

<p>IGP 9</p> <p>Prioritisation for Alerts</p>	<p>a) Security alerts relating to the networks and systems supporting your essential function should be prioritised, investigated and an appropriate action taken.</p> <p>b) Alerts should be triaged according to defined criticality, to determine the priority for investigation aligned with organisational incident management and response processes.</p> <p>c) Prioritised alerts should be investigated to assess the potential impact on essential functions following organisational incident management and response processes.</p> <p>d) Investigation and event correlation may require involvement of IT, OT specialists and third parties.</p> <p>e) Based on the investigation appropriate actions should be identified and executed.</p> <p>f) Actions should be recorded, managed, and monitored for completion.</p> <p>g) Where applicable, the process of prioritising, investigating, and taking appropriate action against alerts is integrated with other operational/management service protection processes (automated and manual response playbooks), which can include but is not limited to:</p> <ul style="list-style-type: none"> <li>• Security incident management and response;</li> <li>• Risk assessment and management;</li> <li>• Remediation activities;</li> <li>• Business continuity and disaster recovery.</li> </ul>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Documented evidence of practices implemented to achieve this security outcome are available and form part of BAU activities.</p>
	<p>Ofgem interprets this IGP as follows:</p>

<p>(Achieved)</p> <p>IGP 10</p> <p>Regular Review of Logs</p>	<p>a) As defined in the monitoring strategy, security logs are reviewed regularly and, if possible, alerts should be reviewed continuously, in real time.</p> <p>b) You employ automated tools to support near real-time analysis of events (e.g. Security information and event management (SIEM), event aggregation tools).</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) System design documents, supporting management processes, instructions detail roles and responsibilities for individuals relating to alert management. This may be backed up by internal audit to assure that measures implemented are being practiced.</p> <p>b) Roles and responsibilities have been assigned to relevant individuals.</p> <p>c) Generation of key performance indicators.</p>
<p>(Achieved)</p> <p>IGP 11</p> <p>Testing of Alerts</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) Alerts are tested to ensure that they are generated reliably and that it is possible to distinguish genuine security incidents from false alarms.</p> <p>b) Alerting systems are optimised prior to deployment and during use, to minimise the generation of nuisance alerts (false positives) with the intent of generating actionable intelligence.</p> <p>c) Detection systems for NIS critical assets should be reviewed at appropriate intervals, in accordance with monitoring strategy, to ensure that they are successfully generating required security alerts and events as intended.</p>

	<p>d) System validation activities should be conducted during design, development and use to verify that the functionality of the tooling has been realised as per design intent, e.g. breach and attack simulation to ensure that the system remains effective.</p> <p>e) Performance testing of event logging components and analysis engines is inbuilt into the tooling to automatically provide system health checking. For example, this could use diagnostic checks to flag unresponsive systems or automatically run test scripts at defined periods (selective subset of events) to verify that the activity conducted generates the required alerts when demanded.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) KPIs relating to system performance are routinely generated and actively reviewed by operational personnel to check on system capability vs design requirements.</p> <p>b) Performance checking of alert systems has been incorporated into testing and exercising (see D1.c) and serves a dual purpose to build capability amongst personnel and provide assurance that events and alerts are generated when demanded.</p>

## References and Further Guidance



- [C.1 Security monitoring - NCSC.GOV.UK](#)
- NIST 800-82 R2 – Appendix G: CA-7 Continuous Monitoring, SI-3 Malicious Code Protection, SI-4 Information System Monitoring
- IEC 62443-2-1 – Section 4.3.4.3 System Development and maintenance
- ISO/IEC 27001 – Section A.10.10 Monitoring
- ISO/IEC 27019 – Section 12.4 Logging and monitoring



C1.d – Identifying Security Incidents

## C1.d – Identifying Security Incidents

*You contextualise alerts with knowledge of the threat and your systems, to identify those security incidents that require some form of response.*



Not achieved	Partially achieved	Achieved
<b>At least one of the following statements is true</b>	<b>All of the following statements are true</b>	<b>All the following statements are true</b>
<p>Your organisation has no sources of threat intelligence.</p> <p>You do not apply updates in a timely way, after receiving them. (e.g. AV signature updates, other threat signatures or Indicators of Compromise (IoCs).</p> <p>You do not receive signature updates for all protective technologies such as AV and IDS or other software in use.</p> <p>You do not evaluate the usefulness of your threat intelligence or share feedback with providers or other users.</p>	<p>1. Your organisation uses some <u>threat intelligence</u> services, but you don't necessarily choose sources or providers specifically because of your <u>business needs</u>, or specific threats in your sector (e.g. sector-based infoshare, ICS software vendors, anti-virus providers, specialist threat intel firms, special interest groups).</p> <p>2. You receive <u>updates</u> for all your <u>signature</u> based protective technologies (e.g. AV, IDS).</p> <p>3. You apply some <u>updates</u>, signatures and IoCs in a <u>timely</u> way.</p> <p>4. You know how <u>effective</u> your <u>threat intelligence</u> is (e.g. by tracking how threat intelligence helps you identify security problems).</p>	<p>5. You have <u>selected threat intelligence</u> feeds using <u>risk-based</u> and <u>threat-informed decisions</u> based on your business needs and sector (e.g. vendor reporting and patching, strong anti-virus providers, sector and community-based infoshare, special interest groups).</p> <p>6. You <u>apply all new signatures and IoCs</u> within a <u>reasonable</u> (risk-based) <u>time</u> of receiving them.</p> <p>7. You <u>receive signature updates</u> for all your <u>protective technologies</u> (e.g. AV, IDS).</p> <p>8. You <u>track</u> the <u>effectiveness</u> of your intelligence feeds and actively share feedback on the usefulness of IoCs and any other indicators with the threat community (e.g. sector partners, threat intelligence providers, Government agencies).</p>



## Ofgem DGE CAF Interpretation



<p>(Partially Achieved)</p> <p>IGP 1</p> <p>Threat Intelligence</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) Selected [threat intelligence] sources should inform your risk assessment and monitoring programmes, as well as your organisational incident response processes. Threat intelligence can be either automated feeds that describe Indicators of Compromise (e.g. hashes of known nefarious files or lists of IP addresses), or more descriptive human readable reports documenting indicators of attacks or reporting on a type of malware. You should consume both types of threat intelligence appropriately.</li> <li>b) For [threat intelligence] to provide impact and contribute effectively (i.e. to inform your understanding of probable threats and threat actors in line with [business needs]), information feeds should be selected to reflect both technology operated and level of activity (motivation), such that you able to prioritise activities to be undertaken. This is in order to manage risk and maintain situational awareness that is based on relevant, context specific information.</li> <li>c) While consuming general threat intelligence can improve your risk understanding, it is likely to result in untargeted activities being created which may distract and deflect resources from critical activities. At worst this may result in unnecessary and inappropriate activities being carried out which are counterproductive to your overall security aims.</li> </ul>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) See IGP 5 for evidence associated with threat intelligence use.</li> </ul>
<p>(Partially Achieved)</p>	<p>Ofgem interprets this IGP as follows:</p>

<p>IGP 3</p> <p>Signature Updates</p>	<p>a) This IGP notes that there may be limitations in your ability to apply updates in line with IGP 6. You understand the importance of carrying out updates for signatures and IoCs and have a prioritised action plan to complete updates on a rolling schedule which reflects the sensitivity of your assets and the importance of detection capability across those assets.</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Your programme of activity to identify and prioritise updates to signatures and indicators of compromise is based on your documented criticality assessment of NIS assets. It is also documented within lifecycle documentation to substantiate and justify practice applied relative to risk context and business needs.</p> <p>b) See IGP 6 for evidence associated with signature updates and IoCs.</p>
<p>(Partially Achieved)</p> <p>IGP 4</p> <p>Effectiveness of Threat Intelligence</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) You routinely report on the success or otherwise of your detection capability and overall monitoring programmes. Drawing out aspects relevant to the way in which threat intelligence has informed your programme of activity and its overall [effectiveness] in maintaining your agreed risk position.</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) You use, as appropriate, selected independent third-party testing and assessment, breach and attack simulation tooling and/or in-house testing and exercising to validate this capability. You draw conclusions from the data derived as to the overall effectiveness of your use of threat intelligence. This informs processes to shape and prioritise continuous improvement of your capability.</p> <p>b) You routinely conduct root cause analysis on incidents experienced to identify deficiencies in coverage and understand how threat intelligence (knowledge and understanding of cyber incidents) can</p>

	<p>be used to bridge gaps e.g. through the selection of alternative sources of information feeds used to shape monitoring programmes and design of controls.</p> <p>c) You use statics learned from detections to derive key performance indicators (leading and lagging) and engage with stakeholders both internally and external to track performance over time.</p> <p>d) You discuss observed cyber activity and seek validation of your capability relative to collective understanding of cyber activity observed by peers within the sector (known unknowns). Seeking to refine threat intelligence sources used, detection capability and overall awareness.</p>
<p>(Achieved)</p> <p>IGP 5</p> <p>Selection of Threat Intelligence</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) When gathering [threat intelligence] you should use your understanding of the operational environment to prioritise identification of cyber threat intelligence that supports the continued development of their security programme. Using a combination of strategic, tactical and operational intelligence to inform their view on current and future security risks. Helping to progress long term improvement programmes and shorter-term needs such as incident response capabilities alike.</p> <p>b) Selected threat intelligence sources should be integrated and utilised as part of organisational incident response processes. Threat intelligence can be either automated feeds that describe Indicators of Compromise (e.g. hashes of known nefarious files or lists of IP addresses) or more descriptive human readable reports documenting indicators of attacks or reporting on a type of malware. You should consume both types of threat intelligence appropriately.</p> <p>Where appropriate, Ofgem would expect to see the following evidence of good practice as follows.</p>

	<p>a) Documented review of use cases for intelligence gathered to ensure that intelligence is used to support security monitoring activities within your business. For example collation and use of:</p> <ul style="list-style-type: none"><li>• Strategic Threat Intelligence is used to support long-term planning and identification of broad trends. It should be used to assess an OESs overall risk posture and to formulate strategies for mitigating those risks. This type of intelligence helps OES identify potential threats and vulnerabilities, as well as understand the motives and capabilities of adversaries.</li><li>• Tactical threat intelligence (TTI) is the gathering and analysis of information about potential threats to an OES, with the goal of identifying and mitigating those threats. TTI can help identify the how (Tactics, techniques and procedures) and where of cyber-attacks. It is shorter-term and more actionable than strategic intelligence.</li><li>• Operational threat intelligence is real-time information that is most useful for responding to active threats. It can be used to track adversary movements and take immediate action to thwart an attack.</li></ul> <p>b) When collecting cyber threat intelligence OES should utilise a range of sources, carefully curated to cover the range of IT and OT systems employed across their estate prioritising feeds for high-risk systems. Information sources could include, but not be limited to the following sources:</p> <ul style="list-style-type: none"><li>• National Cyber Security Centre (NCSC);</li><li>• Cyber Security Information Sharing Partnership (CiSP);</li><li>• Information exchanges and industry groups;</li><li>• Information Sharing and Analysis Centre (ISACs);</li><li>• Original equipment manufacturers (OEMs) and sector specific vendors;</li><li>• Specialist third party providers;</li><li>• Specialised forums, security feeds and mailing lists (e.g. SCADAsec, ICS-CERT).</li></ul>
--	--

<p>(Achieved)</p> <p>IGP 6</p> <p>Updating of IoCs</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) All new signatures and Indications of Compromise (IoCs) are applied within an appropriate time.</li> <li>b) Updates are implemented, based on risk and according to company policy.</li> <li>c) Updates should be applied within an appropriate timeframe dependent on the assigned priority for deployment (e.g. anti-virus and anti-malware signatures, intrusion detection systems updates).</li> <li>d) Where appropriate to do so, updates should occur automatically to reduce the need for manual intervention. Updating of signatures and IOCs should occur across network and information systems unless purposely segregated and isolated from external connection as a preventive control measure.</li> <li>e) Within OT and or IT assets that are not redundant and whose availability is considered essential a suitable and sufficient risk assessment should be carried out prior to deployment where updates have the potential to adversely impact the networks and information systems supporting the essential function. Any risks should be managed according to organisational risk management policy and processes.</li> <li>f) When considering the suitability of signature updates and new IOCs for deployment within operational technology installations and IT systems with critical business impacts OES should always seek to verify the compatibility of updates through testing on a representative "offline" system in the same way vulnerability patches and system updates are managed. Whilst the potential for disruption is lower than system updates and patches, even OEM approved signature updates and IOCs have the potential to create problems within an OT environment where the bespoke nature of the environment can give rise to compatibility issues and false positives may result in performance being impaired. Any deployment of AV therefore needs to be cognisant of the priority</li> </ul>
--	---

	<p>order for OT systems which value safety and availability above all other considerations.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Documented evidence of practices implemented to achieve this security outcome are available and form part of BAU activities.</li> </ul>
<p>(Achieved)  IGP 7  Signature Updates</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) All signature based protective technologies are received for the networks and systems supporting your essential function, in line with monitoring and detection requirements established use case (see C1.c also).</li> <li>b) When obtaining updates, you should ensure that signature updates and IoCs are obtained and verified from trusted sources (e.g. vendor website). Ideally you should look to automate this process to improve efficiency and completeness.</li> <li>c) All signature updates should be reviewed and prioritised for deployment, informed by relevant threat intelligence, within an appropriate timeframe in accordance with company policy. Where the number of assets to be protected is considerable then automated processes for distribution across the enterprise should also be facilitated. Allowing for granular control for automatic application of updates or otherwise depending upon the area of application.</li> </ul>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Documented evidence of practices implemented to achieve this security outcome are available and form part of BAU activities.</li> </ul>

<p>(Achieved)</p> <p>IGP 8</p> <p>Effectiveness of Cyber Threat Intelligence</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) Policy, processes and procedures set up to manage information feeds and cyber threat intelligence data should ensure that periodic review of information held maintain its currency.</p> <p>b) Periodic reviews should consider whether the intelligence received remains:</p> <ul style="list-style-type: none"> <li>• Appropriate and relevant</li> <li>• Actionable</li> <li>• Useful in informing the identification of security incidents according to organisational processes.</li> <li>• Aligned to strategic, tactical and operational needs.</li> <li>• In line with industry best practice and reflective of the state of the art within cyber offensive and defensive tradecraft</li> <li>• is delivered, consumed and actioned efficiently.</li> <li>• Requires supplementing or the addition of revised tooling and or processes to improve its usefulness.</li> </ul>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>See IGP 5 above.</p>
<p>Additional Comments -</p> <p>Wherever protective equipment is used to monitor network and information systems it should be capable of integrating to a centralised management resource, unless the effort to implement is considered disproportionate to the benefit received.</p> <p>Where automation is employed to manage protective equipment, OES should ensure that the status of devices deployed are auditable and understood relative to performance requirements</p>	

i.e. the use of automated dashboards, KPIs and status reports is scheduled into the OES programme of activity to manage assets.

## References and Further Guidance



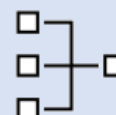
- [C.1 Security monitoring - NCSC.GOV.UK](#)
- NIST 800-82 R2 – Appendix G: CA-7 Continuous Monitoring, SI-3 Malicious Code Protection, SI-4 Information System Monitoring, IR-1 Incident Response Policy and Procedures, IR-4 Incident Handling
- IEC 62443-2-1 – Sections 4.3.4.3 System Development and maintenance, 4.3.4.5 Incident planning and response
- ISO/IEC 27001 – Sections A.10.10 Monitoring, A.13.2 Management of information security incidents and improvements
- ISO/IEC 27019 – Section 12.4 Logging and Monitoring



C1.e – Monitoring Tools and Skills

**C1.e – Monitoring Tools and Skills**

*Monitoring staff skills, tools, and roles, including any that are outsourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have knowledge of the essential functions they need to protect.*



Not achieved	Partially achieved	Achieved
<p><b>At least one of the following statements is true</b></p>	<p><b>All of the following statements are true</b></p>	<p><b>All the following statements are true</b></p>
<p>There are no staff who perform a monitoring function.</p> <p>Monitoring staff do not have the correct specialist skills.</p> <p>Monitoring staff are not capable of reporting against governance requirements.</p> <p>Monitoring staff lack the skills to successfully perform some significant parts of the defined workflow.</p> <p>Monitoring tools are only able to make use of a fraction of logging data being collected.</p> <p>Monitoring tools cannot be configured to make use of new logging streams, as they come online.</p> <p>Monitoring staff have a lack of awareness of the essential functions the organisation provides, what assets relate to those functions and hence the importance of the logging data and security events.</p>	<p>1. Monitoring staff have some <u>investigative skills</u> and a basic understanding of the data they need to work with.</p> <p>2. Monitoring staff can <u>report</u> to other parts of the organisation (e.g. security directors, resilience managers).</p> <p>3. Monitoring staff are <u>capable</u> of following most of the required workflows.</p> <p>4. Your <u>monitoring tools</u> can make use of <u>logging</u> that would capture most unsophisticated and untargeted attack types.</p> <p>5. Your <u>monitoring tools</u> work with most <u>logging data</u>, with some configuration.</p> <p>6. Monitoring staff are <u>aware</u> of some <u>essential functions</u> and can <u>manage alerts</u> relating to them.</p>	<p>7. You have <u>monitoring staff</u>, who are responsible for the <u>analysis, investigation and reporting</u> of monitoring alerts covering both security and performance.</p> <p>8. Monitoring staff have defined roles and skills that cover all parts of the monitoring and investigation process.</p> <p>9. Monitoring staff follow process and procedures that address all governance reporting requirements, internal and external.</p> <p>10. Monitoring staff are <u>empowered</u> to look beyond the fixed process to <u>investigate and understand</u> non-standard threats, by developing their own investigative techniques and making new use of data.</p> <p>11. Your monitoring tools make use of all logging data collected to pinpoint activity within an incident.</p> <p>12. Monitoring staff and tools drive and shape new log data</p>

		<p>collection and can make wide use of it.</p> <p>13. Monitoring staff are aware of the operation of essential functions and related assets and can identify and prioritise alerts or investigations that relate to them.</p>
--	--	---

**Ofgem DGE CAF Interpretation**



<p>(Partially Achieved)</p> <p>IGP 1</p> <p>Investigative Skills</p>	<p>Monitoring staff have some investigative skills and a basic understanding of the data they need to work with.</p> <p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) Competency requirements for personnel involved with operation and management of cyber security monitoring across all aspects of the lifecycle (design, development and implementation) have been understood relative to the complexity of the network and information systems operated. You are proactively addressing any skills gaps identified to build up capability.</li> <li>b) Where required skill sets are not maintained in house you have sought to offset any operational risk through arrangements with third parties as and when required i.e. specialist skills such as forensic analysis capability.</li> <li>c) You have established internal training programmes to provide access to development systems, test beds and learning materials as appropriate given the complexity of your network and information systems.</li> <li>d) Your development programmes are aligned with recognised frameworks and or competency programmes covering the related discipline.</li> <li>e) Support for development is funded and resourced.</li> </ul>
--	---

	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Documented evidence of practices implemented to achieve this security outcome are available and form part of BAU activities.</li> </ul>
<p>(Partially Achieved) IGP 2  Monitoring Staff Incident Reporting</p>	<p>Monitoring staff can report to other parts of the organisation (e.g. security directors, resilience managers).</p> <p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) Processes should exist to allow [reporting] of potential cyber security incidents by all personnel (internal and external). Along with information, instruction and guidance on how to do so.</li> <li>b) Lines of reporting and communication channels have been established to support escalation of security incidents identified by monitoring personnel. This includes appropriate means of feedback and reporting on issues raised to address any concern and escalate incidents based on criticality and threat.</li> </ul> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Policies and procedures detail roles and responsibilities within the organisation and involve necessary stakeholders to support enactment of any required action required to close out the concern identified.</li> <li>b) Forums and working groups are established across the organisation to support discussion and resolution of security challenges and help improve the efficacy of security monitoring and reporting through to close out.</li> </ul>
<p>(Partially Achieved) IGP 3</p>	<p>Monitoring staff are capable of following most of the required workflows.</p> <p>Ofgem interprets this IGP as follows:</p>

<p>Capability</p>	<ul style="list-style-type: none"> <li>a) System capability within tool sets provided has been explored in collaboration with OEMs and knowledgeable third parties to ensure understanding of system functionality. This is translated into operational procedures and internal guidance to support end users in their application and use.</li> <li>b) You have developed within your monitoring strategy use cases to support monitoring staff. You select and apply appropriate tooling based on the required situation, aligned to the complexity of the network and information systems being manage.</li> <li>c) Personnel are familiar with and competent to query log data collected when carrying out incident investigation (see C1.e) and routine operation of NIS assets. Skills sets are actively developed through cross skilling and mentoring, shadowing as required to build both confidence and competency in their use.</li> </ul>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Documented evidence of practices implemented to achieve this security outcome are available and form part of BAU activities.</li> </ul>
<p>(Partially Achieved) IGP 4  Monitoring Tools</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) Your monitoring solution(s) are able to ingest or make use of common Indicators of Compromise (IOCs) and related threat intelligence feeds provided by NCSC, and other relevant third parties (see threat intelligence) to enrich their detection capability. These are used to support analysis of data sets and easily identify and report upon potential security incidents.</li> </ul>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Documented evidence of practices implemented to achieve this security outcome are available and form part of BAU activities.</li> </ul>

<p>(Partially Achieved) IGP 5</p> <p>Monitoring Tools</p>	<p>Ofgem interprets this IGP as follows: See C1.a and C1.d</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Routine update of use cases for monitoring of assets is undertaken to ensure continuous improvement in both the capability of personnel and the selection and use of logging and monitoring solutions (see C1.a), which reflects the complexity of the network and information systems managed and threat.</li> <li>b) Log ingestion and analysis is (partly) automated to ease collection and transform raw data sets into actionable intelligence.</li> </ul>
<p>(Partially Achieved) IGP 6 and (Achieved) IGP 13</p> <p>Operational Awareness</p>	<p>Monitoring personnel should be aware of essential functions and assets in scope and can identify and prioritise alerts or investigations that relate to them.</p> <p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) Monitoring personnel are made aware of the relative importance of assets, functions and systems in use and can prioritise action to be taken based on understanding of the probable impact to the essential service or function provided. Allowing them to make risk informed decisions relating to any response, supporting them to effectively identify, prioritise and investigate alerts, engaging other personnel or third parties where necessary.</li> <li>b) Monitoring staff have a contextual awareness of the overall business operation and understand the importance of functions undertaken to enable the business to maintain and sustain its essential service.</li> </ul>

	<p>c) Within operational technology environments this understanding extends to role that functions may perform in relation to process safety.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Documented evidence of practices implemented to achieve this security outcome are available and form part of BAU activities.</p>
<p>(Achieved)  IGP 7  Support Personnel</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) Personnel are in place who are responsible for the analysis, investigation and reporting of monitoring alerts covering both security and system performance.</p> <p>b) The size and structure of these teams will inevitably vary between organisations and locations and monitoring personnel could be employees or third parties on premises or provided as part of a managed service.</p> <p>c) Irrespective of location and operational alignment (internal or external) monitoring personnel should have: -</p> <ul style="list-style-type: none"> <li>• Detailed understand of the network and information systems employed to support the essential function and their relative importance to the correct operation of the essential service.</li> <li>• poses detailed knowledge of the hardware and software systems in use across both IT and OT domains and the architectural arrangements in place to support management and operation of systems.</li> <li>• an understanding of the importance of data used across the estate and its relative importance to the correct operation of the essential service.</li> </ul>


	<p>d) The selection of personnel and team size should be carefully matched to the expected threat and impact the organisation is likely to encounter. Whether this is basic commodity attacks which may only require basic skill set and familiarity with commercial tools and preventive controls through to highly sophisticated actors requiring equally skilled operatives capable of supporting the detection of rare, targeted custom attacks for example.</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Availability of supporting documentation and information to substantiate selection and retention of appropriately skilled personnel.</p>
<p>(Achieved) IGP 8  Defined Roles and Skills</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) Monitoring personnel have defined roles and skills/competence requirements that, together with other personnel such as operators, system administrators and third parties, are able to cover all parts of the monitoring and investigation process.</p> <p>b) Appropriate roles should be defined and assigned to perform the analysis, investigation, and reporting activities.</p> <p>c) The personnel should have appropriate training in OT and security knowledge to perform their role.</p> <p>d) For OT systems the range of systems employed and varied interfaces and reporting means that likely coverage required to achieve this aim extends to the integration of site operational and maintenance staff.</p> <p>e) Monitoring personnel should report to an appropriate part of the organisation.</p>

	<p>f) Monitoring personnel should report into the appropriate part of the organisation that is able to provide the necessary resources and authority to investigate security monitoring data, alerts, and incidents. This could be, for example, IT, OT, Operations, Information Security and potential third parties.</p> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Documented evidence of practices implemented to achieve this security outcome are available and form part of BAU activities.</p>
<p>(Achieved)</p> <p>IGP 9</p> <p>Documented Processes</p>	<p>Documented Processes –</p> <p>Monitoring personnel follow documented processes, procedures and workflows for the analysis, investigation, and reporting of monitoring alerts.</p> <p>a) Standard workflows and playbooks should be defined and documented to cover the analysis, investigation, and reporting activities (internal and external).</p> <p>b) A workflow should exist to ensure that reportable regulatory events, can be identified and reported to the Competent Authority (CA), within 72 hours of becoming aware of the incident.</p> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>b) Documented evidence of practices implemented to achieve this security outcome are available and form part of BAU activities.</p>




<p>(Achieved)</p> <p>IGP 10</p> <p>Freedom to Investigate</p>	<p>Ofgem interprets this IGP as follows:</p> <p>Monitoring personnel are empowered to look beyond the fixed process to investigate and understand non-standard threats.</p> <p>a) Personnel conducting monitoring investigations should be permitted to conduct their own investigations, going beyond the documented workflows and playbooks where incidents may vary and novel, difficult to detect, techniques may be employed by adversaries<sup>45</sup>.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Review of location policy, processes and practices associated with logging monitoring and detection.</p>
<p>(Achieved)</p> <p>IGP 11</p> <p>Monitoring Tools</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) Your monitoring tools make use of all logging data collected to pinpoint activity within an incident.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Documented evidence of practices implemented to achieve this security outcome are available and form part of BAU activities.</p>
	<p>Ofgem interprets this IGP as follows:</p>


<sup>45</sup> This practice is bordering upon security outcomes associated with system abnormalities for attack detection (C2) and unless specially required to meet the outcomes required under C2 is not an essential element to be met within C1.

<p>(Achieved)</p> <p>IGP 12</p> <p>Monitoring Staff</p>	<p>a) Monitoring staff and tools drive and shape new log data collection and can make wide use of it.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Documented evidence of practices implemented to achieve this security outcome are available and form part of BAU activities.</p>
<p><b>References and Further Guidance</b></p>	
<div style="display: flex; justify-content: space-between; align-items: center;"> <div data-bbox="193 938 1114 1361"> <ul style="list-style-type: none"> <li>• <a href="#">C.1 Security monitoring – NCSC.GOV.UK</a></li> <li>• NIST 800-82 R2 – Appendix G: CA-7 Continuous Monitoring, SI-4 Information System Monitoring</li> <li>• IEC 62443-3-3 – Section 10.4, SR 6.2 Continuous Monitoring</li> <li>• IEC 62443-2-1 – Section 4.3.4.3 System Development and maintenance</li> <li>• ISO/IEC 27001 – Section A.10.10 Monitoring</li> <li>• ISO/IEC 27019 – Section 12.4 Logging and monitoring</li> </ul> </div> <div data-bbox="1114 938 1406 1361" style="text-align: center;">  </div> </div>	

## C2 Proactive Security Event Discovery

C2 Proactive Security Event Discovery		
<p><i>The organisation detects, within networks and information systems, malicious activity affecting, or with the potential to affect, the operation of essential functions even when the activity evades standard signature-based security prevent/detect solutions (or when standard solutions are not deployable).</i></p>		
Related CAF Objective(s)	Ref	Contributing Outcome
C2 – Proactive Security Event Detection	C2.a	System Abnormalities for Attack Detection
	C2.b	Proactive Attack Discovery

### C2.a – System Abnormalities for Attack Detection

C2.a – System Abnormalities for Attack Detection		
<p><i>You define examples of abnormalities in system behaviour that provide practical ways of detecting malicious activity that is otherwise hard to identify.</i></p>		
Not achieved	Achieved	
At least one of the following statements is true	All the following statements are true	
<p>Normal system behaviour is insufficiently understood to be able to use system abnormalities to detect malicious activity.</p> <p>You have no established understanding of what abnormalities to look for that might signify malicious activities.</p>	<p>1. <u>Normal system behaviour</u> is fully <u>understood</u> to such an extent that searching for system abnormalities is a <u>potentially effective</u> way of <u>detecting malicious activity</u> (e.g. you fully understand which systems should and should not communicate and when).</p>	

	<p>2. System <u>abnormality descriptions</u> from past attacks and threat intelligence, on yours and other networks, are used to <u>signify malicious activity</u>.</p> <p>3. The <u>system abnormalities</u> you search for consider the <u>nature of attacks</u> likely to impact on the networks and information systems supporting the operation of essential functions.</p> <p>4. The <u>system abnormality descriptions</u> you use are <u>updated</u> to <u>reflect changes</u> in your networks and information systems and current threat intelligence.</p>
--	--

## Ofgem DGE CAF Interpretation



<p>General commentary</p>	<p>Anomaly detection is the identification of rare events, items, or observations which are suspicious because they differ significantly from standard behaviours or patterns.</p> <p>Proactive security event discovery relies upon good quality security monitoring (C1) having been established and understanding of network and user behaviours to enable baselining of traffic and events across the network.</p>
<p>(Achieved) IGP 1-  Understanding Normal Behaviour</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) You have a comprehensive monitoring programme established (see C1) such that data regarding the normal operation of your network and information systems is available and can be interrogated to analyse and report upon the status of assets and the nature of interaction between systems and end users to create system baselines of expected behaviours. This exercise typically requires:</p>

	<ul style="list-style-type: none"> <li>• Statistical analysis to establish modes, median and normal operational values for data volumes, users and system utilisation based on.</li> <li>• Techniques and tools for monitoring to detect deviations from normal that would indicate compromise or failure of countermeasures, for example:             <ul style="list-style-type: none"> <li>• Network usage and connections</li> <li>• User access (time of day, frequency and activity)</li> <li>• Protocols in use (known and trusted traffic flows)</li> <li>• Security policy settings (OS status)</li> <li>• Services running</li> <li>• Applications running.</li> </ul> </li> </ul> <p>b) The level of logging and monitoring required to establish and periodically update normal and abnormal activity will vary with systems use and a range of data sets and time periods for baselining may be required.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Documented evidence of practices implemented to achieve this security outcome are available and form part of BAU activities.</p>
<p>(Achieved) IGP 3– Identify and Investigate Abnormal Behaviour</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) You have analysed and learnt from relevant cyber security scenarios (IGP 2) to develop understanding of the common tactics, techniques and procedures leveraged by attackers during security incidents and reasoned how similar incidents could occur on your network and information systems during risk assessment.</p> <p>b) You use this understanding to develop detection capability to identify potential malicious activity on your networks and</p>

	<p>information systems supporting your essential function that is relevant to the specific to the technologies employed (hardware and software systems) and their configuration.</p> <p>c) You use advanced detection algorithms beyond monitoring practices employed in C1 alone to support identification of other, less direct, security event indicators for investigation and follow-up.</p> <p>This typically will involve the centralised correlation of a large number of events allied with behavioural understanding of network and information systems users to reveal unusual behaviour. Often artificial intelligence is used to support this level of discovery alongside attack emulation based on actual network configuration together with vulnerability understanding and system wide events visibility.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Documented evidence of practices implemented to achieve this security outcome are available and form part of BAU activities.</p>
<p>(Achieved) IGP 2 Abnormality Descriptions</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) System abnormality descriptions should be developed from precedent cyber-attacks, related threat intelligence and trusted information sources which consider the nature of vulnerabilities within your networks and information systems and common tactics, techniques and procedures that are used by attackers during intrusion to allow detection of suspicious behaviour which deviates from normal systems behaviour (see Threat Intelligence).</p> <p>Common examples noted include unsolicited traffic flows from devices not previously observed or identifiers associated with people, which may potentially be indicators of compromise (see</p>

	<p>C1.a IGP 8) such as access attempts to information that is not relevant to their role and or responsibilities.</p> <p>b) These descriptions should be informed by your vulnerability assessment prioritise detection to protect critical network assets supporting your essential function (see C1).</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Demonstration of processes used to select, refine and incorporate abnormality descriptions into your security monitoring programme.</p> <p>b) Use of automated tooling, such as breach and attack emulation tooling, where practical to do so. Linking together logical attack path analysis techniques with relevant threat intelligence to develop and refine your detection use cases.</p>
<p>(Achieved)</p> <p>IGP 4</p> <p>Learn and Review</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) The system abnormality descriptions should be updated to reflect changes in your networks, systems, and current threat intelligence (link with C1.d).</p> <p>b) The abnormality descriptions should be reviewed and updated, if required, following events such as, but not limited to:</p> <ul style="list-style-type: none"> <li>• Any internal or relevant external incident</li> <li>• Receipt of new and relevant threat intelligence</li> <li>• Significant changes to the networks and systems supporting your essential function.</li> <li>• Significant changes to operating conditions.</li> </ul>

	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Documented evidence of practices implemented to achieve this security outcome are available and form part of BAU activities.</p>
--	--

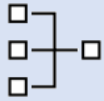
**References and Further Guidance**



- [C.2 Proactive security event discovery - NCSC.GOV.UK](#)
- NIST 800-82 R2 – Appendix G: IR-5 Incident Monitoring, SI-2 Flaw Remediation, SI-4 Information System Monitoring
- IEC62443-1-1 – Section 5.6.5
- ISO27002 – Sections 13.1.1, 14.2.5



C2.b – Proactive Attack Discovery

C2.b – Proactive Attack Discovery	
<p><i>You use an informed understanding of more sophisticated attack methods and of normal system behaviour to monitor proactively for malicious activity.</i></p> <div style="text-align: right;">  </div>	
<b>Not achieved</b>	<b>Achieved</b>
<b>At least one of the following statements is true</b>	<b>All the following statements are true</b>
<p>You do not routinely search for system abnormalities indicative of malicious activity.</p>	<ol style="list-style-type: none"> <li>1. You <u>routinely</u> search for system <u>abnormalities</u> indicative of <u>malicious activity</u> on the networks and information systems supporting the operation of your essential function, <u>generating alerts</u> based on the results of such searches.</li> <li>2. You have <u>justified confidence</u> in the effectiveness of your searches for system abnormalities indicative of malicious activity.</li> </ol>
Ofgem DGE CAF Interpretation	
<p>General commentary</p>	<p>Anomaly detection is the identification of rare events, items, or observations which are suspicious because they differ significantly from standard behaviours or patterns (see C2.a).</p> <p>To observe behaviour OES should adopt a combination of network based, agent based or process data historian or sensor-based anomaly detection techniques to monitor critical assets for unusual behaviour. Further information on monitoring is provided in C1.</p>

	<p>Network-based anomaly detection requires the aggregation of all network traffic into a single collection point. Multiple appliances can also be used with centralised management to collect network traffic data from different zones and sites. Network traffic is examined and compared with a pre-existing baseline, which is assumed to be normal at the time that it is captured. Should the network traffic show deviations from this baseline or show any other types of behaviour considered suspicious or unauthorized, an alert will be generated based on preconfigured parameters.</p> <p>Agent-based anomaly detection combines some of the features of network-based anomaly detection with the nonintrusive monitoring of end points. Agent-based anomaly detection uses distributed software agents installed onto or close to devices, such as servers, HMIs, network switches, and controllers. Agents collect and pre-process device information, such as the use of removable media; logged-in users; ingress/egress traffic; device configurations; process and program details; and device parameters, such as memory, disk, and processor utilisation. The collected information is sent securely to a detection engine. The detection engine alerts on deviations from the preconfigured security policies and pre-existing baselines. The pre-existing baselines are reviewed and accepted as normal at the time that they are captured.</p> <p>Operational historian/sensor-based anomaly detection relies on the collection of sensor data into OT network components, such as operational historians. Because historians are constantly being fed real-time operational data, which has already been configured within operational bounds, or set points, any deviations from these thresholds will produce an alert that can be captured. Typically, this would be considered an operational anomaly.</p>
<p>(Achieved) IGP 1</p> <p>Exception Monitoring</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) The critical networks and systems supporting your essential function are [routinely] monitored and searched for abnormalities indicative of malicious activities.</li> </ul>

	<ul style="list-style-type: none"><li>b) In achieving this outcome, the use of threat hunting techniques, network and host intrusion detection solutions specifically tailored for IT/OT are all considered appropriate.</li> <li>c) When establishing any monitoring programme the use of automation to support continuous monitoring should be considered wherever practical to do so. Dedicated tooling to support detection of anomalies in network behaviour can be far more effective when deployed continuously to monitor network and information systems for unexpected trends or events for analysis and action. However, while capabilities in this area are improving, reducing the effort and cost of deployment, particular for OT systems, deployment at scale can require significant effort to deploy successfully and depending upon circumstances may only offer marginal benefits in terms of risk reduction. Therefore a targeted approach, covering high risk or critical assets, is considered appropriate when seeking to employ exception monitoring at scale. OES should use risk assessment outputs, detailing systems criticality, to identify network assets and systems (for example, control centres) and implement routine monitoring for these critical elements.</li> <li>d) When looking to monitor standalone or isolated high-risk systems it is not always practical, or indeed advisable, to enable remote connect of these systems to a larger network to support remote monitoring, as this may result in an increased attack surface for the isolated asset. In these circumstances you should set out to provide local event capture and routinely export system data to be analysed offline at a defined frequency according to the critical of the asset.</li> <li>e) To support the overall monitoring goals, you should establish and document a use case for abnormality monitoring across NIS critical assets. Providing instruction and guidance to local asset owners through policy documents and templates, to outline expectations for monitoring solutions to be deployed and alternative measures required for abnormality detection where continuous monitoring is considered impractical.</li> <li>f) At minimum, exception monitoring should be carried out on critical assets on a routine basis.</li></ul>
--	---

	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Documented evidence of practices implemented to achieve this security outcome are available and form part of BAU activities.</li> </ul>
<p>(Achieved) IGP 1  Alert Generation</p>	<p>Alert Generation –</p> <ul style="list-style-type: none"> <li>a) Alerts are generated when abnormalities are detected and that these are addressed through the security alert and incident response investigation processes.</li> <li>b) Monitoring systems should be tuned to collect events and generate relevant alerts and to reduce false negatives. These alerts should be investigated through the normal alert investigation processes.</li> <li>c) Follow C1.e Monitoring Tools &amp; Skills and C1.a Monitoring Coverage guidelines for additional details and supporting information.</li> </ul> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Documented evidence of practices implemented to achieve this security outcome are available and form part of BAU activities.</li> </ul>
<p>(Achieved) IGP 2  Detection capability</p>	<p>Confidence in detection capability –</p> <ul style="list-style-type: none"> <li>a) Practice developed for detection aligns with testing and exercising guidance to validate and test both system performance to detect anomalous behaviour but also the coverage.</li> <li>b) You employ advanced tooling such as breach and attack simulation (BAS) to verify your detection coverage running</li> </ul>

	exercises routinely to evolve your capabilities in line which is informed by your use of threat intelligence gathered.
	Where appropriate, Ofgem would expect the following evidence of good practice:  a) See D1.c.

**References and Further Guidance**




- [C.2 Proactive security event discovery - NCSC.GOV.UK](#)
- NIST SP800-82 R2 – Sections 5.16, 5.17, Appendix G: IR-5 Incident Monitoring, SI-4 Information System Monitoring

# Objective D – Minimising the impact of cyber security incidents


## Annex B.4 - Objective D. Minimising the impact of cyber security incidents

*Capabilities exist to minimise the adverse impact of a cyber security incident on the operation of essential functions, including the restoration of those functions where necessary.*

### D1 Response and Recovery Planning

D1 Response and Recovery Planning		
<p><i>There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential functions in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.</i></p>		
Related CAF Objective(s)	Ref	Contributing Outcome
D1 – Response Plan	D1.a	Response Plan
	D1.b	Response and Recovery Plan
	D1.c	Testing and exercising

#### D1.a – Response Plan

D1.a – Response Plan		
<p><i>You have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of your essential function and covers a range of incident scenarios.</i></p>		
<b>Not achieved</b>	<b>Partially achieved</b>	<b>Achieved</b>

At least one of the following statements is true	All of the following statements are true	All the following statements are true
<p>Your incident response plan is not documented.</p> <p>Your incident response plan does not include your organisation's identified essential function.</p> <p>Your incident response plan is not well understood by relevant staff.</p>	<p>1. Your <u>response plan</u> covers your essential functions.</p> <p>2. Your response plan <u>comprehensively</u> covers <u>scenarios</u> that are focused on likely <u>impacts</u> of <u>known and well-understood attacks</u> only.</p> <p>3. Your response plan is <u>understood by all staff who are involved</u> with your organisation's response function.</p> <p>4. Your response plan is <u>documented and shared</u> with all <u>relevant stakeholders</u>.</p>	<p>5. Your incident response plan is based on a <u>clear understanding</u> of the <u>security risks</u> to the networks and information systems supporting your essential function.</p> <p>6. Your incident response plan is <u>comprehensive</u> (i.e., covers the complete <u>lifecycle</u> of an incident, roles and responsibilities, and reporting) and <u>covers likely impacts</u> of both known attack patterns and of possible attacks, previously unseen.</p> <p>7. Your incident response plan is documented and <u>integrated with wider organisational</u> business and <u>supply chain response plans</u>.</p> <p>8. Your incident response plan is <u>communicated</u> and <u>understood</u> by the business areas involved with the operation of your essential functions.</p>

**Ofgem DGE CAF Interpretation**



<p>General Commentary</p>	<p>General Commentary: -</p> <p>a) OES should prepare for disruption to the operation of network and information systems (availability or performance degradation) upon which its essential service relies. Detailing and documenting a comprehensive response and recovery management plan (policy, process and procedures) that shapes the organisational response to incidents, setting out the required actions, responsibilities and practices that individuals across the organisation need to adhere to in order to maintain the risk appetite and cyber security posture the you have set.</p>
---------------------------	--



	<p>b) Whilst more generally cyber security good practice requires consideration of all interruption risks in the context of NIS compliance this applies to networks and information systems which, if disrupted or impaired, would significantly impact the availability of your essential service or challenge your ability to maintain continuity of service in the future.</p> <p>c) While the CAF collection and the language used is primarily aimed at improving cybersecurity, NIS-R relates to any 'incident' that has an impact on a service, where that impact produces a significant disruptive effect. It includes impacts that have 'non-cyber' causes and covers physical and environmental factors too e.g. interruptions to power supplies or natural disasters such as flooding. All of which should be used when considering business interruption.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Referential linking between business interruption risk management activities and activities specifically targeted to address cyber security concerns should be demonstrable through policy, process and overarching governance structures to provide holistic risk management of NIS critical digital assets and supporting systems.</p> <p>Whilst the management of aspects relating to non-cyber related threats may be outside of documentation covering cyber security improvements OES should be able to provide evidence to note its coverage within an overall business risk management framework.</p>
<p>(Partially Achieved)</p> <p>IGP 2</p>	<p>Your response plan [comprehensively] covers [scenarios] that are focused on [likely impacts] of [known and well-understood attacks] only.</p> <p>Ofgem interprets this IGP as follows:</p>

<p>Response Plan</p>	<p>a) You use analysis from open-source reporting, information provided by trusted security advisors and sources detailing precedent cyber incidents as a valuable source of intelligence to understand attacker capabilities and impacts realised during cyber intrusion. This intelligence is used to shape your defensive posture (see CAF objective B), detection capability (see CAF objective C1) and response and recovery plans.</p> <p>You adopt preventative security, including defences that protect from known attacks (e.g., firewalls, policies). Additionally, you have prepared your response to an intrusion and the potential impact this may have on your network and information systems.</p> <p>b) To determine impacts resulting from cyber intrusions, you have knowledge of common tactics, techniques and procedures used by threat actors. You have learnt from precedent cyber-attacks, often presented as overlays to popular frameworks such as MITRE attack for Enterprise and ICS, and have broken down cyber intrusions into multiple stages of attack to understand how an attacker may operate within your environment. This informs your assessment of [likely impacts] that could impact your essential service. You use and apply this understanding during your risk assessment (see CAF outcome A2) and related activities.</p> <p>c) You apply learning from a wide range of scenarios drawn from your threat intelligence sources (see C1.d) which includes, as a minimum, [known and well-understood attacks] scenarios when preparing your response plans. Using outputs from subsequent impact analysis (severity/residual risk) to prioritise development of your response capability.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) You can demonstrate that you have used information within scenarios selected to derive understanding of probable impacts during risk assessment process (see A2). Enabling you to prepare [comprehensive] post breach mitigation actions, allowing you to</p>

	<p>respond and recover in line with your documented business continuity requirements should a compromise occur.</p> <p>b) You have conducted testing and exercising (see D1.c) to demonstrate the effectiveness of your response and recovery plans which covers [known and well-understood attacks] as a minimum.</p>
<p>(Partially Achieved)</p> <p>IGP 3</p> <p>Response Plan is Understood</p>	<p>Your response plan is [understood] by all staff who are involved with your organisation's response function.</p> <p>Ofgem interprets this IGP as follows:</p> <p>a) See IGP 4</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) See IGP 4</p>
<p>(Partially Achieved)</p> <p>IGP 4</p> <p>Sharing Response Plans</p>	<p>Your response plan is [documented] and [shared] with all [relevant stakeholders].</p> <p>Ofgem interprets this IGP as follows:</p> <p>a) You have prepared [documented] information, instruction and guidance relating to your incident response requirements which has been communicated to [relevant stakeholders].</p> <p>b) [relevant stakeholders] have been identified through organisational structures and have been consulted as to the purpose and application (use of) of information, instruction and guidance provided to support response plans derived.</p> <p>c) Stakeholders may be involved to formally approve content developed.</p> <p>d) Information provided has been [shared], this is achieved through a variety of formats e.g. formal training, information cascades, toolbox talks, workshops, testing and exercising programmes and walk throughs and / or formal assignment of reading requirements.</p>

	<p>e) Consideration has been made as to the availability of information, instruction and guidance provided in the event of incident that impacts availability of electronic records e.g., controlled paper copies of material needed by incident responders and related stakeholders is available for use should the need arise.</p> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Documented evidence of practices implemented to achieve this security outcome are available and form part of BAU activities.</p>
<p>(Achieved)  IGP 5  Response Planning</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) OES should prepare and document incident response plans for each NIS critical digital asset based on an [clear understanding] of the risks posed (see A2.a) to the networks and information systems supporting the essential function.</p> <p>b) The requirement for incident response planning should address all in scope systems under NIS (NIS Critical Digital Assets) and may, depending upon the OESs risk tolerance, include additional systems which the OES considers important to the general functioning of the business but falling below its criticality assessment under NIS.</p> <p>c) For NIS critical digital assets any plans developed should be [comprehensively] designed, including an assessment process which identifies all credible incident scenarios that plans need to provide coverage of. This is expected to require an overarching incident response and recovery procedure which:</p> <ul style="list-style-type: none"> <li>• covers the mission and business functions and associated contingency requirements of network and information systems considered essential;</li> <li>• details recovery objectives, restoration priorities, and metrics;</li> </ul>

	<ul style="list-style-type: none"> <li>• identifies roles and responsibilities for nominated individuals and instruction along with communication plans and contact information;</li> <li>• addresses maintaining of essential mission and business functions through contingency planning despite a system disruption, compromise, or failure;</li> <li>• addresses eventual, full system restoration without deterioration of the controls originally planned and implemented.</li> </ul> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Incident response planning is recognised as a formal process which is reflected through the establishment of documented policies, processes and procedures that detail the organisations approach to minimise the impact of cyber security incidents (see principle A1 Governance) and supports the organisations overall approach to managing security of its network and information systems.</p> <p>b) Incident response plans demonstrate clear linkage to the operator’s assessment process to identify both NIS critical digital assets.</p> <ul style="list-style-type: none"> <li>• Establishment and execution of Policy, processes and procedures to detail and document Incident Response and Recovery Plan(s).</li> <li>• Identification of and documenting of the security risks to the organisation. This links to organisations risk management and may be evidenced within A2 (Risk Management) and links to the asset register (see A3) as well as NIS scoping documentation.</li> </ul>
	<p>Ofgem interprets this IGP as follows:</p>

<p>(Partially Achieved)</p> <p>IGP 1</p> <p>(Achieved)</p> <p>IGP 6</p> <p>IRR Plan Coverage</p>	<p>a) Incident response therefore should not be limited to cyber security risks alone (see objective E).</p> <p>b) Incident response plans should address the whole incident management [lifecycle] from preparing to respond to an incident, responding to an incident and post-incident follow-up.</p> <p>c) It is important that organisations develop and implement a co-ordinated approach to incident response. Understanding of organisational missions, business functions, strategies, goals, and objectives for incident response should combine to help determine the structure of incident response capabilities.</p> <p>d) When developing response and recovery requirements the organisation develops incident response plans that provides information, instruction and guidance based upon recognised standards and/or guidelines to inform cybersecurity event and incident response as well as continuity of operations activities.</p> <p>e) Some recommended sources of guidance and advice to support development of incident response and recovery (IRR) policies and processes are:</p> <ul style="list-style-type: none"> <li>• Good Practice Guide for Incident Management. ENISA</li> <li>• CRR Supplemental Resource Guide, Volume 5: Incident Management (cisa.gov)</li> <li>• Incident Handler’s Handbook. SANS</li> <li>• Computer Security Incident Handling Guide. NIST</li> <li>• NCSC Incident Management Guidance</li> </ul>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Review of incident response artifacts to challenge the overall scope and alignment of incident response plans with existing business continuity and disaster recovery activities. This should ensure linking between programmes of activities and risk</p>

	<p>assessment is transparent and the inputs (risk assessment findings) and outputs (procedures and how to documents) are suitable for the essential service being protected.</p> <p>b) Examples of topics to be include within any incident and response and recovery procedures addressed are:</p> <ul style="list-style-type: none"><li>• How and when to initiate incident response and recovery, highlighting events that would activate the plan;</li><li>• Procedures to characterise and classify events as reportable security incidents;</li><li>• Procedures for liaison with the authorities as per the organisation’s Business Continuity Plan (BCP);</li><li>• Procedures to report security incidents to internal stakeholders e.g. senior management;</li><li>• Incremental steps to taken by incident responders, identifying key sources of information, personnel and stages of response and recovery;</li><li>• Triage of incidents to allow prioritisation of response and recovery activities based on business criticality and effected assets;</li><li>• Instruction and guidance for operating in a degraded state, where possible, until normal operational conditions are restored;</li><li>• Information sources and locations of supporting documentation and detailed instruction (manuals, configurations, procedures, vendors contact lists, network diagrams etc.) to enact response and recovery steps;</li><li>• System components restoration order/sequence;</li><li>• Offsite backups recall and restoration procedures;</li><li>• Defining the structure and organisation of the incident response capability;</li><li>• Defining the members and their roles and responsibilities;</li><li>• Details of personnel authorised to allow physical and logical access to sensitive systems;</li><li>• Defining the general methodology to identify, contain, make safe (eradicate), and recover to normal operational conditions;</li><li>• Identifying the information, tools, and resources, including third parties, required to support the plans;</li></ul>
--	---

	<ul style="list-style-type: none"> <li>• Procedures for escalation of incident response;</li> <li>• Internal and external reporting procedures.</li> </ul>
<p>(Achieved)</p> <p>IGP 6</p> <p>IRR Plans consider likely impacts</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) Where security incidents relate specifically to cyber incidents OES should use learning from known cyber incidents coupled with an understanding of tactics, techniques and procedures commonly employed by adversaries allied with their understanding of the vulnerabilities effecting network and information systems to build knowledge of incidents that could occur within the operating environment and the likely impact these could have on the essential service provided.</p> <p>b) Information sources that aid development of this understanding include but are not limited to:</p> <ul style="list-style-type: none"> <li>• Risk assessments;</li> <li>• Past incidents;</li> <li>• Threat intelligence;</li> <li>• Threat modelling;</li> <li>• Vulnerability assessments;</li> <li>• Known attack patterns.</li> </ul> <p>c) For non cyber risks, OES adopt an “all risks” engineering approach to the security of its network and information systems which considers both environmental and physical security aspects within its assessment of probable loss or failure upon which incident response planning is grounded.</p> <p>OES use this combined knowledge and understanding gained to inform the design of its incident response and recovery processes to enable personnel dealing with incidents to respond effectively to the nature of any evolving incidents faced. Predicting escalation stages of known cyber security incidents to allow predetermined mitigations to be enacted when respond to an incident. As well as educating responders on the probable escalation pathways for novel attack scenarios.</p>



	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ol style="list-style-type: none"> <li>a) Demonstration and review of artifacts used to shape the design of the organisations IRR process (risk assessments, past incidents, cyber threat intelligence, vulnerability assessments).</li> <li>b) Review of processes used to link threat intelligence to assets within the organisation including distribution and ingestion of artifacts above alongside technology and people involved.</li> </ol>
<p>(Achieved) IGP 7  Alignment of IRR activities</p>	<p>Ofgem interprets this IGP as follows:</p> <ol style="list-style-type: none"> <li>a) Depending upon the nature of the incident being managed the required activities to deal with security incidents may form part of wider business interruption management activity.</li> <li>b) Incident response plans should therefore be aligned with and linked to other response plans to ensure co-ordinated response across the company and with relevant third parties.</li> <li>c) Business interruption risk management may include but not limited to: <ul style="list-style-type: none"> <li>• Emergency response;</li> <li>• Crisis management;</li> <li>• Business continuity;</li> <li>• Capacity management;</li> <li>• Financial management;</li> <li>• Physical management;</li> <li>• Safety management;</li> <li>• Disaster recovery;</li> <li>• Upstream and downstream supply chain response and continuity plans.</li> </ul> </li> </ol>

	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Example of disaster recovery procedures for selected HW and SW systems from both IT (where relied upon) and OT assets is used to demonstrate and challenge referential linking with wider business continuity activities.</li> <li>b) Policy review and guidance provided to persons with executive function to draft IRR documentation.</li> </ul>
<p>(Achieved) IGP 7 Review of Practices</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) Given the dynamic nature of incident response and recovery activities, plans need to be regularly reviewed and improved upon based on changing business context, newly learned scenarios, revised impact assessment, cyber threat intelligence and learning from related incidents, as well as changes within the operating environment impacting management of the network and information systems comprising the essential function / service.</li> <li>b) IRR plans and related artefacts should link to wider business processes relating to security management, detailing both dependencies upon related lifecycle management activities against which the practice has been drafted providing context for practitioners to support understanding of IRR purpose.</li> </ul> <p>To fulfil this aim policy, procedures and practice derived should be formally integrated into the OESs governance framework for asset management. Ensuring roles and responsibilities for artefacts associated with IRR process are owned and updated through regular review. Providing written evidence of such activities, capturing updates through documented change management and formal review processes.</p>

	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Execution of a documented continuous improvement process (QA) to drive updating and periodic review of practices e.g. production of meeting minutes, documentation reviews, documented interaction and information exchanges to support lifecycle management.</li> </ul>
<p>(Achieved)</p> <p>IGP 8</p> <p>Comms detailing IRR processes</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) Your incident response plan is [communicated] and understood by the business areas involved with the operation of your essential functions.</li> <li>b) Appropriate information to support awareness of incident response and recovery policy, procedures and practice is incorporated into the overall security and awareness programme established by the organisation (see B6).</li> <li>c) Personnel assigned specific roles within incident response plans are provided with necessary information, instruction and training on IRR practices to be implemented to build understanding which is reinforced through testing and exercising (see D1.c) to familiarise practitioners with IRR processes established by the organisation.</li> <li>d) Appropriate summary information of IRR practices is incorporated into support agreements and contracts, where appropriate, to inform 3<sup>rd</sup> parties of the organisation's expectations around IRR activities and any duties they may have to support the organisation with the activity. When appropriate, your incident management process and that of your suppliers provides mutual support in the resolution of incidents (see A4).</li> </ul>

	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Periodic and triggered reviews of policy, processes and procedures developed to support IRR activities including execution.</li> <li>b) Contractual documentation, support agreements or related co-operation agreements with third parties to establish obligations to support (directly or indirectly) incident response activities carried out by the organisation.</li> <li>c) Review of training materials and publications used to communicate requirements for IRR activities.</li> <li>d) Review of roles and responsibilities defined for individuals supporting IRR activities alongside competency profiles.</li> <li>e) Individual training records and competency assessments.</li> </ul>
<p>(Achieved)  IGP 8  Formalised Process for Incident Reporting</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) Establish and maintain an enterprise process for the organisation to enable capture of and reporting of security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported.</li> <li>b) Ensure [incident reporting] processes are publicly available for use by all personnel within the organisation.</li> </ul>

	<p>c) Any process developed should be reviewed periodically, or when significant organisational changes occur that could impact this control.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Establishment and execution of periodic review (passive or active) of documentation supporting incident reporting processes and procedures.</p> <p>b) Evidence of workflow management for incident reporting which may include KPIs, dash boards and management reports relative to size of organisation and complexity of estate being managed.</p> <p>c) Interviews with personnel, including external suppliers and third-party vendors to assess effectiveness of training and awareness for the topic.</p>

**References and Further Guidance**

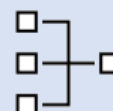


- [D.1 Response and recovery planning – NCSC.GOV.UK](#)
- NIST SP 800-53 Rev. 4 Appendix D: CP-2 Contingency Plan, IR-8 Incident Response Plan, IR-4 Incident Handling
- OG86 – Appendix 2 D1 Response and Recovery Planning
- ISA 62443-2-1:2009 Sections 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8, 4.3.2.5.3, 4.3.4.5.1
- ISO/IEC 27001:2013 Sections A.16.1.6, A.16.1.1, A.17.1.1, A.17.1.2
- ISO 27019 – Section 16
- NIST CSF PR.IP-9

D1.b – Response and Recovery Capability

## D1.b – Response and Recovery Capability

*You have the capability to enact your incident response plan, including effective limitation of impact on the operation of your essential function. During an incident, you have access to timely information on which to base your response decisions.*



Not achieved	Achieved
<p><b>At least one of the following statements is true</b></p>	<p><b>All the following statements are true</b></p>
<p>Inadequate arrangements have been made to make the right resources available to implement your response plan.</p> <p>Your response team members are not equipped to make good response decisions and put them into effect.</p> <p>Inadequate back-up mechanisms exist to allow the continued operation of your essential function during an incident.</p>	<ol style="list-style-type: none"> <li>1. You <u>understand the resources</u> that will likely be needed to carry out any <u>required response activities</u>, and <u>arrangements</u> are in place to make these resources available.</li> <li>2. You understand the <u>types of information</u> that will likely be needed to <u>inform response decisions</u> and <u>arrangements</u> are in place to make this <u>information available</u>.</li> <li>3. Your <u>response team</u> members have the <u>skills and knowledge</u> required to decide on the response actions necessary to limit harm, and the <u>authority</u> to carry them out.</li> <li>4. Key roles are <u>duplicated</u>, and operational <u>delivery knowledge is shared</u> with <u>all individuals</u> involved in the <u>operations and recovery</u> of the essential function.</li> <li>5. <u>Back-up mechanisms</u> are available that can be readily activated to <u>allow continued operation</u> of your essential function (although possibly at a reduced level) if primary networks and information systems <u>fail or are unavailable</u>.</li> <li>6. Arrangements exist to <u>augment your organisation's incident response capabilities</u> with <u>external support</u> if necessary (e.g. specialist cyber incident responders).</li> </ol>

## Ofgem DGE CAF Interpretation



<p>(Achieved)</p> <p>IGP 1</p> <p>Resource</p>	<p>Adequate resources (people, funding, and tools) are provided to support cybersecurity event and incident response as well as continuity of operations activities.</p> <p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) Establishing the required capability and building a team OES may seek to involve dedicated internal capability, third-party vendors, or a hybrid approach.</li> <li>b) The core team should include personnel familiar with the operation and management of the essential functions and the networks and information systems supporting your essential function. Providing context and risk understanding across the wider team.</li> <li>c) To support identification of the [resources] required to carry out any incident response activities OES should designate key personnel with appropriate authority to manage the development and oversight of incident handling policy, processes and procedures across the organisation.</li> <li>d) Personnel assigned responsibilities use learning from internal risk management activities, allied with cyber threat intelligence to identify and make available [resource] (people, funding and tooling) as appropriate for the size and complexity of the organisation to enable incident response to be enacted effectively should the need arise.</li> <li>e) Whilst incident response may leverage internal capability to provide support through business-as-usual activities, resource demands are likely to challenge the ability of personnel to sustain</li> </ul>
--	---

	<p>any support activity required. In most cases incident response will require the establishment of a dedicated support function, often referred to as a Cyber Security Incident Response Team (CSIRT) with its own funding and management.</p> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Evidenced execution of 'key activities such as 'review', 'planning' and 'implementing' procedures/plan/process/policy.</li> <li>b) Participation in internal and external working groups to discuss service continuity for the OES to build confidence in selection of response and recovery scenarios and assumptions held (credibility).</li> <li>c) Evidence of stress testing to challenge response and recovery capability (see D1.c) including review of service level agreements and contractual documentation in conjunction with IRR scenarios and resource projections.</li> <li>d) All personnel involved are provided with the required authority (empowered) to shape the organisations incident response capability in line with their assigned duties.</li> <li>e) Incident response team roles and responsibilities should be formalised (e.g. by inclusion in job descriptions) helping to build identity and allow for personnel development and training against a defined business objective.</li> <li>f) Personnel appointed to support incident response are tasked with the goal of systematically planning for and preparing the organisations response to foreseeable security incidents.</li> </ul>
(Achieved)	Ofgem interprets this IGP as follows:



<p>IGP 2</p> <p>Incident Response Information</p>	<p>a) You understand the types of information that will likely be needed to inform response and recovery decisions and arrangements are in place to make this information available.</p> <p>b) The information required to enable informed response decisions is known and can be made available to the incident response team.</p> <p>c) To ensure that response decisions can be made, appropriate information should be made available to the incident response teams examples of which may include, but is not limited to:</p> <ul style="list-style-type: none"> <li>• Incident response plan and supporting procedures</li> <li>• Interfaces to other supporting teams including detailed workflows to support liaison and stages of response (playbooks)</li> <li>• Monitoring and alert information</li> <li>• Detailed hardware and software engineering information, network diagrams, system descriptions and functional specifications</li> <li>• Asset register with a list of critical sites and systems</li> <li>• Escalation path and authorisation requirements</li> <li>• Supporting tools such as incident management tools etc</li> <li>• External contact information</li> <li>• Communication plans</li> <li>• Criteria to close out incidents and evidence of post incident activities such as “root cause analysis” and “lessons learned” (see later).</li> </ul>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Documented implementation of above artefacts.</p>
<p>(Achieved)</p>	<p>Ofgem interprets this IGP as follows:</p>

<p>IGP 2</p> <p>Informed Response Capability</p>	<p>Informing Response Decisions –</p> <p>a) The process loop of observing, orientating, deciding upon action, and acting may be a period of intensity during incident response. To support personnel respond appropriately in what may be stressful situation, IRR processes should be designed to guide responders through a sequenced programme of activities controlling the flow of information to stakeholders while allowing subject matter experts to focus on their tasks.</p> <p>Documented Triage Process (playbooks) –</p> <p>b) Those identifying a potential incident and those performing triage for an incident, are following a documented and established procedure.</p> <p>c) There should be a defined and documented procedure to enable first responders to triage events. The procedure could include, but not be limited to:</p> <ul style="list-style-type: none"> <li>• Decision trees</li> <li>• Criteria</li> <li>• Incident severity classification</li> <li>• Escalation procedure if additional expertise is required to triage the event.</li> </ul> <p>Scenario specific response playbooks will differ dependent upon the environment being managed. It is expected that response playbooks are logically aligned with Logging and Monitoring processes (see C1 and C2).</p> <p>d) Playbooks are expected to provide sufficient details in response activities, referencing supplementary documentation where necessary, so that errors during their execution or unintended consequences are minimised.</p> <p>e) Playbooks should be kept under review to demonstrate that they remain effective as the environment under management changes and the threat landscape evolves.</p>
--	---

	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Technical review of selected incident response and recovery playbooks and supporting materials referenced.</li> <li>b) Walk through applications and tooling established to support IRR.</li> <li>c) Review of discipline-based development assurance activities undertaken to manage the creation of and management of IRR playbooks.</li> </ul>
<p>(Achieved) IGP 2  Communication</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) IRR should confirm approved communication methods should be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, messaging services.</li> <li>b) OES should consider the possibility that normal channels of communication may not be available therefore planning should include consideration of communication methods should business as usual IT / OT communication systems fail (out of band comms).</li> </ul> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Execution of policy, process and procedures detailing communication arrangements during incident response to highlight contingency planning to mitigate loss of normal communication channels.</li> </ul>
<p>(Achieved)</p>	<p>Response Team Skills –</p>

<p>IGP 3</p> <p>Response Team Skills</p>	<ul style="list-style-type: none"> <li>a) Personnel performing cybersecurity event and incident response as well as continuity of operations activities have the [skills, knowledge and authority] required to perform their assigned responsibilities within the organisations response and recovery policies, processes and procedures.</li> <li>b) OES should provide role-based training, addressing incident management, operational duties, and technical support capability for personnel involved with incident management. Such training should include information, instruction and guidance on organisational policies, procedures and processes involved with incident response and cover the use of tooling and artifacts for the individual roles defined.</li> <li>c) Given the nature of response and recovery activities on IT and OT hardware and software systems this is likely to require specialised training to fully develop skills required for incident response and recovery. OES should ensure that they maintain a thorough understanding of any skills gaps across the organisation based on the technology operated and probable incidents to ensure sufficient resource is available when required.</li> <li>d) To support development of the required pre-requisite skills OES use incident response testing and exercising (see D1.c) to involve personnel directly with incident response activity to maintain awareness and comfort in responding to real-world threats. Exercises devised therefore should be designed to simulate probable incidents so far as is reasonably practical; testing communication channels, decision making, and incident responders technical capabilities using tools and data available to them.</li> <li>e) OES should maintain skills and capability for response roles within a system (preferably a database), to maintain currency (ref B.6).</li> <li>f) Where OES are utilising third party response capabilities, contracts should contain provision of appropriate skills.</li> <li>g) Persons nominated as responsible for incident response and recovery activities require sufficient autonomy to respond in an appropriate</li> </ul>
--	---

	<p>and timely manner to incidents as they evolve. This may require temporary delegations of authority or other measures to be in place to support individuals perform effectively in the role which should be agreed in advance.</p> <p>[NIST SP 800-181] provides guidance on role-based information security training in the workplace.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) The OES has established a documented training and development programme and executes these in line with their periodic roll outs for personnel which drives assessment of competency and provides targets for individuals, teams and functions within the organisation relative to the discipline held.</li> </ul>
<p>(Achieved) IGP 4  Strength and Depth (Team)</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) OES should manage competency of personnel involved with security of network and information systems through a formal development programme which is used to track the strength and depth of coverage across the organisation. Identifying where capability is limited, allowing informed decisions to be made on the organisational structure and develop needs of teams and individuals alike.</li> </ul> <p>Further information on staff awareness and training maybe found in B6.</p> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Review of competency assessments for IRR personnel.</li> <li>b) Organisations training and development programme relative to IRR security roles.</li> </ul>

	<ul style="list-style-type: none"> <li>c) Identification of skills gap, competency gaps and succession planning.</li> <li>d) Training and development is tracked to address competency needs of both individuals and teams relative to business needs.</li> </ul>
<p>(Achieved)</p> <p>IGP 5</p> <p>Back up Mechanisms</p>	<p>Ofgem interprets this IGP as follows:</p> <p>Back-up Mechanisms –</p> <ul style="list-style-type: none"> <li>a) Where the delivery of the essential function may be impacted and service interruption is considered intolerable (see A2.a), the organisation should establish alternative operating mechanisms which can be readily activated to enable continued delivery of the service with minimal disturbance to normal operation.</li> </ul> <p>System Failure or Loss -</p> <ul style="list-style-type: none"> <li>a) Depending upon the criticality of individual functions supporting your essential service the provision of redundant, fail over systems or alternative operating mechanisms (back-up systems) are made available to protect against common system failures or loss. Allowing continued operation, possibly at a reduced level, of your essential service in the event that primary systems are not available.</li> </ul> <p>Incident Response –</p> <ul style="list-style-type: none"> <li>a) During a cyber security incident, where the delivery of the essential function has not been impacted, to reduce the attack surface and prevent lateral movement the organisation may need to limit connectivity and or information exchange between systems to contain an incident. During this period it may be necessary to utilise backup systems to continue service provision using ancillary mechanisms to and from the operational environment. Which may require establishment of additional backup systems as part of business continuity planning.</li> </ul>

	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Criticality assessments / Risk Assessments detailing back up requirements .</li> <li>b) IT/OT architecture to validate levels of redundancy, duplication.</li> <li>c) Application of reference design architectures to build resilience into system designs.</li> <li>d) Routine testing and proving of individual systems to demonstrate serviceability.</li> <li>e) Examination of quality assurance activities to verify and validate discipline practices to build resilience into deployed solutions e.g. Site acceptance tests / Factory Acceptance / Validation plans.</li> </ul>
<p>(Achieved) IGP 6  External Support</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) There are arrangements in place to augment your incident response capability with [external support] where required.</li> <li>b) The incident response plans should identify potential external support to respond to an incident. The external support may include, but is not limited to: <ul style="list-style-type: none"> <li>• National Technical Authority</li> <li>• Specialist cyber security incident response and digital forensics providers</li> <li>• Law enforcement.</li> </ul> </li> <li>c) Where external support is deemed to be required, clear terms of engagement should be drafted to give preference to contending priorities such as maintaining chain of custody or restoration of services.</li> </ul>

	<ul style="list-style-type: none"> <li>d) Special arrangements should be pre-agreed with vendors such as OEMs, to gain commitment during times of incident response, irrespective if there are multiple external entities affected.</li> <li>e) Where external support may be required, you should ensure appropriate contractual arrangements are in place.</li> <li>f) The processes to activate augmentation of the incident response capability should be defined and documented, including both during normal working hours and out-of-hours contact arrangements.</li> </ul>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Contractual documentation and service level agreements.</li> <li>b) Review of processes and procedures to manage initiation of support arrangements.</li> <li>c) Contact list for extended support for selected NIS Assets.</li> <li>d) Documented review of third-party support (technical due diligence) to assess suitability of service capability relative to nature of incident response and recovery capability identified (see previous).</li> </ul>
<p>Additional IGP Emergency communication</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) Incident response and recovery planning. If major disturbances, natural disasters, accidents or any other emergencies occur, or if there is a risk of occurrence thereof, organisations should ensure that essential communication links are maintained with their own emergency staff and/or the emergency staff of other utilities, with essential control systems and with external emergency organisations necessary for the protection and handling of, or recovery from, such incidents.</li> </ul>



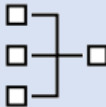

	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Implementation of technical requirements for emergency communication. Periodic review of the effectiveness of support agreements with external support for exercising and continuity planning.</li> <li>b) Linking requirements for response and recovery planning with exercising and testing activities to verify capability. For example demonstration of alternate / fail over comms pathways established to enable communication between emergency response and recovery co-ordinators and effected locations (e.g. use of priority channel mobile network links).</li> <li>c) Exercising of response scenarios at sufficient scale to demonstrate effectiveness of measures enacted for communication with continuous improvement and learning (allies with D1.c).</li> </ul>
--	---

**References and Further Guidance**



- [D.1 Response and recovery planning - NCSC.GOV.UK](#)
- NIST SP 800-53 Rev. 4 Appendix D: CA-2 Security Assessments, CA-7 Continuous Monitoring, PM-14 Testing, Training, and Monitoring, IR-4 Incident handling, IR-5 Incident Monitoring, IR-8 Incident Response Plan, CP-2 Contingency Plan, CP-3 Contingency Training, IR-3 Incident Response Testing, PE-6 Monitoring Physical Access, RA-5 Vulnerability Scanning, SI-4 Information System Monitoring
- ISA 62443-2-1:2009 Sections 4.4.3.1, 4.2.3.10, 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4
- ISO/IEC 27001:2013 Sections A.6.1.1, A.16.1.1, A.16.1.2

*D1.c – Testing and Exercising*

<b>D1.c – Testing and Exercising</b>	
<p><i>Your organisation carries out exercises to test response plans, using past incidents that affected your (and other) organisation, and scenarios that draw on threat intelligence and your risk assessment.</i></p> 	
<b>Not achieved</b>	<b>Achieved</b>
<b>At least one of the following statements is true</b>	<b>All the following statements are true</b>
<p>Exercises test only a discrete part of the process (e.g. that backups are working), but do not consider all areas.</p> <p>Incident response exercises are not routinely carried out or are carried out in an ad-hoc way.</p> <p>Outputs from exercises are not fed into the organisation's lessons learned process.</p> <p>Exercises do not test all parts of the response cycle.</p>	<ol style="list-style-type: none"> <li>1. <u>Exercise scenarios</u> are <u>based on</u> incidents experienced by your and other organisations or are composed using <u>experience</u> or <u>threat intelligence</u>.</li> <li>2. Exercise scenarios are <u>documented</u>, regularly <u>reviewed</u>, and <u>validated</u>.</li> <li>3. Exercises are <u>routinely</u> run, with the <u>findings documented</u> and used to <u>refine</u> incident response <u>plans</u> and <u>protective security</u>, in line with the <u>lessons learned</u>.</li> <li>4. Exercises <u>test all parts</u> of your <u>response</u> cycle relating to your essential functions (e.g. <u>restoration of normal function</u> levels).</li> </ol>
<p><b>Ofgem DGE CAF Interpretation</b></p> 	
<p>General Interpretation</p>	<p>Incident Response and Recovery Exercising –</p> <p style="margin-left: 40px;">a) Carrying out incident exercising, usually through tabletops or simulated incidents, gives an opportunity to assess an organisation's readiness to respond to an attack and continuously improve incident response processes, policies, and procedures.</p>

	<p>b) OES should plan for and conduct routine incident, response exercises and scenarios for the workforce involved in the incident response to Test Efficacy of Response Plans, maintain awareness and comfort in responding to real-world threats.</p> <p>c) Exercises should test communication channels, decision making, and incident responders' strength and depth alongside technical capabilities to use tools and data available to them (see D1.b).</p> <p>d) Where practical, incident response testing can also include a determination of the effects on organisational operations (e.g. reduction in mission capabilities), organisational assets, and individuals due to incident response. With an overall aim of challenging the assumptions made by an OES around capacity (stress testing).</p> <p>e) OES should draw upon the cyber threat intelligence (CTI) gathered to support prioritisation of scenarios.</p> <p>Exercises could include, but are not limited to:</p> <ul style="list-style-type: none"><li>• Orientation/walkthroughs;</li><li>• Table-top exercises;</li><li>• Functional testing of sections of the plans;</li><li>• Full scale test of all elements;</li><li>• Activation of DR (Disaster Recovery) plans;</li><li>• Communications tests – suppliers, emergency services, media, etc.;</li><li>• Any other tests required to meet legal &amp; regulatory requirements.</li></ul> <p>Scope and Coverage –</p> <p>a) Each plan should include the process for Return to Normal Operations after an incident has occurred.</p>
--	--

	<p>Exercises should be used to:</p> <ul style="list-style-type: none"> <li>• Test they are accurate, complete, and effective;</li> <li>• Train the incident response team;</li> <li>• Train new personnel;</li> <li>• Provide refresher training.</li> </ul> <p>b) Records of all testing should be kept for an appropriate period in accordance with legal and regulatory requirements.</p> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Documented evidence of practices implemented to achieve this security outcome are available and form part of BAU activities.</p>
<p>(Achieved)</p> <p>IGP 1</p> <p>Selecting Scenarios</p>	<p>Ofgem interprets this IGP as follows:</p> <p>Identification and Selection of credible scenarios –</p> <p>a) OES should develop exercise [scenarios] to test and exercise incident response and recovery plans, processes and procedures using credible and relevant cyber threat intelligence (see C1.d).</p> <p>b) OES should use a combination of strategic, tactical, and operational intelligence learned about their operating environment, threats, and threat actors to purposefully design a range of tests and exercises that provides appropriate challenge, in terms of scale and complexity (high to low), to the continuity of the essential function relative to the risks being managed by the business.</p> <p>c) OES should draw upon well-known and widely documented precedent cyber security incidents to build understanding of potential impacts resulting from cyber security incidents, translating the tactics, techniques and procedures used by attackers into probable scenarios</p>

	<p>within their own environment against which the organisation can demonstrate its ability to sustain operation and minimise impact.</p> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Review of cyber threat intelligence lifecycle operated to understand information source identified, process for ingestions and methodology applied to convert information collected into meaningful intelligence upon which the organisation can build IRR.</li> <li>b) Calibration of intelligence feeds.</li> <li>c) Review of membership of and active participation in industry forums and expert working groups.</li> <li>d) Incorporation of both asset register and risk registers within design and selection of and conversion of intelligence data into threat intelligence.</li> </ul>
<p>(Achieved) IGP 2  Exercise Documentation</p>	<p>Ofgem interprets this IGP as follows:</p> <p>Maintain Scenarios</p> <ul style="list-style-type: none"> <li>a) OES should apply strategic, tactical, and operational cyber threat intelligence learned (see C1.d), to maintain the relevance of any scenarios devised considering the immediacy of any probable attack scenarios.</li> <li>b) Documented exercise scenarios should be reviewed regularly and updated, if necessary, in accordance with company policy to: <ul style="list-style-type: none"> <li>• Test they are still effective;</li> <li>• Incorporate changes or new threats or experience;</li> <li>• Incorporate changes to contacts, procedures, augmentation, etc.;</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>• Maintain alignment with other relevant plans such as Business Continuity, Crisis Management, etc.</li> </ul> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ol style="list-style-type: none"> <li>a) Review of inputs and outputs used to shape policy, procedures and practices adopted to support incident response and recovery activities relative to testing and exercising undertaken. Examining lifecycle updates to documentation.</li> </ol>
<p>(Achieved)</p> <p>IGP 3</p> <p>Exercise Routines</p>	<p>Ofgem interprets this IGP as follows:</p> <ol style="list-style-type: none"> <li>a) Exercises are routinely scheduled against a published Policy. The Policy could state multiple schedules, for example; new starters, operational personal, management and Executives.</li> <li>b) Exercises of the OES incident response plan(s) for security incidents involving the crucial networks and information systems supporting your essential function should be carried out a frequency (described in the Policy), such that knowledge and understanding of the policies, processes and procedures associated with incident response and, or business continuity activities is sufficient to enable effective implementation when called upon.</li> <li>c) Where OES maintain and operate alternative operational sites such as redundant operations centres, remote control rooms, hot-swap hardware configurations testing, and exercising shall exercise the arrangements to: <ul style="list-style-type: none"> <li>• familiarise personnel with the facility and available resources.</li> <li>• evaluate the capabilities of the alternate site / system to support contingency operations as part of any planned restoration of service.</li> </ul> </li> </ol>

	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Evidence of exercises are maintained on a system (preferably a database), including but not limited to participant roles, scenarios, playbooks utilised, and lessons learned for continuous improvement (ref D.2).</li> </ul>
<p>(Achieved) IGP 3  Learning form Experience</p>	<p>Ofgem interprets this IGP as follows:</p> <p>This security outcome aligns with contributing outcome D2.b (lessons learned).</p> <ul style="list-style-type: none"> <li>a) Findings from testing and exercising of incident response and recovery processes should be documented and reviewed as part of a continuous improvement activity to identify opportunities (see D2.b) to improve organisational (people plant and processes) established to respond and recovery from security incidents.</li> <li>b) In addition, learning from incident response may also provide opportunities to identify improvements to protective security of the networks and information systems supporting your essential function. Helping to identify, protect, detect and respond/recovery more efficiently.</li> <li>c) OES should share experience of incident response and recovery across the sector through active participation in industry working groups and communities of interest. Highlighting good practice and collaborating with industry peers to resolve challenges encountered.</li> </ul>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p>

	<p>a) Documented evidence of practices implemented to achieve this security outcome are available and form part of BAU activities.</p>
<p>(Achieved)  IGP 4  Comprehensive Testing Programme</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) Exercises should test all parts of the incident response lifecycle and the responses appropriate to the exercise’s scenario.</p> <p>b) Processes and procedures for testing and exercising include full recovery and reconstitution of the essential function to a known state as part of incident response and recovery testing and exercising.</p> <p>c) OES should design exercises to test all elements of the incident response lifecycle. Tests do not have to test all elements together. Individual component tests can be designed to provide end-to-end assurance of the incident response lifecycle.</p> <p>d) Where incident response effectiveness is not tested under realistic operational situations (stress tested (see D1.b) i.e., individual elements are proven in isolation, it is important that OES use an alternate (suitable) approach to determine the overall effectiveness of the response capabilities. Helping to identify potential weaknesses or deficiencies.</p> <p>e) For hardware and or software recovery, wherever practical to do so, OES should fully exercise physical recovery steps to verify that recovery of assets can be assured. Testing should be conducted using offline, redundant, or spare hardware and software systems wherever practical and the use of live system avoided.</p> <p>f) For some obsolete systems it may not be possible to effectively test disaster recovery procedures without significant disruption to the essential service to demonstrate serviceability, or without incurring comparable risk of loss when actively testing recovery processes on hardware or software systems due to uncertainty in any programme devised.</p>




	<p>In such circumstances, confidence in the ability to recover these systems should be sought through alternate means. Such as the ability to redeploy alternate resource to provide equivalent service duty using proven (timely) re-engineering capability, migrating the service onto alternate hardware and or software systems for example.</p> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Documenting of disaster response and recovery testing within lifecycle documentation.</li> <li>b) Regular scheduling of testing and exercising across systems or system types.</li> <li>c) Review of information, instruction and training provided to personnel to support incident response and recovery processes.</li> <li>d) Alternate engineering solutions for untested systems, demonstrating capability to migrate failed systems or provide equivalent solutions at scale should the need arise.</li> </ul>
<p>Additional Guidance</p>	<p>Information, Instruction and Training</p> <ul style="list-style-type: none"> <li>a) Incident response training is associated with the assigned roles and responsibilities of organisational personnel to ensure that the appropriate content and level of detail are included in such training.</li> <li>b) For example, users may only need to know who to call or how to recognise an incident; system administrators may require additional training on how to handle incidents; and incident responders may receive more specific training on forensics, data collection techniques, reporting, system recovery, and system restoration.</li> </ul>

## References and Further Guidance

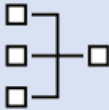


- [D.1 Response and recovery planning - NCSC.GOV.UK](#)
- NIST SP 800-53 Rev. 4 Appendix D: CM-2 Baseline Configuration, CP-4 Contingency Plan Testing, IR-3 Incident Response Testing, PM-14 Testing, Training and Monitoring, CA-2 Security Assessments, CA-7 Continuous Monitoring, PL-2 System Security Plan, RA-5 Vulnerability Scanning, SI-4 Information System Monitoring, CP-2 Contingency Plan, IR-4 Incident Handling, IR-8 Incident Response Plan
- ISA 62443-2-1:2009 Sections 4.3.2.5.7, 4.3.4.5.11, 4.4.3.4, 4.3.4.5.10
- ISA 62443-3-3:2013 SR 3.3 Software Functionality Verification
- ISO/IEC 27001:2013 Sections A.12.1.4, A.17.1.3, A.16.1.6

## D2 Lessons learned

D2 Lessons Learned		
<p><i>When an incident occurs, steps are taken to understand its root causes and to ensure appropriate remediating action is taken to protect against future incidents.</i></p>		
Related CAF Objective(s)	Ref	Contributing Outcome
D2 – Lessons Learned	D1.a	Response Plan
	D2.b	Response and Recovery Plan

### D2.a – Incident Root Cause Analysis

D2.a – Incident Root Cause Analysis	
<p><i>When an incident occurs, steps must be taken to understand its root causes and ensure appropriate remediating action is taken.</i></p>	
	
Not achieved	Achieved
<p><b>At least one of the following statements is true</b></p>	<p><b>All the following statements are true</b></p>
<p>You are not usually able to resolve incidents to a root cause.</p> <p>You do not have a formal process for investigating causes.</p>	<p>1. Root cause analysis is conducted <u>routinely</u> as a key part of your <u>lessons learned</u> activities following an incident.</p> <p>2. Your root cause analysis is <u>comprehensive</u>, covering <u>organisational process issues</u>, as well as <u>vulnerabilities</u> in your <u>networks, systems, or software</u>.</p> <p>3. All <u>relevant incident data</u> is made <u>available</u> to the analysis team to <u>perform root cause analysis</u>.</p>

## Ofgem DGE CAF Interpretation



<p>(Achieved)</p> <p>IGP 1</p> <p>Policy, Procedures and Processes</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) The OES should develop and enact a policy and associated procedures and processes for investigating the root cause of incidents. The scope of which is shaped by requirements further on in this document.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Demonstration of policy, procedure and practice around root cause analysis which is integrated into overall business risk management programme.</p>
<p>(Achieved)</p> <p>IGP 1</p> <p>Routinely Conduct RCA</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) Root cause analysis should be routinely conducted following an incident as part of the incident investigation and response process. It is expected that systematic analysis processes are developed and used to understand the root cause of incidents.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Demonstration of policy, procedure and practice around RCA in practice.</p>

	<p>b) Documentation to capture findings and recommendations from RCA reporting to demonstrate above recommendations.</p>
<p>(Achieved)  IGP 2  RCA Scope</p>	<p>Ofgem interprets this IGP as follows:</p> <p>RCA is comprehensive -</p> <p>a) RCA is expected to but not be limited to:</p> <ul style="list-style-type: none"> <li>• Determine an overall view of the incident lifecycle.</li> <li>• Establish the events that led to an incident occurring, including how long any attacker was present within the environment.</li> <li>• Understand the weaknesses (both technical and non-technical) that were exploited prior to and during the incident.</li> <li>• Understand any human factors that contributed towards the emergence and/or development of the incident.</li> <li>• Assess the efficacy of existing tools or processes designed to detect and prevent security incidents.</li> <li>• Output an action plan, based upon RCA findings, that identifies appropriate enhancements to increase resilience.</li> </ul> <p>b) RCA outputs should be communicated to the business to co-ordinate the financial and resourcing support necessary to manage and close out all the RCA findings.</p> <p>c) When conducting root cause analysis: -</p> <ul style="list-style-type: none"> <li>• the purpose of the analysis should be clear to all stakeholders and just enough to balance lessons learned and not hindering restoration of services.</li> <li>• Where required by law enforcement entities, evidence should be kept in a state where chain of custody is maintained.</li> <li>• Forensic analysis should be compared against last known good states.</li> <li>• You should consider whether the team conducting incident root cause analysis should be independent.</li> </ul>

	<ul style="list-style-type: none"> <li>• You should have call-off contracts with external specialists to lead or augment the root cause analysis team.</li> <li>• OEMs should be involved throughout the process to assist and direct the process where required.</li> </ul> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Established policy, procedure and practice around RCA.</li> <li>b) Review of documentation provided to capture findings and recommendations from RCA reporting to demonstrate above recommendations.</li> </ul>
<p>(Achieved)</p> <p>IGP 3</p> <p>Information Availability</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) All available relevant information should be made available to the team carrying out the root cause analysis.</li> </ul> <p>This should include, but not be limited to:</p> <ul style="list-style-type: none"> <li>• Incident response plan and supporting procedures;</li> <li>• Restoration prioritisation;</li> <li>• Logs, monitoring, and alert information;</li> <li>• System information and network diagrams;</li> <li>• Asset register with a list of critical sites and systems;</li> <li>• Forensic information e.g. device images, memory dumps, packet captures;</li> <li>• Incident handling logs and records;</li> <li>• Physical and logical access records.</li> </ul> <ul style="list-style-type: none"> <li>b) The root cause analysis team may require specialist investigation technologies, techniques, processes to help with the investigation. These should have minimal linkages and connections with company systems until such time that they are required. These</li> </ul>

	<p>are privileged technologies that should not be accessible by others outside of the analysis team.</p> <p>c) The root cause analysis process should ensure a comprehensive analysis.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Documentation review of artefacts associated with incident response and recovery presented for RCA alongside internal/ external processes established.</p>
<p>Achieved IGP 3 RCA Reporting</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) For each incident analysed (beyond trivial), a report should be issued to appropriate stakeholders and authorities detailing the findings and recommendations (supporting D2.b Lessons Learned).</p> <p>b) Where appropriate, an annual report should be produced summarising trends and making further recommendations if appropriate.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a) Review of documentation provided to capture findings and recommendations from RCA reporting to demonstrate:</p> <ul style="list-style-type: none"> <li>• integration of RCA process into business-as-usual activities to manage business activities.</li> </ul>

	<ul style="list-style-type: none"><li>• Assignment of roles and responsibilities to carry out RCA activities through to close out including review of change control applied to systems and documentation.</li></ul>
--	--

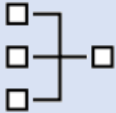

**References and Further Guidance**



- a. [D.2 Lessons learned - NCSC.GOV.UK](#)
- b. ISO 27002 – Section 17.1.3



D2.b – Using Incidents to Drive Improvements


D2.b – Using Incidents to Drive Improvements	
<p><i>Your organisation uses lessons learned from incidents to improve your security measures.</i></p> 	
Not achieved	Achieved
<b>At least one of the following statements is true</b>	<b>All the following statements are true</b>
<p>Following incidents, lessons learned are not captured or are limited in scope.</p> <p>Improvements arising from lessons learned following an incident are not implemented or not given sufficient organisational priority.</p>	<ol style="list-style-type: none"> <li>1. You have a <u>documented incident review process / policy</u> which ensures that lessons learned from each incident are <u>identified</u>, <u>captured</u>, and <u>acted upon</u>.</li> <li>2. <u>Lessons learned</u> cover issues with reporting, roles, governance, skills, and organisational processes as well as technical aspects of networks and information systems.</li> <li>3. You use <u>lessons learned</u> to <u>improve</u> security measures, including updating and retesting response plans when necessary.</li> <li>4. <u>Security improvements</u> identified as a result of lessons learned are <u>prioritised</u>, with the highest priority improvements completed <u>quickly</u>.</li> <li>5. <u>Analysis</u> is fed to <u>senior management</u> and incorporated into <u>risk management</u> and <u>continuous improvement</u>.</li> </ol>
Ofgem DGE CAF Interpretation	
	
<p>General Commentary</p>	<p>Knowledge gained from analysing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents. After completing a root cause analysis, the next step is to implement preventive action. This involves determining what documents should be updated, which processes need to be modified, who needs new</p>

	<p>or re-training, and other considerations. Much of these will be determined by the RCA. The goal being that preventative action taken will ensure the resolved incident cannot reoccur.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Evidence of execution of a documented Incident review process/policy.</li> </ul>
<p>(Achieved) IGP 1  Documented Incident Review Process</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) There should be a formal process that ensures that lessons learned from security incidents involving the networks and information systems supporting your essential function are identified, documented, and acted upon as part of the incident response lifecycle.</li> <li>b) OES should undertake a full analysis of notable incidents (beyond trivial), the causes (inc. exploited system weaknesses), the adequacy of the response plan, restoration activities, personnel competences. Using the analysis as a tool to feedback on incident response and other processes to extract full value from the learnings of the incident.</li> </ul>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Formal inclusion of incident review activities within the IRR policy, processes and procedures.</li> <li>b) Review of RCA execution (sample).</li> </ul>

<p>(Achieved)</p> <p>IGP 3</p> <p>Review Process Scope</p>	<p>Ofgem interprets this IGP as follows:</p> <p>a) The lessons learned process should cover technology, people, processes, and management to inform all aspects of your cyber security, including but not limited to:</p> <ul style="list-style-type: none"> <li>• System configuration</li> <li>• Security monitoring and reporting</li> <li>• Investigation procedures</li> <li>• Containment/recovery strategies</li> <li>• Governance and communication around incident management</li> <li>• Interdependence of systems</li> <li>• Reliability of measures enacted when demanded including backup systems</li> <li>• Understanding of system complexity.</li> </ul> <p>b) The lessons learned exercise should involve participants from all stages of the incident response and to identify opportunities for continuous improvement across people, processes and technology themes in relation to the management of essential networks and information systems supporting your essential function. Enabling:</p> <ul style="list-style-type: none"> <li>• Development of security controls employed to identify, detect, respond and recover to security incidents reducing the likelihood and potential impact of future incidents;</li> <li>• Improvement to the incident response and recovery capability enacted to minimise the impact of security incidents;</li> <li>• challenge the basis of design for critical network and information systems to lower the impact of future incidents should they occur.</li> </ul> <p>c) Carrying out lessons learned also provides an opportunity to gather pertinent information about incident response performance to support co-operation and collaboration with external organisations to correlate and share information on incidents and the effectiveness of measures employed to achieve a cross-sector</p>
--	---

	<p>perspective on incident awareness and more effective incident responses.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Formal inclusion of incident review activities within the IRR policy, processes and procedures.</li> <li>b) Review of RCA execution (sample).</li> </ul>
<p>(Achieved) IGP 4  Prioritising Improvements</p>	<p>Ofgem interprets this IGP as follows:</p> <ul style="list-style-type: none"> <li>a) Improvements identified in the lessons learned should be prioritised and implemented in an appropriate timescale.</li> <li>b) The lessons learned exercise should capture any findings and develop improvement actions, priorities, and assign responsible persons to support remediation or business improvement through a recognised business improvement process to drive improvement in line with business priorities.</li> <li>c) Any changes to incident response and recovery documentation are expected to be managed through change control processes, with any non-approved changes investigated to establish the validity of the changes made and any necessary corrections.</li> </ul> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Review of change management activities associated with IRR RCA findings covering technology, people, processes, and management framework.</li> </ul>

<p>(Achieved)</p> <p>IGP 5</p> <p>Analysis and Reporting</p>	<p>Ofgem interprets this IGP as follows:</p> <ol style="list-style-type: none"> <li>a) Analysis is fed to an accountable board member and incorporated into risk management and continuous improvement.</li> <li>b) Where notable learning has occurred the lessons learned exercise allows formal capture of opportunities for continuous improvement to risk management and incident response capability, processes, and plans. Learning should be supported by data gathered from the operation of incident response processes.</li> <li>c) Analysis of the type, frequency, and nature of incidents experienced and key performance indicators from incident response processes should be used to support overall assessment of incident response and recovery capability which can be made available to senior management. Allowing an informed view to be drawn on the success or otherwise of incident response and recovery capabilities.</li> <li>d) Analysis should include, but not be limited to, data such as:             <ul style="list-style-type: none"> <li>• Trends of incident type that highlight areas of weakness.</li> <li>• Frequency of incidents (e.g. heightened relative frequency may indicate that the organisation is being actively targeted).</li> <li>• Commonalities between separate incidents, indicating potential common attack vectors / vulnerabilities.</li> <li>• Statistical anomalies relating to certain assets / asset types affected by incidents.</li> <li>• Mean time taken to detect incident.</li> <li>• Mean time taken to respond to incident.</li> <li>• Mean time take to recover from an incident.</li> <li>• 3rd party support responsiveness against service level agreements.</li> </ul> </li> </ol> <p>Ultimately, it is expected that the data analysed as part of any response is converted into actionable improvement activities and integrated into cyber resilience enhancement plans when presented. For example, if a certain asset type is the common</p>
--	---

	<p>source of an incident, it would be expected that the specific characteristic of the asset that causes susceptibility to attack is understood and addressed.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Review of IRR management database.</li> <li>b) Review of IRR reports produced for key stakeholders.</li> </ul>
<p>(Achieved) IGP 5  Reporting</p>	<p>Ofgem interprets this IGP as follows:</p> <p>Maintain Contact Information for Reporting Security Incidents</p> <ul style="list-style-type: none"> <li>a) Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant Government departments, vendors, and Information Sharing and Analysis Centre (ISAC) partners.</li> </ul> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a) Review of identified stakeholders and contact identified.</li> <li>b) Formal inclusion of reporting activities within the IRR policy, processes and procedures.</li> </ul>
<p><b>References and Further Guidance</b></p> <div style="text-align: right;">  </div>	
<ul style="list-style-type: none"> <li>• <a href="#">D.2 Lessons learned - NCSC.GOV.UK</a></li> <li>• IEC 62443/ISA99 2-1 – Section A.3.4.5.4</li> <li>• IEC 27002 – Section 16.1.6</li> </ul>	

- NCSC D2 Lessons learned

# Ofgem Supplementary Objective – Physical Security, Principles and Guidance



## Annex C – Ofgem Supplementary Objective – Physical Security, Principles and Guidance

### Annex C.1 - Objective E: Protecting against non-cyber risks

*The risks of physical events leading to adverse effects on network and information systems are understood and systematically managed.*

DSIT's interpretation of OES' NIS security duties includes taking non-cyber measures to manage the risk of 'physical events that might have an adverse effect on networks and information systems'<sup>46</sup>. DESNZ's NIS Policy Guidance re-iterates DSIT's interpretation and requires an OES to 'identify and manage other'<sup>47</sup> security issues in an appropriate and proportionate manner'<sup>48</sup>.

The NCSC have produced the CAF collection to assist organisations improve the security of network and information systems. The CAF collection focuses on cyber-based threats to networks and covers supply chain and personnel risks. However, the CAF's treatment of risks arising through physical events is limited<sup>49</sup>.

The aim of this supplementary security objective is to detail Ofgem's expectations regarding the management of physical events that might have an adverse network and information systems that are in an OES' NIS scope. Ofgem have produced this security objective in the same format as NCSC's CAF security objectives, the intent is that this will lead to a consistent approach in the self-assessment of cyber and physical security objectives.

Ofgem intend that their physical security objective is used as a supplement to the CAF and refer to it as Objective E. Objective E specifies security outcomes relating to 2 distinct categories of physical risk. Principle E1 relates to the risks presented by malicious threat actors gaining physical access to the components of network and

---

<sup>46</sup> DCMS, Security of Network and Information Systems, Guidance for Competent Authorities, dated Apr 2018.

<sup>47</sup> Where 'other' refers to other than cyber security.

<sup>48</sup> DESNZ, Policy Guidance for the Implementation of the Network and Information Systems Regulations for the Energy Sector in Great Britain.

<sup>49</sup> This was intentional, as the provision of this advice is outside of the remit of NCSC. Responsibility for the provision of this advice rests with the Competent Authority (CA).

information systems. Principle E2 relates to non-malicious risks such as those caused by environmental hazards and accidents.

## **Principle E1: Physical security of network and information systems**

Providing physical security measures that will reduce the risk of malicious actors gaining physical access to components of network and information systems.

### **E1: Physical security of network and information systems**

**Principle**

*Appropriate and proportionate physical security measures are in place to protect network and information systems from unauthorised physical access and tampering.*



**Description**

Effective security of network and information systems requires that components of the networks are protected against the threat of unauthorised physical access. The risks associated with unauthorised physical access are numerous and include, but are not limited to, attackers directly connecting to device ports for the purpose of downloading malware or extracting data, and attackers using plant HMIs to change system parameters.

**Guidance**

Holistic cyber security requires an integrated approach. Physical and cyber security management systems must complement each other, and security teams must work together closely to manage those elements of the security systems that overlap. Examples of these overlaps include the cyber security of the security systems used to enforce physical security (such as access control systems and video management systems) and the identification of

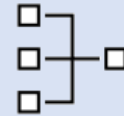
zones within facilities that contain critical network components that require enhanced physical security.

Objective E relates only to the physical security of the components of the network and information systems on which the essential function relies. The physical security of the generation, transmission and distribution equipment (e.g. turbines, conductors and transformers) that the network and information systems support are not covered within this guidance.

*E1.a – Governance and risk management processes relating to physical security risks*

**E1.a Governance and risk management processes relating to physical security risks.**

*You manage your physical and cyber security risks in an integrated manner and your physical and cyber-security risk management processes are mutually supporting.*



Not achieved	Achieved
<p><b>At least one of the following statements is true</b></p> <p>Your organisation does not have a board-level individual who has overall accountability for physical security of sites hosting network and information systems.</p> <p>Your organisation has not conducted a risk assessment that takes account of the risks of unauthorised physical access to network and information system components across your sites.</p> <p>Your organisation does not have a security management system with an explicit objective of reducing the risk of unauthorised access to network and information systems.</p>	<p><b>All the following statements are true</b></p> <ol style="list-style-type: none"> <li>1. The physical security of your network and information systems is delivered via appropriate organisational structures, well-defined responsibilities and accountabilities and suitably qualified and experienced personnel. These structures are designed to ensure that physical and cyber security policies and plans are mutually supporting/complimentary.</li> <li>2. Your management systems (cyber or physical or both) include security objectives relating to the physical security of your network and information systems.</li> <li>3. You have identified and registered all facilities, and specific zones within those facilities, that require physical security control measures for the purpose of securing network and information systems.</li> <li>4. Your physical security risk assessments take account of the potential impacts resulting from unauthorised physical access to network and information system components. Your investment in physical security measures reflects these potential impacts.</li> <li>5. Your organisation has made use of NPSA guidance to help inform its view of appropriate and proportionate physical security measures for its sites.</li> </ol>

## Ofgem DGE CAF Interpretation



<p>(Achieved)</p> <p>IGP 1</p>	<p>Ofgem intends that this IGP will:</p> <ol style="list-style-type: none"> <li>a. guide OES to develop the structures and teams to ensure that the physical security of network and information systems is comprehensively managed. This IGP aims to avoid the tendency for physical security of network and information systems to be managed on an ad-hoc basis by IT/OT staff, it encourages OES to use the expertise of their existing physical security staff to manage physical aspects of NIS security. Mutually supporting/complimentary physical and cyber security policies and plans describes a situation in which OES have considered how physical security controls can be used to augment cyber controls, or to provide compensating controls, where required.</li> <li>b. avoid situations in which the physical security of network and information systems is not considered due to gaps between physical and cyber security teams.</li> </ol>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ol style="list-style-type: none"> <li>a. A master list of security roles and responsibilities that is maintained as part of the security management system (this is often achieved in a RACI table format).</li> </ol>
<p>(Achieved)</p>	<p>Ofgem intends that this IGP will avoid situations in which the physical security of network and information systems are not considered due to gaps between physical and cyber security teams.</p>

<p>IGP 2</p>	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a. References to the physical security of network and information systems within one, or both, of the cyber and physical security management systems.</li> </ul>
<p>(Achieved)</p> <p>IGP 3</p>	<p>Ofgem intends that this IGP will guide OES toward identifying and recording all those facilities that contain network and information systems that are in their NIS scopes. These facilities may include manned and unmanned sites. The register should also identify any zones/areas within these facilities that require enhanced physical access control measures (such as control rooms and equipment rooms).</p> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a. Demonstration that the OES is aware of all the facilities that contain network and information systems that are in NIS scope.</li> <li>b. Demonstration that the OES is aware of the zones/areas within its facilities that require enhanced physical access control measures (examples may include control rooms and equipment/server rooms).</li> </ul>
<p>(Achieved)</p> <p>IGP 4</p>	<p>Ofgem intend that this IGP will:</p> <ul style="list-style-type: none"> <li>a. guide OES to take account of the risk posed by physical security breaches and to provide network and information systems with a level of physical protection that is proportionate to the risk.</li> </ul>

	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a. risk assessments that document physical security risks against network and information systems and NIS improvement plan actions that respond to those risks that require treatment.</li> </ul> <p>Ofgem accepts that many OES will conduct these risk assessments by facility type/group, rather than by individual facility. This is because of the number of remote facilities involved and that risks are may be common between facilities within the same type/group.</p> <p>.</p> <p>OES are reminded that the protective security needs of different types of sites will vary significantly and that it may be appropriate and proportionate to afford a lower level of physical security to less critical sites.</p>
<p>(Achieved)</p> <p>IGP 5</p>	<p>Ofgem intends this IGP to:</p> <ul style="list-style-type: none"> <li>a. guide OES to make use of NPSA guidance where appropriate and to liaise with NPSA security advisors. In the case of OES with designated CNI sites, OES should ensure that they have established and maintain contact with a NPSA security advisor. In the case of OES who do not have designated CNI sites, liaison should be achieved through involvement with the relevant NPSA sector forum. OES should request access to NPSA’s extranet to provide them with access to detailed guidance on physical security measures.</li> </ul> <hr/> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a. Evidence of liaison with NPSA advisors.</li> </ul>

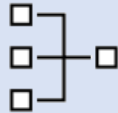

## References and Further Guidance




1. [www.npsa.gov.uk](http://www.npsa.gov.uk)



*E1.b – Designing and implementing physical security controls*

<b>E1.b – Designing and implementing physical security controls</b>	
<p>You have referenced relevant NPSA physical security guidance when designing and implementing controls</p> <div style="text-align: right;">  </div>	
<b>Not achieved</b>	<b>Achieved</b>
<b>At least one of the following statements is true</b>	<b>All the following statements are true</b>
<p>You have not referred to any NPSA physical security guidance when implementing controls.</p>	<ol style="list-style-type: none"> <li>1. You reference relevant NPSA guidance when designing and implementing new physical security controls.</li> <li>2. You have identified any IT networked physical security systems that your cyber security management system relies on and have included these systems as part of your NIS scope.</li> <li>3. Projects to implement new IT networked physical security systems employ devices that are assured under the Cyber Assurance of Physical Security Systems (CAPSS) scheme<sup>50</sup>, or recognised equivalent.</li> </ol>
<b>Ofgem DGE CAF Interpretation</b>	
	
<p>(Achieved)</p> <p>IGP 1</p>	<p>Ofgem intends this IGP to:</p> <ol style="list-style-type: none"> <li>a. guide OES toward making full use of NPSA physical security advice and guidance. Doing so will assist in the implementation of appropriate and proportionate security controls. NPSA’s physical security guidance can be found on the NPSA internet and extranet sites at the ‘Advice’ tab.</li> </ol>

<sup>50</sup> CAPSS is a joint NPSA and NCSC scheme.

	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a. Confirmation that the OES is aware of, and making use of, relevant NPSA advice and guidance.</li> </ul>
<p>(Achieved)  IGP 2</p>	<p>Ofgem intends this IGP to:</p> <ul style="list-style-type: none"> <li>a. ensure that an OES' NIS scope is comprehensive and takes account of the essential service's reliance on the networked physical security systems that are used to protect it.</li> </ul> <p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <ul style="list-style-type: none"> <li>a. Inclusion of any network and information systems that provide physical security functionality that the essential service relies upon.</li> </ul>
<p>(Achieved)  IGP 3</p>	<p>Ofgem does not have any additional interpretation for this security outcome.</p>
<p><b>References and Further Guidance</b></p> <div style="text-align: right;">  </div>	
<p>1. <a href="http://www.npsa.gov.uk">www.npsa.gov.uk</a></p>	

## Principle E2: Broader network and information systems resilience risks

Managing the broader risks to network and information system security. In this context, 'broader risks' refers to those risks arising from non-malicious hazards.

### E2: Broader Resilience Risks

**Principle**

*Proportionate and appropriate control measures are in place to manage the risk to network and information system security from risks arising from non-malicious hazards.*

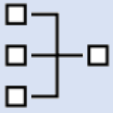


**Description**

*The security of network and information systems relies on the control of risks arising from both malicious and non-malicious hazards.*

*Non malicious hazards, such as fire and accidental damage, can have significant impacts on the delivery of the essential function and must be controlled. Risk assessments are required to identify and prioritise the potential for accidents, failures and environmental factors to adversely impact the operation of network and information systems. Adequate controls are then required to reduce these risks to a level that is appropriate and proportionate.*

E2.a – Broader resilience risks

<b>E2.a – Broader resilience risks</b>	
<p><i>Proportionate and appropriate control measures are in place to manage the risks to network and information system security arising from non-malicious hazards.</i></p> 	
<b>Not achieved</b>	<b>Achieved</b>
<p><b>At least one of the following statements is true</b></p> <p>Your network and information system resilience risk assessments are limited to cyber and physical security risks and do not consider broader resilience risks.</p>	<p><b>All the following statements are true</b></p> <p>1. Your risks assessment take account of the risks to NIS system that are associated with accidents, failures and environmental factors. You are actively and effectively controlling all risks.</p>
<b>Ofgem DGE CAF Interpretation</b>	
<p>(Achieved) IGP 1</p>	<p>IGP 1. Ofgem intends this IGP to:</p> <p>a. direct OES to identify risks to the network and information systems other than just cyber and physical tampering. These could include, but are not limited to the following operational risks:</p> <ul style="list-style-type: none"> <li>• loss of power</li> <li>• hardware failure and long lead-times for replacements</li> <li>• software failures</li> <li>• hardware failure and inability to procure replacements due to obsolescence</li> <li>• accidental physical damage, e.g. severed network cables</li> <li>• environmental hazards such as fire and flooding. In this context, flooding refers to the risk of flooding caused by malfunction of plant and services <b>on</b> the site (e.g.</li> </ul>

	<p>inadvertent activation of fire suppression system), it does not take account flooding <b>of</b> the site.</p> <p>b. direct OES to apply appropriate and proportionate controls.</p>
	<p>Where appropriate, Ofgem would expect the following evidence of good practice:</p> <p>a. risk assessments that document broader resilience risks to network and information systems and NIS improvement plan actions that respond to those risks that require treatment.</p>

## References and Further Guidance



1. [www.npsa.gov.uk](http://www.npsa.gov.uk)

## Annex D – Representative Scopes

### Background

Ofgem requires OES to compile NIS system scopes, and to submit them as part of their NIS Self-Assessment submissions<sup>51</sup>. An OES' NIS scope details those network and information systems that are used for the **provision** of the essential service, or upon which the essential service **relies**.

A set of seven scoping principles are defined in Ofgem's NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in GB v2.0', dated Apr 2022 [Ofgem's NIS Guidance, Apr '22]. The guidance states that Ofgem expects OES to follow the seven principles when compiling their NIS scopes.

Ofgem facilitated a series of NIS scoping workshops in Jan/Feb '23 with the aim of improving the degree of standardisation between the NIS scopes of OES operating in the same sub-sectors<sup>52</sup>.

The scoping workshops discussed the existing seven scoping principles,<sup>53</sup> and built upon them by agreeing a set of functions that were critical for all OES delivering essential services. These functions were then used to define agreed and standardised functional viewpoints<sup>54</sup> for each of the sub-sectors.

The functional viewpoints were then populated with the system types<sup>55</sup> that Ofgem would **typically** expect to see in a NIS scope. Use of the word **typically** indicates that some of the system types will not be relevant to all OES. Ofgem identified relevant system types by referencing and aggregating the OES' 2022 self-assessment scope lists. The completed functional viewpoints were then reviewed and agreed by OES and the viewpoints are included as embedded documents to this Annex.

---

<sup>51</sup> This requirement is explained in Ofgem's Apr '22 NIS guidance.

<sup>52</sup> Scoping workshops were held for the Electrical Generation, Electrical Distribution, Gas Distribution & Transmission and Electrical Transmission and Interconnector sub-sectors.

<sup>53</sup> The seven scoping principles have not been changed in any way. The benefit of the workshops was to improve and standardise the interpretation of the existing principles.

<sup>54</sup> The production and description of functional viewpoints is a requirement specified in Ofgem's Apr '22 NIS Guidance.

<sup>55</sup> The systems are described as system types rather than by proprietary system names. This is intended to keep descriptions generic and relevant to all OES.

## Aim

The aim of the functional viewpoints is to increase the degree of standardisation between OES' NIS scopes, and to provide Ofgem with higher levels of assurance that OES' NIS scopes comprehensively capture the network and information systems that are used for the **provision** of essential services, or upon which essential services **rely**.

## Use of Functional Viewpoints

Ofgem expects functional viewpoints to be used as follows:

By OES to:

- Validate their NIS scope. OES should cross-reference the typical system types listed in the sub-sector functional viewpoint, against their own NIS scope. Where an OES identifies systems in the functional viewpoint that aren't included in its own scoping list, it should make one of the following determinations:
  - The system type in question should be added to the OES' own NIS scope.
  - In the context of the OES' own operating environment, the system type isn't used for the provision of the essential service, nor is it relied upon by the essential service. Consequently, it is not included in the OES' NIS scope<sup>56</sup>.

By Ofgem to:

- Standardise Ofgem's Own Understanding of Typical OES Scopes. The functional viewpoints will be used as a reference by Ofgem's Cyber Regulatory Team. They will help to improve the consistency of advice, guidance, and direction that Ofgem issues to OES.

## Customer Impact Thresholds and Site Criticality

The use of customer impact thresholds, and determination of site criticality, has been identified as a key point of divergence between many OES' NIS scopes.

---

<sup>56</sup> There is no requirement to document these exclusions, however, OES are to be aware that Ofgem representatives may enquire as to the justification for exclusions during inspection and advisory activity.

The following scoping principles clarify Ofgem's position:

- Bullet Point 6, Ofgem's NIS Guidance Apr '22 - *'For those OES that are designated as a result of exceeding a cumulative or total capacity threshold requirement under Schedule 2 of the NIS Regulations, all sites and systems relevant to meeting said threshold should be detailed with the NIS scope'.*
- Bullet Point 7, Ofgem's NIS Guidance Apr '22 - *'OES must not use the incident reporting thresholds, that they are to have regard to when notifying incidents under Regulation 11, when defining the functions, sites or network and information systems within their NIS scope'.*

OES should start from the basis that all network and information systems used for the provision of the essential service, or upon which the essential service relies are to be included in scope, regardless of the number of consumers that are served. The following justification explains this position:

- It is acknowledged that individual network and information systems, or components thereof, located at the extremities of networks may individually serve a relatively small number of consumers. However, it is typically the case that these devices are built and configured to a common standard (a gold-build) and are networked. Meaning that it is feasible that a single cyber event could simultaneously impact multiple devices<sup>57</sup>.

Some OES have used impact thresholds in the order of 1000 consumers to exclude specific instances of network and information systems at the extremities of their networks. In these cases, where impacts are in the order of circa 1000 consumers, and in which specific claims and arguments have been substantiated, Ofgem has accepted the use of such a threshold.

## **Time to Impact**

The use of 'time to impact' thresholds has been identified as a key point of divergence between many OES' NIS scopes.

The following scoping principles clarify Ofgem's position:

---

<sup>57</sup> This risk was identified by a number of OES in their NIS Self-Assessment Risk Assessments.



- Bullet Point 5, Ofgem’s NIS Guidance Apr ’22 – *‘Network and information systems related to maintenance, integration, security, or similar activity, that might not necessarily be required during immediate essential service operations but are required for the long-term provision of the essential service, should be included withing the NIS Scope’<sup>58</sup>.*

OES should not only consider cyber events that lead to a direct and immediate loss of the essential service. They should also consider events that may degrade their ability to enact Business Continuity Plans, or otherwise minimise the impact of cyber events and incidents<sup>59</sup>. They should also consider risks relating to the loss of integrity of data that may lead to delayed impacts to the essential service.

The following justification explains this position:

- OES are expected to act in accordance with the legislation and make decisions based on the potential for impact to the ‘maintenance of critical societal or economic *activities*’<sup>60</sup>. Neither the legislation, nor or any subsequent guidance, makes a distinction between whether the impact is immediate or delayed; the sole consideration is maintenance. The following scenarios have been used by OES in the DGE sector to describe how they have taken delayed impacts into account when defining their scope.
  - OES’ have included warehousing and stores systems in their NIS scope. Their rationale was that if they were to lose access to these systems in the aftermath of a storm, they would be unable to locate and distribute the stores needed to enable rapid restoration of their network. This reasoning takes account of the fact that a cyber incident may be synchronised with a storm event, to achieve maximum disruption.
  - OES’ have described how they had included customer fault reporting systems and ERP work/task management tooling in their NIS scope. Their rationale was that if they were unable to identify the location of outages, and deploy field engineers, they would be unable to respond and enable rapid restoration of their network. This reasoning takes account of the fact that a cyber incident may be multi-stage. Early stages may aim

---

<sup>58</sup> As detailed at bullet point 5 of the scoping principles defined in Ofgem’s Apr ’22 NIS Guidance

<sup>59</sup> The requirement to for OES to take appropriate and proportionate measures to minimise the impact of incidents is detailed as a security duty under clause 10 (2) of the NIS regulations.

<sup>60</sup> Clause 1(2) of The Network and Information Systems Regulations 2018

to cause disruption the network, later stages may aim to limit the OES' ability to respond<sup>61</sup>.

- OES' have described how they had included Enterprise Content Management Systems in their NIS scope. Their rationale was that loss of availability or integrity of this data would significantly impair their ability to re-configure and restore devices in the aftermath a cyber event.

## **Functional Viewpoints**

### **Electricity Transmission, ESO and Interconnector**

Available on request

### **Gas Transmission, Distribution and Interconnector**

Available on request

### **Electricity Distribution**

Available on request

### **Generation**

Available on request

---

<sup>61</sup> This strategy was employed during the 2015 cyber-attack against the Ukrainian power grid.

## Annex E – Cyber Security Framework Mappings

### Annex E-1 – NIST CSF to CAF

Many OES have previously adopted the NIST Cybersecurity Framework (CSF)<sup>62</sup> as a means for guiding cybersecurity activities and considering cybersecurity risks. The Framework consists of five concurrent and continuous Functions — Identify, Protect, Detect, Respond, and Recover — for presenting industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organisation. When considered together, much like the CAF, these functions provide a high-level, strategic view for cybersecurity risk management. The Framework further identifies underlying key Categories and Subcategories for each Function and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory. Table 3 below maps the CSF functions to the NCSC CAF contributing outcomes.

Table 3 – Mapping of NIST Cyber Security Framework to CAF

NIST Cyber Security Framework				
Function	Category	Subcategory	NIST References	CAF Contributing Outcome
<b>IDENTIFY (ID)</b>	<b>Asset Management (ID.AM):</b> The facilities (data, personnel, devices,	<b>ID.AM-1:</b> Physical devices and systems within the organisation are inventoried	CM-8, PM-5	A3.a

<sup>62</sup> Cybersecurity Framework | NIST - <https://www.nist.gov/cyberframework>

<p><b>Business Environment (ID.BE):</b> The OES mission, activities, stakeholders, and objectives are understood and prioritised. Providing key direction to cybersecurity roles, responsibilities, and risk management</p>	<p>systems,) that enable the OES to operate successfully are identified and managed proportionately relative to importance and risk.</p>	<p><b>ID.AM-2:</b> Software platforms and applications within the organisation are inventoried</p>	<p>CM-8, PM-5</p>	<p>A3.a</p>
	<p><b>ID.AM-3:</b> Organisational communication and data flows are mapped</p>	<p>AC-4, CA-3, CA-9, PL-8</p>	<p>B3.a</p>	
	<p><b>ID.AM-4:</b> External information systems are catalogued</p>	<p>AC-20, SA-9</p>	<p>A3.a</p>	
	<p><b>ID.AM-5:</b> Resources (e.g. hardware, devices, data, time, personnel, and software) are prioritised based on their classification, criticality, and business value</p>	<p>CP-2, RA-2, SA-14, SC-6</p>	<p>A2.a</p>	
	<p><b>ID.AM-6:</b> Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g. suppliers, customers, partners) are established</p>	<p>CP-2, PS-7, PM-11</p>	<p>A1.b</p>	
	<p><b>ID.BE-1:</b> The organisation’s role in the supply chain is identified and communicated</p>	<p>CP-2, SA-12</p>	<p>None</p>	
	<p><b>ID.BE-2:</b> The organisation’s place in critical infrastructure and its industry sector is identified and communicated</p>	<p>PM-8</p>	<p>None</p>	
	<p><b>ID.BE-3:</b> Priorities for organisational mission, objectives, and activities are established and communicated</p>	<p>PM-11, SA-14</p>	<p>A1.a</p>	
	<p><b>ID.BE-4:</b> Dependencies and critical functions for delivery of critical services are established</p>	<p>CP-8, PE-9, PE-11, PM-8, SA-14</p>	<p>A2.a</p>	

<p><b>Governance (ID.GV):</b> The instruments (policies, procedures, and processes) to manage and monitor OES' compliance, risk and operational needs are understood and detail the cybersecurity risk to management.</p> <p><b>Risk Assessment (ID.RA):</b> OES acknowledges the cybersecurity risk to its operations (such as mission, image, or reputation), organisational assets, and individuals.</p>	<p><b>ID.BE-5:</b> Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)</p>	CP-2, CP-11, SA-13, SA-14	B5.a, B5.b
	<p><b>ID.GV-1:</b> Organisational cybersecurity policy is established and communicated</p>	-1 controls from all security control families	B1.a, B1.b
	<p><b>ID.GV-2:</b> Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners</p>	PS-7, PM-1, PM-2	A1.b
	<p><b>ID.GV-3:</b> Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed</p>	-1 controls from all security control families	B1.a, B1.b
	<p><b>ID.GV-4:</b> Governance and risk management processes address cybersecurity risks</p>	SA-2, PM-3, PM-7, PM-9, PM-10, PM-11	A2.a
	<p><b>ID.RA-1:</b> Asset vulnerabilities are identified and documented</p>	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5	B4.d
	<p><b>ID.RA-2:</b> Cyber threat intelligence is received from information sharing forums and sources</p>	SI-5, PM-15, PM-16	B5.a, C1.d
	<p><b>ID.RA-3:</b> Threats, both internal and external, are identified and documented</p>	RA-3, SI-5, PM-12, PM-16	A2.a
<p><b>ID.RA-4:</b> Potential business impacts and likelihoods are identified</p>	RA-2, RA-3, SA-14, PM-9, PM-11	A2.a	

	<p><b>Risk Management Strategy (ID.RM):</b> OES' priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.</p>	<p><b>ID.RA-5:</b> Threats, vulnerabilities, likelihoods, and impacts are used to determine risk</p>	RA-2, RA-3, PM-16	A2.a
		<p><b>ID.RA-6:</b> Risk responses are identified and prioritised</p>	PM-4, PM-9	A2.a
		<p><b>ID.RM-1:</b> Risk management processes are established, managed, and agreed to by organisational stakeholders</p>	PM-9	A2.a
	<p><b>Supply Chain Risk Management (ID.SC):</b> OES uses third party risk management techniques when understanding supply chain risk. OES has established and implemented the processes to manage supply chain risks.</p>	<p><b>ID.RM-2:</b> Organisational risk tolerance is determined and clearly expressed</p>	PM-9	A1.a, A2.a
		<p><b>ID.RM-3:</b> The organisation's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis</p>	SA-14, PM-8, PM-9, PM-11	A2.a
		<p><b>ID.SC-1:</b> Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organisational stakeholders</p>	SA-9, SA-12, PM-9	A4.a
		<p><b>ID.SC-2:</b> Suppliers and third-party partners of information systems, components, and services are identified, prioritised, and assessed using a cyber supply chain risk assessment process</p>	RA-2, RA-3, SA-12, SA-14, SA-15, PM-9	A4.a
		<p><b>ID.SC-3:</b> Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organisation's cybersecurity program and Cyber Supply Chain Risk Management Plan.</p>	SA-9, SA-11, SA-12, PM-9	A4.a

		<p><b>ID.SC-4:</b> Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.</p>	<p>AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12</p>	<p>A4.a</p>
	<p><b>Identity Management, Authentication and Access Control (PR.AC):</b> Access to physical and logical assets and facilities is limited to authorised users, processes, and devices, and is managed consistently.</p>	<p><b>ID.SC-5:</b> Response and recovery planning and testing are conducted with suppliers and third-party providers</p>	<p>CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9</p>	<p>D1.a</p>
<p><b>PROTECT (PR)</b></p>		<p><b>PR.AC-1:</b> Identities and credentials are issued, managed, verified, revoked, and audited for authorised devices, users, and processes</p>	<p>AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11</p>	<p>B2.a, B2.b, B2.c, B2.d</p>
		<p><b>PR.AC-2:</b> Physical access to assets is managed and protected</p>	<p>PE-2, PE-3, PE-4, PE-5, PE-6, PE-8</p>	<p>B2.a, B2.c</p>
		<p><b>PR.AC-3:</b> Remote access is managed</p>	<p>AC-1, AC-17, AC-19, AC-20, SC-15</p>	<p>B2.a</p>
		<p><b>PR.AC-4:</b> Access permissions and authorisations are managed, incorporating the principles of least privilege and separation of duties</p>	<p>AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24</p>	<p>B2.a, B2.c, B2.d</p>
		<p><b>PR.AC-5:</b> Network integrity is protected (e.g. network segregation, network segmentation)</p>	<p>AC-4, AC-10, SC-7</p>	<p>B4.a, B5.b</p>
		<p><b>PR.AC-6:</b> Identities are proofed and bound to credentials and asserted in interactions</p>	<p>AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3</p>	<p>B2.a, B2.c, B2.d</p>

	<p><b>Awareness and Training (PR.AT):</b> OES personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.</p>	<p><b>PR.AC-7:</b> Users, devices, and other assets are authenticated (e.g. single-factor, multi-factor) commensurate with the risk of the transaction (e.g. individuals’ security and privacy risks and other organisational risks)</p>	AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11	B2.a, B2.c
		<p><b>PR.AT-1:</b> All users are informed and trained</p>	AT-2, PM-13	B6.b
		<p><b>PR.AT-2:</b> Privileged users understand their roles and responsibilities</p>	AT-3, PM-13	A1.b, B6.b
		<p><b>PR.AT-3:</b> Third-party stakeholders (e.g. suppliers, customers, partners) understand their roles and responsibilities</p>	PS-7, SA-9, SA-16	None
		<p><b>PR.AT-4:</b> Senior executives understand their roles and responsibilities</p>	AT-3, PM-13	A1.a, A1.b
	<p><b>Data Security (PR.DS):</b> Data is managed consistent with the OES risk strategy to protect the confidentiality, integrity, and availability of information.</p>	<p><b>PR.AT-5:</b> Physical and cybersecurity personnel understand their roles and responsibilities</p>	AT-3, IR-2, PM-13	A1.b
		<p><b>PR.DS-1:</b> Data-at-rest is protected</p>	MP-8, SC-12, SC-28	B3.c
		<p><b>PR.DS-2:</b> Data-in-transit is protected</p>	SC-8, SC-11, SC-12	B3.b
		<p><b>PR.DS-3:</b> Assets are formally managed throughout removal, transfers, and disposition</p>	CM-8, MP-6, PE-16	A3.a, B3.e
		<p><b>PR.DS-4:</b> Adequate capacity to ensure availability is maintained</p>	AU-4, CP-2, SC-5	B5.b



<p><b>Information Protection Processes and Procedures (PR.IP):</b></p> <p>Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination across OES), processes, and procedures are maintained and used to manage protection of data, systems, and assets.</p>	<p><b>PR.DS-5:</b> Protections against data leaks are implemented</p>	<p>AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4</p>	<p>B3.a, B3.b, B3.c, B3.d</p>
	<p><b>PR.DS-6:</b> Integrity checking mechanisms are used to verify software, firmware, and information integrity</p>	<p>SC-16, SI-7</p>	<p>B4.b, B4.d</p>
	<p><b>PR.DS-7:</b> The development and testing environment(s) are separate from the production environment</p>	<p>CM-2</p>	<p>B4.a, B5.b</p>
	<p><b>PR.DS-8:</b> Integrity checking mechanisms are used to verify hardware integrity</p>	<p>SA-10, SI-7</p>	<p>B4.b</p>
	<p><b>PR.IP-1:</b> A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)</p>	<p>CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10</p>	<p>B4.b</p>
	<p><b>PR.IP-2:</b> A System Development Life Cycle to manage systems is implemented</p>	<p>PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17</p>	<p>B1.b</p>
	<p><b>PR.IP-3:</b> Configuration change control processes are in place</p>	<p>CM-3, CM-4, SA-10</p>	<p>B4.b</p>
	<p><b>PR.IP-4:</b> Backups of information are conducted, maintained, and tested</p>	<p>CP-4, CP-6, CP-9</p>	<p>B3.c, B5.c</p>
	<p><b>PR.IP-5:</b> Policy and regulations regarding the physical operating environment for organisational assets are met</p>	<p>PE-10, PE-12, PE-13, PE-14, PE-15, PE-18</p>	<p>B1.b</p>

<p><b>Maintenance (PR.MA)</b> Maintenance and repairs of information system components are performed consistent with policies and procedures.</p>	<p><b>PR.IP-6:</b> Data is destroyed according to policy</p>	MP-6	B1.b, B3.e
	<p><b>PR.IP-7:</b> Protection processes are improved</p>	CA-2, CA-7, CP-2, IR-8, PL-2, PM-6	B1.a, D2.b
	<p><b>PR.IP-8:</b> Effectiveness of protection technologies is shared</p>	AC-21, CA-7, SI-4	None
	<p><b>PR.IP-9:</b> Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed</p>	CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17	D1.a, B5.a
	<p><b>PR.IP-10:</b> Response and recovery plans are tested</p>	CP-4, IR-3, PM-14	D1.c
	<p><b>PR.IP-11:</b> Cybersecurity is included in human resources practices (e.g. deprovisioning, personnel screening)</p>	PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21	B1.b, B2.d, B2.c
	<p><b>PR.IP-12:</b> A vulnerability management plan is developed and implemented</p>	RA-3, RA-5, SI-2	B1.a, B1.b, B4.d
	<p><b>PR.MA-1:</b> Maintenance and repair of organisational assets are performed and logged, with approved and controlled tools</p>	MA-2, MA-3, MA-5, MA-6	None
	<p><b>PR.MA-2:</b> Remote maintenance of organisational assets is approved, logged, and performed in a manner that prevents unauthorised access</p>	MA-4	B2.a

	<p><b>Protective Technology (PR.PT):</b> Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.</p>	<p><b>PR.PT-1:</b> Audit/log records are determined, documented, implemented, and reviewed in accordance with policy</p>	AU Family	B2.d, C1.b, C1.c, B2.c
		<p><b>PR.PT-2:</b> Removable media is protected, and its use restricted according to policy</p>	MP-2, MP-3, MP-4, MP-5, MP-7, MP-8	B3.a
		<p><b>PR.PT-3:</b> The principle of least functionality is incorporated by configuring systems to provide only essential capabilities</p>	AC-3, CM-7	B4.b
		<p><b>PR.PT-4:</b> Communications and control networks are protected</p>	AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43	B4.a, B4.b, B4.c
		<p><b>PR.PT-5:</b> Mechanisms (e.g. failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations</p>	CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6	B5.b
<p><b>DETECT (DE)</b></p>	<p><b>Anomalies and Events (DE.AE):</b> Anomalous activity is detected, and the potential impact of events is understood.</p>	<p><b>DE.AE-1:</b> A baseline of network operations and expected data flows for users and systems is established and managed</p>	AC-4, CA-3, CM-2, SI-4	C1.a, C2.a, B3.a
		<p><b>DE.AE-2:</b> Detected events are analysed to understand attack targets and methods</p>	AU-6, CA-7, IR-4, SI-4	C1.c, C1.d, C1.e
		<p><b>DE.AE-3:</b> Event data are collected and correlated from multiple sources and sensors</p>	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4	C1.a

	<p><b>Security Continuous Monitoring (DE.CM):</b> The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.</p>	<p><b>DE.AE-4:</b> Impact of events is determined</p>	CP-2, IR-4, RA-3, SI-4	D2.a
		<p><b>DE.AE-5:</b> Incident alert thresholds are established</p>	IR-4, IR-5, IR-8	C1.c
		<p><b>DE.CM-1:</b> The network is monitored to detect potential cybersecurity events</p>	AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4	B4.c, C1.a, C1.c, C2.a
		<p><b>DE.CM-2:</b> The physical environment is monitored to detect potential cybersecurity events</p>	CA-7, PE-3, PE-6, PE-20	B4.c, C1.a, C1.c, C2.a
		<p><b>DE.CM-3:</b> Personnel activity is monitored to detect potential cybersecurity events</p>	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	B2.c, C1.a, C1.c, C2.a
		<p><b>DE.CM-4:</b> Malicious code is detected</p>	SI-3, SI-8	B4.c, C1.a
		<p><b>DE.CM-5:</b> Unauthorised mobile code is detected</p>	SC-18, SI-4, SC-44	B4.c, C1.a
		<p><b>DE.CM-6:</b> External service provider activity is monitored to detect potential cybersecurity events</p>	CA-7, PS-7, SA-4, SA-9, SI-4	A4.a, C1.a
		<p><b>DE.CM-7:</b> Monitoring for unauthorised personnel, connections, devices, and software is performed</p>	AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	B2.b, B4.c, C1.a, C2.b
		<p><b>DE.CM-8:</b> Vulnerability scans are performed</p>	RA-5	B4.d
	<p><b>Detection Processes (DE.DP):</b> Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.</p>	<p><b>DE.DP-1:</b> Roles and responsibilities for detection are well defined to ensure accountability</p>	CA-2, CA-7, PM-14	A1.b, C1.e
		<p><b>DE.DP-2:</b> Detection activities comply with all applicable requirements</p>	AC-25, CA-2, CA-7, SA-18, SI-4, PM-14	C1.a
		<p><b>DE.DP-3:</b> Detection processes are tested</p>	CA-2, CA-7, PE-3, SI-3, SI-4, PM-14	C1.c

		<b>DE.DP-4:</b> Event detection information is communicated	AU-6, CA-2, CA-7, RA-5, SI-4	C1.c, C1.e
		<b>DE.DP-5:</b> Detection processes are continuously improved	CA-2, CA-7, PL-2, RA-5, SI-4, PM-14	A2.b, B1.a, B1.b, D2.b
<b>RESPOND (RS)</b>	<b>Response Planning (RS.RP):</b> Response processes and procedures are executed and maintained, to ensure proportionate response to detected cybersecurity events.	<b>RS.RP-1:</b> Response plan is executed during or after an incident	CP-2, CP-10, IR-4, IR-8	D1.b
		<b>RS.CO-1:</b> Personnel know their roles and order of operations when a response is needed	CP-2, CP-3, IR-3, IR-8	D1.b, A1.b
	<b>Communications (RS.CO):</b> Response activities are coordinated with internal and external stakeholders	<b>RS.CO-2:</b> Incidents are reported consistent with established criteria	AU-6, IR-6, IR-8	D1.a, D1.b
		<b>RS.CO-3:</b> Information is shared consistent with response plans	CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4	D1.a, D1.b, D2.b
		<b>RS.CO-4:</b> Coordination with stakeholders occurs consistent with response plans	CP-2, IR-4, IR-8	D1.b
		<b>RS.CO-5:</b> Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	SI-5, PM-15	C1.d
		<b>Analysis (RS.AN):</b> Analysis is conducted to ensure effective response and support recovery activities.	<b>RS.AN-1:</b> Notifications from detection systems are investigated	AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
	<b>RS.AN-2:</b> The impact of the incident is understood		CP-2, IR-4	D1.a, D1.b

	<p><b>Mitigation (RS.MI):</b> Activities are performed to control and limit an event, mitigate its effects, and resolve the incident.</p> <p><b>Improvements (RS.IM):</b> Organisational response activities are improved by incorporating lessons learned from current and previous detection/response activities.</p>	<p><b>RS.AN-3:</b> Forensics are performed</p>	AU-7, IR-4	None
		<p><b>RS.AN-4:</b> Incidents are categorised consistent with response plans</p>	CP-2, IR-4, IR-5, IR-8	B5.a, C1.c, C1.e, D1.a
		<p><b>RS.AN-5:</b> Processes are established to receive, analyse, and respond to vulnerabilities disclosed to the organisation from internal and external sources (e.g. internal testing, security bulletins, or security researchers)</p>	SI-5, PM-15	A2.a, B1.a, B1.b, B4.d
		<p><b>RS.MI-1:</b> Incidents are contained</p>	IR-4	B4.c, D1.b
		<p><b>RS.MI-2:</b> Incidents are mitigated</p>	IR-4	D1.b
		<p><b>RS.MI-3:</b> Newly identified vulnerabilities are mitigated or documented as accepted risks</p>	CA-7, RA-3, RA-5	A2.a, B4.d
		<p><b>RS.IM-1:</b> Response plans incorporate lessons learned</p>	CP-2, IR-4, IR-8	D2.b
		<p><b>RS.IM-2:</b> Response strategies are updated</p>	CP-2, IR-4, IR-8	D2.b, B1.a, B1.d
<p><b>RECOVER (RC)</b></p>	<p><b>Recovery Planning (RC.RP):</b> Recovery processes and procedures are executed and maintained to</p>	<p><b>RC.RP-1:</b> Recovery plan is executed during or after a cybersecurity incident</p>	CP-10, IR-4, IR-8	D1.b

	ensure restoration of systems or assets affected by cybersecurity events.			
	<p><b>Improvements (RC.IM):</b> Recovery planning and processes are improved by incorporating lessons learned.</p>	<p><b>RC.IM-1:</b> Recovery plans incorporate lessons learned</p>	CP-2, IR-4, IR-8	D2.b
		<p><b>RC.IM-2:</b> Recovery strategies are updated</p>	CP-2, IR-4, IR-8	D2.b, B1.a, B1.b
	<p><b>Communications (RC.CO):</b> Restoration activities are coordinated with internal and external parties (e.g. Application Service providers, Internet Service Providers, CSIRTs, and vendors).</p>	<p><b>RC.CO-1:</b> Public relations are managed</p>	None	None
		<p><b>RC.CO-2:</b> Reputation is repaired after an incident</p>	None	None
		<p><b>RC.CO-3:</b> Recovery activities are communicated to internal and external stakeholders as well as executive and management teams</p>	CP-2, IR-4	D1.b

## Annex E-2 - Mitre Attack-ICS to CAF

MITRE ATT&CK for ICS<sup>63</sup> is a curated knowledge base for cyber adversary behaviour in the ICS (OT) technology domain. It reflects the various phases of an adversary’s attack life cycle and the assets and systems they are known to target. ATT&CK for ICS originated from MITRE internal research focused on applying the ATT&CK methodology to the ICS technology domain. Table 4 below references the available mitigations from the framework, referencing the CAF contributing outcome(s) that may be supported through their application, based on discovered vulnerabilities within the environment being protected.

Table 4 – Mitre Attack-ICS mitigations mapped to the CAF

Mitre Attack-ICS to CAF		
Mitigation	Description	CAF Contributing Outcome
M0801 Access Management	Access Management technologies can be used to enforce authorisation polices and decisions, especially when existing field devices do not provide sufficient capabilities to support user identification and authentication. These technologies typically utilize an in-line network device or gateway system to prevent access to unauthenticated users, while also integrating with an authentication service to first verify user credentials	B2.a, B2.c, B2.b, B4.c, B2.d
M1036 Account Use Policies	Configure features related to account use like login attempt lockouts, specific login times, etc.	C1.a, C1.c, B4.b, B2.c
M1015 Active Directory Configuration	Configure Active Directory to prevent use of certain techniques; use security identifier (SID) Filtering, etc.	B4.b, B2.a

<sup>63</sup> MITRE Corporation (2022) ATT&CK® 3274 for Industrial Control Systems. 3275 Available at <https://collaborate.mitre.org/attackics>



<p>M1049 Antivirus/Antimalware</p>	<p>Use signatures or heuristics to detect malicious software.</p> <p>Within industrial control environments, antivirus/antimalware installations should be limited to assets that are not involved in critical or real-time operations. To minimize the impact to system availability, all products should first be validated within a representative test environment before deployment to production systems.</p>	<p>B4.c, B4.b, C2.b, C1.c</p>
<p>M1013 Application Developer Guidance</p>	<p>This mitigation describes any guidance or training given to developers of applications to avoid introducing security weaknesses that an adversary may be able to take advantage of.</p>	<p>B6.b, B3.c</p>
<p>M1048 Application Isolation and Sandboxing</p>	<p>Restrict the execution of code to a virtual environment on or in-transit to an endpoint system.</p>	<p>B4.b</p>
<p>M1047 Audit</p>	<p>Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses. Perform periodic integrity checks of the device to validate the correctness of the firmware, software, programs, and configurations. Integrity checks, which typically include cryptographic hashes or digital signatures, should be compared to those obtained at known valid states, especially after events like device reboots, program downloads, or program restarts.</p>	<p>C1.a, B4.b, B2.a, B4.d</p>
<p>M0800 Authorization Enforcement</p>	<p>The device or system should restrict read, manipulate, or execute privileges to only authenticated users who require access based on approved security policies. Role-based Access Control (RBAC) schemes can help reduce the overhead of assigning permissions to the substantial number of devices within an ICS. For example, IEC 62351 provides examples of roles used to support common system operations within the electric power sector 1, while IEEE 1686 defines standard permissions for users of IEDs.</p>	<p>B2.a, B2.c, B4.a, B2.d</p>
<p>M1046 Boot Integrity</p>	<p>Use secure methods to boot a system and verify the integrity of the operating system and loading mechanisms.</p>	<p>B4.a, B4.b, B4.d</p>
<p>M1045 Code Signing</p>	<p>Enforce binary and application integrity with digital signature verification to prevent untrusted code from executing.</p>	<p>B4.b, A4.a</p>

M0802 Communication Authenticity	When communicating over an untrusted network, utilize secure network protocols that both authenticate the message sender and can verify its integrity. This can be done either through message authentication codes (MACs) or digital signatures, to detect spoofed network messages and unauthorized connections.	B4.b
M1053 Data Backup	Take and store data backups from end user systems and critical servers. Ensure backup and storage systems are hardened and kept separate from the corporate network to prevent compromise.  Maintain and exercise incident response plans, including the management of 'gold-copy' back-up images and configurations for key systems to enable quick recovery and response from adversarial activities that impact control, view, or availability.	D1.b, D1.c, B5.c, B3.c, B5.a
M0803 Data Loss Prevention	Data Loss Prevention (DLP) technologies can be used to help identify adversarial attempts to exfiltrate operational information, such as engineering plans, trade secrets, recipes, intellectual property, or process telemetry. DLP functionality may be built into other security products such as firewalls or standalone suites running on the network and host-based agents. DLP may be configured to prevent the transfer of information through corporate resources such as email, web, and physical media such as USB for host-based solutions.	C1.c, B4.a, B4.b
M1042 Disable or Remove Feature or Program	Remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.	B4.d
M0808 Encrypt Network Traffic	Utilize strong cryptographic techniques and protocols to prevent eavesdropping on network communications.	B3.b
M1038 Execution Prevention	Block execution of code on a system through application control, and/or script blocking.	B4.b
M1050 Exploit Protection	Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring.	C2.b, B4.a, C1.c

<p>M1037 Filter Network Traffic</p>	<p>Use network appliances to filter ingress or egress traffic and perform protocol-based filtering. Configure software on endpoints to filter network traffic.</p> <p>Perform inline allow/deny listing of network messages based on the application layer (OSI Layer 7) protocol, especially for automation protocols. Application allowlists are beneficial when there are well-defined communication sequences, types, rates, or patterns needed during expected system operations. Application denylists may be needed if all acceptable communication sequences cannot be defined, but instead a set of known malicious uses can be denied (e.g. excessive communication attempts, shutdown messages, invalid commands). Devices performing these functions are often referred to as deep-packet inspection (DPI) firewalls, context-aware firewalls, or firewalls blocking specific automation/SCADA protocol aware firewalls</p>	<p>B4.a</p>
<p>M0804 Human User Authentication</p>	<p>Require user authentication before allowing access to data or accepting commands to a device. While strong multi-factor authentication is preferable, it is not always feasible within ICS environments. Performing strong user authentication also requires additional security controls and processes which are often the target of related adversarial techniques (e.g. Valid Accounts, Default Credentials). Therefore, associated mitigations should be considered in addition to this, including Multi-factor Authentication, Account Use Policies, Password Policies, User Account Management, Privileged Account Management, and User Account Control</p>	<p>B2.a, B2.c, B2.b, B2.d</p>
<p>M1035 Limit Access to Resource Over Network</p>	<p>Prevent access to file shares, remote access to systems, unnecessary services. Mechanisms to limit access may include use of network concentrators, RDP gateways, etc.</p>	<p>B4.a, B3.c, B2.a</p>
<p>M1034 Limit Hardware Installation</p>	<p>Block users or groups from installing or using unapproved hardware on systems, including USB devices.</p>	<p>B2.b</p>
<p>M0805 Mechanical Protection Layers</p>	<p>Utilize a layered protection design based on physical or mechanical protection systems to prevent damage to property, equipment, human safety, or the environment. Examples include interlocks, rupture disk, release valves, etc</p>	<p>B4.a, B4.b</p>

M0806 Minimize Wireless Signal Propagation	Wireless signals frequently propagate outside of organizational boundaries, which provide opportunities for adversaries to monitor or gain unauthorized access to the wireless network. To minimize this threat, organizations should implement measures to detect, understand, and reduce unnecessary RF propagation.	B4.a
M0816 Mitigation Limited or Not Effective	This type of attack technique cannot be easily mitigated with preventative controls since it is based on the abuse of system features.	
M1032 Multi-factor Authentication	Use two or more pieces of evidence to authenticate to a system; such as username and password in addition to a token from a physical smart card or token generator.  Within industrial control environments assets such as low-level controllers, workstations, and HMIs have real-time operational control and safety requirements which may restrict the use of multi-factor.	B2.a, B2.c
M0807 Network Allowlists	Network allowlists can be implemented through either host-based files or system hosts files to specify what connections (e.g. IP address, MAC address, port, protocol) can be made from a device. Allowlist techniques that operate at the application layer (e.g. DNP3, Modbus, HTTP) are addressed in Filter Network Traffic mitigation.	B4.b
M1031 Network Intrusion Prevention	Use intrusion detection signatures to block traffic at network boundaries.  In industrial control environments, network intrusion prevention should be configured so it will not disrupt protocols and communications responsible for real-time functions related to control or safety.	C1.c, B4.c, C1.a, C2.b

<p>M1030 Network Segmentation</p>	<p>Architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a DMZ to contain any internet-facing services that should not be exposed from the internal network.</p> <p>Restrict network access to only required systems and services. In addition, prevent systems from other networks or business functions (e.g. enterprise) from accessing critical process control systems. For example, in IEC 62443, systems within the same secure level should be grouped into a "zone", and access to that zone is restricted by a "conduit", or mechanism to restrict data flows between zones by segmenting the network.</p>	<p>B4.a, B5.b, B3.c, B4.b, B2.b, A3.a</p>
<p>M1028 Operating System Configuration</p>	<p>Make configuration changes related to the operating system or a common feature of the operating system that result in system hardening against techniques.</p>	<p>B4.b</p>
<p>M0809 Operational Information Confidentiality</p>	<p>Deploy mechanisms to protect the confidentiality of information related to operational processes, facility locations, device configurations, programs, or databases that may have information that can be used to infer organizational trade-secrets, recipes, and other intellectual property (IP).</p>	<p>B3.c</p>
<p>M0810 Out-of-Band Communications Channel</p>	<p>Have alternative methods to support communication requirements during communication failures and data integrity attacks</p>	<p>B3.b, B5.b</p>
<p>M1027 Password Policies</p>	<p>Set and enforce secure password policies for accounts.</p>	<p>B1.b, B4.b</p>

M1026 Privileged Account Management	Manage the creation, modification, use, and permissions associated to privileged accounts, including SYSTEM and root.	B2.c, B2.d, B2.a
M0811 Redundancy of Service	Redundancy could be provided for both critical ICS devices and services, such as back-up devices or hot standbys.	B5.b, D1.b
M1022 Restrict File and Directory Permissions	Restrict access by setting directory and file permissions that are not specific to users or privileged accounts.	B3.c, B2.d, B2.a
M1044 Restrict Library Loading	Prevent abuse of library loading mechanisms in the operating system and software to load untrusted code by configuring appropriate library loading mechanisms and investigating potential vulnerable software.	B4.b, B4.d, B4.c
M1024 Restrict Registry Permissions	Restrict the ability to modify certain hives or keys in the Windows Registry.	B4.b
M1021 Restrict Web-Based Content	Restrict use of certain websites, block downloads/attachments, block JavaScript, restrict browser extensions, etc.	B4.c
M0812 Safety Instrumented Systems	Utilize Safety Instrumented Systems (SIS) to provide an additional layer of protection to hazard scenarios that may cause property damage. A SIS will typically include sensors, logic solvers, and a final control element that can be used to automatically respond to a hazardous condition. Ensure that all SISs (Safety Instrumented Systems) are segmented from operational networks to prevent them from being targeted by additional adversarial behaviour.	C1.c

M1054 Software Configuration	Implement configuration changes to software (other than the operating system) to mitigate security risks associated with how the software operates.	B4.a
M0813 Software Process and Device Authentication	Require the authentication of devices and software processes where appropriate. Devices that connect remotely to other systems should require strong authentication to prevent spoofing of communications. Furthermore, software processes should also require authentication when accessing APIs.	B4.b
M1020 SSL/TLS Inspection	Break and inspect SSL/TLS sessions to look at encrypted web traffic for adversary activity.	B2.a, B2.b, B2.c
M0814 Static Network Configuration	Configure hosts and devices to use static network configurations, when possible, protocols that require dynamic discovery/addressing (e.g. ARP (Address Resolution Protocol), DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name System)) can be used to manipulate network message forwarding and enable various MitM (man in the middle) attacks. This mitigation may not always be usable due to limited device features or challenges introduced with different network configurations.	B4.b
M0817 Supply Chain Management	Implement a supply chain management program, including policies and procedures to ensure all devices and components originate from a trusted supplier and are tested to verify their integrity.	
M1019 Threat Intelligence Program	A threat intelligence program helps an organization generate their own threat intelligence information and track trends to inform defensive priorities to mitigate risk.	C1.d, C2.a, B5.a, D1.c
M1051 Update Software	Perform regular software updates to mitigate exploitation risk. Software updates may need to be scheduled around operational down times.	B4.d, B4.b
M1018 User Account Management	Manage the creation, modification, use, and permissions associated to user accounts.	B2.c, B2.d

M1017 User Training	Train users to be aware of access or manipulation attempts by an adversary to reduce the risk of successful spear phishing, social engineering, and other techniques that involve user interaction.	B6.b
M1016 Vulnerability Scanning	Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them.	B4.d
M0815 Watchdog Timers	Utilise watchdog timers to ensure devices can quickly detect whether a system is unresponsive.	B4.b



### Annex E-3 – Mitre Enterprise to CAF

MITRE ATT&CK for Enterprise<sup>64</sup> is a curated knowledge base for cyber adversary behaviour in the Enterprise (IT) domain. It reflects the various phases of an adversary’s attack life cycle and the assets and systems they are known to target. ATT&CK for Enterprise originated from MITRE internal research focused on applying the ATT&CK methodology to the Enterprise domain. Table 5 below references the available mitigations from the framework, referencing the CAF contributing outcome(s) that may be supported through their application, based on discovered vulnerabilities within the environment being protected.

Table 5 – Mitre Enterprise mitigations mapped to the CAF

Mitre Attack-Enterprise to CAF		
Mitigation	Description	CAF Contributing Outcome
M1013 - Application Developer Guidance	This mitigation describes any guidance or training given to developers of applications to avoid introducing security weaknesses that an adversary may be able to take advantage of.	B6.b
M1015 Active Directory Configuration	Configure Active Directory to prevent use of certain techniques; use SID (security identifier) Filtering, etc.	B4.b, B4.d, B2.d
M1016 Vulnerability Scanning	Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them.	B4.d
M1017 User Training	Train users to be aware of access or manipulation attempts by an adversary to reduce the risk of successful spear phishing, social engineering, and other techniques that involve user interaction.	B6.b

<sup>64</sup> [Matrix - Enterprise | MITRE ATT&CK®](https://attack.mitre.org/matrices/enterprise/) - <https://attack.mitre.org/matrices/enterprise/>

## NIS Supplementary Guidance and CAF Overlay for DGE Sector

M1018 User Account Management	Train users to be aware of access or manipulation attempts by an adversary to reduce the risk of successful spear phishing, social engineering, and other techniques that involve user interaction.	B2.a B2.c B4.b
M1019 Threat Intelligence Program	A threat intelligence program helps an organisation generate their own threat intelligence information and track trends to inform defensive priorities to mitigate risk.	A2.a, B1.a, B5.a, C1.d, C2.a, D1.c
M1020 SSL/TLS Inspection	Break and inspect SSL/TLS sessions to look at encrypted web traffic for adversary activity.	C1.c, C1.a
M1021 Restrict Web-Based Content	Restrict use of certain websites, block downloads/attachments, block JavaScript, restrict browser extensions, etc.	B4.c, B4.b
M1022 Restrict File and Directory Permissions	Restrict access by setting directory and file permissions that are not specific to users or privileged accounts.	B2.c, B4.c, B3.c, B2.a, C1.b, B4.b
M1024 Restrict Registry Permissions	Restrict the ability to modify certain hives or keys in the Windows Registry.	B2.a, B2.c
M1025 Privileged Process Integrity	Protect processes with high privileges that can be used to interact with critical system components through use of protected process light, anti-process injection defences, or other process integrity enforcement measures.	B4.b
M1026 Privileged Account Management	Manage the creation, modification, use, and permissions associated to privileged accounts, including SYSTEM and root.	B2.c
M1027 Password Policies	Set and enforce secure password policies for accounts.	B1.a, B1.b, B4.b
M1028 Operating System Configuration	Make configuration changes related to the operating system or a common feature of the operating system that result in system hardening against techniques.	B4.d, B4.b, B2.b, B1.a, B2.a

M1029 Remote Data Storage	Use remote security log and sensitive file storage where access can be controlled better to prevent exposure of intrusion detection log data or sensitive information.	B5.c, B5.a, B3.c, B4.c, B4.a
M1030 Network Segmentation	Architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a DMZ to contain any internet-facing services that should not be exposed from the internal network. Configure separate virtual private cloud (VPC) instances to isolate critical cloud systems.	B4.a, B5.b, B4.b
M1031 Network Intrusion Prevention	Use intrusion detection signatures to block traffic at network boundaries.	C1.a, C1.c, C1.d
M1032 Multi-factor Authentication	Use two or more pieces of evidence to authenticate to a system; such as username and password in addition to a token from a physical smart card or token generator.	B2.a, B2.c
M1033 Limit Software Installation	Block users or groups from installing unapproved software.	B4.b, B4.c
M1034 Limit Hardware Installation	Block users or groups from installing or using unapproved hardware on systems, including USB devices.	B2.b
M1035 Limit Access to Resource Over Network	Prevent access to file shares, remote access to systems, unnecessary services. Mechanisms to limit access may include use of network concentrators, RDP (Remote Desktop Protocols) gateways, etc.	B4.a, B4.b
M1036 Account Use Polices	Configure features related to account use like login attempt lockouts, specific login times, etc.	B4.b, C1.b
M1037 Filter Network Traffic	Use network appliances to filter ingress or egress traffic and perform protocol-based filtering. Configure software on endpoints to filter network traffic.	B4.a, B5.b
M1038 Execution Prevention	Block execution of code on a system through application control, and/or script blocking.	B4.c

M1039 Environment Variable Permissions	Prevent modification of environment variables by unauthorized users and groups.	B4.b, B2.a
M1040 Behaviour Prevention on Endpoint	Use capabilities to prevent suspicious behaviour patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behaviour.	B4.b, B4.c
M1041 Encrypt Sensitive Information	Protect sensitive information with strong encryption.	B3.b, B3.c, B4.b, B5.c
M1042 Disable or Remove Feature or Program	Remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.	B4.b, B4.d
M1043 Credential Access Protection	Use capabilities to prevent successful credential access by adversaries; including blocking forms of credential dumping.	B4.b
M1044 Restrict Library Loading	Prevent abuse of library loading mechanisms in the operating system and software to load untrusted code by configuring appropriate library loading mechanisms and investigating potential vulnerable software.	B4.c, B4.b
M1045 Code Signing	Enforce binary and application integrity with digital signature verification to prevent untrusted code from executing.	B4.b, B4.a
M1046 Boot Integrity	Use secure methods to boot a system and verify the integrity of the operating system and loading mechanisms.	B4.d, B4.b
M1047 Audit	Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.	C1.a, B4.d, B2.d, B2.a, B2.c, B4.b
M1048 Application Isolation and Sandboxing	Restrict execution of code to a virtual environment on or in transit to an endpoint system.	B4.b, B4.d
M1049 Antivirus/Antimalware	Use signatures or heuristics to detect malicious software.	B4.c, C1.d, C2.b, C1.c, B4.d, C1.a

M1050 Exploit Protection	Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring.	B4.c, C1.a
M1051 Update Software	Perform regular software updates to mitigate exploitation risk.	B4.d
M1052 User Account Control	Configure Windows User Account Control to mitigate risk of adversaries obtaining elevated process access.	B2.c, A4.a, B4.b
M1053 Data Backup	Take and store data backups from end user systems and critical servers. Ensure backup and storage systems are hardened and kept separate from the corporate network to prevent compromise.	B5.c, D1.b, B3.c
M1054 Software Configuration	Implement configuration changes to software (other than the operating system) to mitigate security risks associated to how the software operates.	A4.a, B4.b
M1055 Do Not Mitigate	This category is to associate techniques that mitigation might increase risk of compromise and therefore mitigation is not recommended.	
M1056 Pre-compromise	This category is used for any applicable mitigation activities that apply to techniques occurring before an adversary gains Initial Access, such as Reconnaissance and Resource Development techniques.	
M1057 Data Loss Prevention	Use a data loss prevention (DLP) strategy to categorize sensitive data, identify data formats indicative of personal identifiable information (PII), and restrict exfiltration of sensitive data.	

## Annex E-4 – ISO27002/19 to CAF

The mapping table in this appendix (table 6) provides OES with a general indication of security control coverage with respect to ISO/IEC 27002/19. ISO/IEC 27002 and the energy industry interpretation contained in ISO/IEC 27019 are designed for organisations to use as a reference for selecting controls within the process of implementing an Information Security Management System (ISMS) based on ISO/IEC 27001.

Table 6 – ISO / IEC 27002-19 Controls mapped to the CAF

ISO 27002/19 to CAF		
Clause	Description	CAF Contributing Outcome
<b>5. Information Security Policies</b>		
5.1 Management direction for information security		
5.1.1	Policies for information Security	B1.a, B1.b
5.1.2	Review of the policies for information security	B1.a
<b>6. Organization of information security</b>		
6.1 Internal organisation		
6.1.1	Information security roles and responsibilities	A1.b
6.1.2	Segregation of duties	
6.1.3	Contact with authorities	
6.1.4	Contact with special interest groups	B5.a, C1.d
6.1.5	Information security in project management	B4.a, A2.a
6.1.6	27019 only – Identification of risks related to external parties	

6.1.7	27019 only – Addressing security when dealing with customers	
6.2 Mobile devices and teleworking		
6.2.1	Mobile Device Policy	B1.b
6.2.2	Teleworking	B1.b
7. Human Resources Security		
7.1 Prior to Employment		
7.1.1	Screening	B2.d
7.1.2	Terms and conditions of employment	
7.2 During employment		
7.2.1	Management responsibilities	B6.a, B1.b
7.2.2	Information security, awareness, education, and training	B6.b, B6.a
7.2.3	Disciplinary process	B1.b
7.3 Termination and change of employment		
7.3.1	Termination or change of employment responsibilities	B6.b
8 Asset Management		
8.1 Responsibility for assets		
8.1.1	Inventory of assets	A3.a, B3.a
8.1.2	Ownership of assets	A3.a
8.1.3	Acceptable use of assets	B1.b
8.1.4	Return of assets	A3.a
8.2 Information Classification		
8.2.1	Classification of information	A3.a, B3.a,

8.2.2	Labelling of information	B1.a, B1.b
8.2.3	Handling of assets	B1.a, B1.b, A3.a
8.3 Media Handling		
8.3.1	Management of removable media	A3.a, B1.b
8.3.2	Disposal of media	A3.a, B3.e
8.3.3	Physical media transfer	B3.d
9 Access Control		
9.1 Business requirement of access control		
9.1.1	Access control policy	B1.a, B1.b
9.1.2	Access to networks and network services	B2.a, B2.c, B2.d
9.2 User access management		
9.2.1	User registration and de-registration	B1.b, B2.d
9.2.2	User access provisioning	B1.b, B2.d
9.2.3	Management of privileged access rights	B2.c, B2.d
9.2.4	Management of secret authentication information of users	B1.b
9.2.5	Review of user access rights	B2.a, B2.c, B2.d
9.2.6	Removal or adjustment of access rights	B2.d
9.3 User Responsibilities		
9.3.1	Use of secret authentication information	B1.a, B1.b
9.4 System and application access control		
9.4.1	Information access restriction	B1.b, B2.a
9.4.2	Secure log-on procedures	B1.b, B2.a, B2.c
9.4.3	Password management system	B2



9.4.4	Use of privileged utility programs	B2
9.4.5	Access control to program source code	B3.c
<b>10 Cryptography</b>		
<b>10.1 Cryptographic controls</b>		
10.1.1	Policy on the use of cryptographic controls	B1.a, B1.b
10.1.2	Key management	B1.a, B1.b,
<b>11 Physical and environmental security</b>		
<b>11.1 Secure areas</b>		
11.1.1	Physical security perimeter	B2.c, B3.b, B3.c
11.1.2	Physical entry controls	B2.a, B2.c
11.1.3	Securing offices, rooms, and facilities	B2
11.1.4	Protecting against external and environmental threats	B5.a
11.1.5	Working in secure areas	B1.b,
11.1.6	Delivery and loading areas	
11.1.7	27019 only – Securing control centres	
11.1.8	27019 only – Securing equipment rooms	
11.1.9	27019 only – Securing peripheral sites	
<b>11.2 Equipment</b>		
11.2.1	Equipment siting and protection	
11.2.2	Supporting utilities	A3.a, B5.b
11.2.3	Cabling security	B3.b
11.2.4	Equipment maintenance	
11.2.5	Removal of assets	A3.a
11.2.6	Security of equipment and assets off-premises	
11.2.7	Secure disposal or re-use of equipment	A3.a, B3.e

11.2.8	Unattended user equipment	
11.2.9	Clear desk and clear screen policy	B1.a, B1.b, B6.b
11.3 Security in premises of external parties		
11.3.1	27019 only – Equipment sited on the premises of other energy utility organisations	
11.3.2	27019 only – Equipment sited on customer’s premises	
11.3.3	27019 only – Interconnected control and communication systems	
12 Operations Security		
12.1 Operational procedures and responsibilities		
12.1.1	Documented operating procedures	B1.a, B1.b
12.1.2	Change management	B1.a, B4.b
12.1.3	Capacity management	A3.a, B3.a, B5.b, B5.c
12.1.4	Separation of development, testing, and operational environments	B4.a, B4.c
12.2 Protection from malware		
12.2.1	Controls against malware	B4.c, B4.d, C1.a, B6.b, B5.a, B4.b
12.3 Backup		
12.3.1	Information backup	B5.c, B1.a, B3.c, A3.a
12.4 Logging and monitoring		
12.4.1	Event Logging	B2.d, C1.a, C1.c
12.4.2	Protection of log information	C1.b
12.4.3	Administrator and operator logs	B2.c, C1.a, C1.b
12.4.4	Clock synchronisation	C1.b
12.5 Control of operational software		

12.5.1	Installation of software on operational systems	B4.b, B4.d
12.6 Technical vulnerability management		
12.6.1	Management of technical vulnerabilities	B4.d
12.6.2	Restrictions on software installation	B4.b
12.7 Information systems audit considerations		
12.7.1	Information systems audit controls	A2.b
12.8 ENR Treatment of legacy systems		
12.8.1	ENR – Treatment of legacy systems	
12.9 ENR Safety Functions		
12.9.1	ENR – Integrity and Availability of Safety Functions	
13 Communication Security		
13.1 Network Security Management		
13.1.1	Network controls	B4.c, C1.a, B2.a, B4.b
13.1.2	Security of network services	A4.a
13.1.3	Segregation in networks	B4.a, B5.b
13.1.4	27019 only – Securing process control data communication	
13.1.5	27019 only – Logical connection of external process control systems	
13.2 Information transfer		
13.2.1	Information transfer policies and procedures	B1.b
13.2.2	Agreements on information transfer	A4.a
13.2.3	Electronic messaging	B3.b
13.2.4	Confidentiality or non-disclosure agreement	

<b>14 System acquisition, development, and maintenance</b>		
<b>14.1 Security requirements of information systems</b>		
14.1.1	Information security requirements analysis and specification	B1.a
14.1.2	Securing application services on public networks	B3.b
14.1.3	Protecting application services transactions	B3.a B3.b
<b>14.2 Security in development and support processes</b>		
14.2.1	Secure development policy	B1.a B1.b
14.2.2	System changes control procedures	B4.b
14.2.3	Technical review of applications after operating platform changes	B4.b
14.2.4	Restrictions on changes to software packages	B4.b
14.2.5	Secure system engineering principles	B1.a B1.b
14.2.6	Secure development environment	B4.b
14.2.7	Outsourced development	A4.a
14.2.8	System security testing	A2.b
14.2.9	System acceptance testing	B1.a, B3.c
14.2.10	27019 only – Least Functionality	
<b>15 Supplier Relationship</b>		
<b>15.1 Information security in supplier relationships</b>		
15.1.1	Information security policy for supplier relationships	A4.a
15.1.2	Addressing security within supplier agreements	A4.a
15.1.3	Information and communication technology supply chain	A4.a
<b>15.2 Supplier service delivery management</b>		
15.2.1	Monitoring and review of supplier services	A4.a
15.2.2	Managing changes to supplier services	A4.a

<b>16 Information Security Incident Management</b>		
<b>16.1 Managing of information security incidents and improvements</b>		
16.1.1	Responsibilities and procedures	A1.b, D1.a
16.1.2	Reporting information security events	B6.a
16.1.3	Reporting information security weaknesses	B6.a
16.1.4	Assessment of and decision on information security events	
16.1.5	Response to information security incidents	D1.a
16.1.6	Learning from information security incidents	D2.a, D2.b
16.1.7	Collection of evidence	B1.b, D2.a
<b>17 Information security aspects of business continuity management</b>		
<b>17.1 Information security continuity</b>		
17.1.1	Planning information security continuity	B5.a
17.1.2	Implementing information security continuity	B1.a, B5.a
17.1.3	Verify, review, and evaluate information security continuity	B1.a, B4.b
<b>17.2 Redundancies</b>		
17.2.1	Availability of information processing facilities	B5.b
17.2.2	27019 only – Emergency communication	
<b>18 Compliance</b>		
<b>18.1 Compliance with legal and contractual requirements</b>		
18.1.1	Identification of applicable legislation and contractual requirements	B1.a
18.1.2	Intellectual property rights	B1.a
18.1.3	Protection of records	B3.c, B5.a
18.1.4	Privacy and protection of personally identifiable information	B3.c
18.1.5	Regulation of cryptographic controls	B1.a

18.2 Information security reviews		
18.2.1	Independent review of information security	B1.a
18.2.2	Compliance with security policies and standards	B1.b
18.2.3	Technical compliance review	B1.a, B4.d, A2.b

Note: -

ISO/IEC 27019:2017 provides guidance based on ISO/IEC 27002 applied to process control systems used by the energy utility industry for controlling and monitoring the production or generation, transmission, storage and distribution of electric power, gas, oil, and heat, and for the control of associated supporting processes. This includes the following:

- central and distributed process control, monitoring, and automation technology as well as information systems used for their operation, such as programming and parameterisation devices;
- digital controllers and automation components such as control and field devices or Programmable Logic Controllers (PLCs), including digital sensor and actuator elements;
- all further supporting information systems used in the process control domain, e.g. for supplementary data visualisation tasks and for controlling, monitoring, data archiving, historian logging, reporting and documentation purposes;
- communication technology used in the process control domain, e.g. networks, telemetry, telecontrol applications and remote-control technology;
- Advanced Metering Infrastructure (AMI) components, e.g. smart meters;
- measurement devices, e.g. for emission values;
- digital protection and safety systems, e.g. protection relays, safety PLCs, emergency governor mechanisms;
- energy management systems, e.g. of Distributed Energy Resources (DER), electric charging infrastructures, in private households, residential buildings or industrial customer installations;

## NIS Supplementary Guidance and CAF Overlay for DGE Sector

---

- distributed components of smart grid environments, e.g. in energy grids, in private households, residential buildings or industrial customer installations;
- all software, firmware and applications installed on above-mentioned systems, e.g. DMS (Distribution Management System) applications or OMS (Outage Management System);
- any premises housing the above-mentioned equipment and systems;
- remote maintenance systems for above-mentioned systems.

## **Annex E-5 – ISA/IEC 62443-2-1 mapped to CAF**

The standard presents the elements that constitute a proposed cyber security management system for IACS (Industrial Automation and Control Systems). These elements represent what shall and should be included in the CSMS (Cyber Security Management System) to protect IACS against cyber-attacks. The elements are presented in the following three main categories:

- Risk analysis,
- addressing risk with the CSMS, and
- Monitoring and improving the CSMS.

Each of these categories is further divided into element groups and/or elements as detailed in table 7.

Table 7 – IEC 62443-2-1:2009 Security Requirements mapped to the CAF

ISA / IEC 62443-2-1:2009 - Security for industrial automation and control systems mapped to CAF		
Clause	Description	CAF Contributing Outcome
Category: Risk analysis		
Element: Risk identification, classification, and assessment		
4.2.3.1	Select a risk assessment methodology	A2.a
4.2.3.2	Provide risk assessment background information	A2.a      B6.b
4.2.3.3	Conduct a high-level risk assessment	A2.a
4.2.3.4	Identify the industrial automation and control systems	A3.a      B4.b
4.2.3.5	Develop Simple Network Diagrams	B4.a
4.2.3.6	Prioritise Systems	A3.a



## NIS Supplementary Guidance and CAF Overlay for DGE Sector

4.2.3.7	Perform a detailed vulnerability assessment	B4.d	
4.2.3.8	Identify a detailed risk assessment methodology	A2.a	B4.d
4.2.3.9	Conduct a detailed risk assessment	A2.a	
4.2.3.10	Identify the reassessment frequency and triggering criteria	A2.a	
4.2.3.11	Integrate physical, HSE and cyber security risk assessments	A2.a	
4.2.3.12	Conduct risk assessments throughout the lifecycle of the IACs	A2.a	
4.2.3.13	Document the Risk Assessment	A2.a	
4.2.3.14	Maintain vulnerability assessment records	A2.a	
<b>Category: Addressing risk with the CSMS</b>			
Element: CSMS scope			
4.3.2.2.1	Define the scope of the CSMS	A2.a	
4.3.2.2.2	Define the scope content	A2.a	
Element: Organizing for security			
4.3.2.3.1	Obtain senior management support	A1.a	
4.3.2.3.2	Establish the security organisation	A1.a	A1.b
4.3.2.3.3	Define the organisational responsibilities	A1.b	
4.3.2.3.4	Define the stakeholder team management	A1.a	
Element: Staff training and security awareness			
4.3.2.4.1	Develop a training program	B6.b	
4.3.2.4.2	Provide procedure and facility training	B6.b	
4.3.2.4.3	Provide training for support personnel	B6.b	
4.3.2.4.4	Validate the training program	B6.b	
4.3.2.4.5	Revise the training program over time	B6.b	
4.3.2.4.6	Maintain employee training record	B6.b	
Element: Business continuity plan			

## NIS Supplementary Guidance and CAF Overlay for DGE Sector

4.3.2.5.1	Specify recovery objectives	B5.b		
4.3.2.5.2	Determine the impacts and consequences to each system	A3.a		
4.3.2.5.3	Develop and implement business continuity plans	B5.a		
4.3.2.5.4	Form a continuity team	A1.b		
4.3.2.5.5	Define and communicate specific roles and responsibilities	A1.b		
4.3.2.5.6	Create the backup procedures that support business continuity plan	B5.a	B5.c	
4.3.2.5.7	Test and update the business continuity plan	B5.a		
Element: Security policies and procedures				
4.3.2.6.1	Develop security policies	B1.a		
4.3.2.6.2	Develop security procedures	B1.a		
4.3.2.6.3	Maintain consistency between risk management systems	B1.a		
4.3.2.6.4	Define cyber security policies and procedure compliance requirements	B1.b		
4.3.2.6.5	Determine the organisations tolerance for risk	A2.a		
4.3.2.6.6	Communicate the policies and procedures to the organisation	B1.b		
4.3.2.6.7	Review and update the cyber security policies and procedures	B1.a		
4.3.2.6.8	Demonstrate senior leadership support for cyber security	A1.a		
Element: Personnel security				
4.3.3.2.1	Personnel security	B1.a		
4.3.3.2.2	Screen personnel initially			
4.3.3.2.3	Screen personnel on an ongoing basis			
4.3.3.2.4	Address security responsibilities	B1.a		
4.3.3.2.5	Document and communicate security expectations and responsibilities	A1.b	B1.b	B6.a
4.3.3.2.6	State cyber security terms and conditions of employment clearly			
4.3.3.2.7	Segregate duties to maintain appropriate checks and balances			
Element: Physical and environmental security				
4.3.3.3.1	Establish complimentary physical and cyber security policies	B1.b		

## NIS Supplementary Guidance and CAF Overlay for DGE Sector

4.3.3.3.2	Establish physical security perimeters	B3.c	B2.c
4.3.3.3.3	Provide entry controls	B2.c	B3.c
4.3.3.3.4	Protect assets against environmental damage	B3.c	
4.3.3.3.5	Require employees to follow security procedures	B1.b	
4.3.3.3.6	Protect connections	B3.b	B5.b
4.3.3.3.7	Maintain equipment assets	A3.a	
4.3.3.3.8	Establish procedures for monitoring and alarming	C1.a	C1.c
4.3.3.3.9	Establish procedures for the addition, removal, and disposal of assets	B3.e	A3.a
4.3.3.3.10	Establish procedures for the interim protection of critical assets	B5.a	
Element: Network segmentation			
4.3.3.4.1	Develop the network segmentation architecture	B4.a	B5.b
4.3.3.4.2	Employ isolation or segmentation on high-risk IACS	B4.a	B5.b
4.3.3.4.3	Block non-essential communications with barrier devices	B4.a	B5.b
4.3.3.5.1	Access accounts implement authorization security policy	B1.a	
4.3.3.5.2	Identify individuals	B2.a	B2.c
4.3.3.5.3	Authorize account access	A1.b	
Element: Access control – Account administration			
4.3.3.5.4	Record access accounts	B2.c	
4.3.3.5.5	Suspend or remove unneeded accounts	B2.a	B2.c
4.3.3.5.6	Review account permissions	B2.a	B2.c
4.3.3.5.7	Change default passwords	B4.b	
4.3.3.5.8	Audit account administration	B2.a	B2.c
Element: Access control – Authentication			
4.3.3.6.1	Develop an authentication strategy	B1.a	
4.3.3.6.2	Authenticate all users before system use	B2.a	

## NIS Supplementary Guidance and CAF Overlay for DGE Sector

4.3.3.6.3	Require strong authentication methods for system administration and application configuration	B2.a			
4.3.3.6.4	Log and review all access attempts to critical systems	C1.a			
4.3.3.6.5	Authenticate all remote users at the appropriate level	B2.a			
4.3.3.6.6	Develop a policy for remote login and connections	B1.a			
4.3.3.6.7	Disable access account after failed remote login attempts	B1.a	B4.b		
4.3.3.6.8	Require re-authentication after remote system inactivity	B1.a	B4.b		
4.3.3.6.9	Employ authentication for task-to task communication	B2.a			
Element: Access control – Authorisation					
4.3.3.7.1	Define an authorization security policy	B1.a			
4.3.3.7.2	Establish appropriate logical and physical permission methods to access IACS devices	B2.a	B2.c		
4.3.3.7.3	Control access to information or systems via role-based access accounts				
4.3.3.7.4	Employ multiple authorization methods for critical IACS	B2.a	B2.c		
Element: Risk management and implementation					
4.3.4.2.1	Manage IACS risk on an ongoing basis	A2.a			
4.3.4.2.2	Employ a common set of countermeasures	A2.a			
Element: System development and maintenance					
4.3.4.3.1	Define and test security functions and capabilities	B4.b			
4.3.4.3.2	Develop and implement a change management system				
4.3.4.3.3	Assess all the risks of changing the IACS	A2.a			
4.3.4.3.4	Require security policies for system development or maintenance changes	B1.a			
4.3.4.3.5	Integrate cyber security and process safety management (PSM) change management procedures	B1.a	B4.b		
4.3.4.3.6	Review and maintain policies and procedures	B1.a			
4.3.4.3.7	Establish and document a patch management procedure	B4.b			
4.3.4.3.8	Establish and document antivirus/malware management procedure	B4.c	C1.d	C1.c	C2.b

## NIS Supplementary Guidance and CAF Overlay for DGE Sector

4.3.4.3.9	Establish backup and restoration procedure	B5.c	D1.b
Element: Information and document management			
4.3.4.4.1	Develop lifecycle management processes for IACS information	B1.a	
4.3.4.4.2	Define information classification levels	B1.a	
4.3.4.4.3	Classify all CSMS information assets	A3.a	
4.3.4.4.4	Ensure appropriate records control	B1.a	B3.e
4.3.4.4.5	Ensure long-term records retrieval		
4.3.4.4.6	Maintain information classifications	B3.a	
4.3.4.4.7	Audit the information and document management process	A2.b	
Element: Incident planning and response			
4.3.4.5.1	Implement an incident response plan	D1.a	
4.3.4.5.2	Communicate the incident response plan	D1.a	
4.3.4.5.3	Establish a reporting procedure for unusual activities and events	B6.a	
4.3.4.5.4	Educate employees on reporting cyber security incidents	B6.a	
4.3.4.5.5	Report cyber security incidents in a timely manner	B6.a	
4.3.4.5.6	Identify and respond to incidents	D1.a	
4.3.4.5.7	Identify failed and successful cyber security breaches	C1.c	
4.3.4.5.8	Document the details of incidents	D2.a	D2.b
4.3.4.5.9	Communicate the incident details		
4.3.4.5.10	Address and correct issues discovered	D2.b	
4.3.4.5.11	Conduct drills	D1.c	
Category: Monitoring and improving the CSMS			
Element: Conformance			
4.4.2.1	Specify the methodology of the audit process	A2.b	
4.4.2.2	Conduct periodic IACS audits	A2.b	
4.4.2.3	Establish conformance metrics	A2.b	

## NIS Supplementary Guidance and CAF Overlay for DGE Sector

4.4.2.4	Establish a document audit trail	
4.4.2.5	Define punitive measures for nonconformance	
Element: Review, improve and maintain the CSMS		
4.4.3.1	Assign an organization to manage and implement changes to the CSMS	
4.4.3.2	Evaluate the CSMS periodically	B1.a
4.4.3.3	Establish triggers to evaluate CSMS	B1.a
4.4.3.4	Identify and implement corrective and preventive actions	B1.b
4.4.3.5	Review risk tolerance	A2.a
4.4.3.6	Monitor and evaluate industry CSMS strategies	A2.a
4.4.3.7	Monitor and evaluate applicable legislation relevant to cyber security	
4.4.3.8	Request and report employee feedback on security suggestions	B1.a

## Annex E-6 – ISA/IEC 62443-3-3 mapped to CAF

The standard presents the controls that can be used to support cyber security management system for IACS (Industrial Automation and Control Systems). The elements are described in 62443 as foundational requirements across the following categories:

1. Identification and authentication control
2. Use Control
3. System Integrity
4. Data Confidentiality
5. Restricted Data Flow
6. Timely Response to Events
7. Resource Availability

Each of these categories is further divided into security requirements as detailed in table 8.

Table 8 – IEC 62443-3-3:2013 Security Requirements mapped to the CAF

ISA / IEC 62443-3-3: 2013 to CAF		
Clause	Description	CAF Contributing Outcome
Foundational Requirement 1 - Identification and authentication control		
SR 1.1	Human User Identification and Authentication	B2.a, B2.c, B2.d
SR 1.2	Software process and device identification and authentication	B2.a, B2.c, B2.d
SR 1.3	Account management	B2.d
SR 1.4	Identifier management	B2.a, B2.c, B2.d

SR 1.5	Authenticator management	B2.a, B2.c, B2.d, B3.b, B3.c, B4.b, B4.c
SR 1.6	Wireless access management	B2.a, B2.b
SR 1.7	Strength of password-based authentication	B4.b
SR 1.8	Public key infrastructure (PKI) certificates	B3.c
SR 1.9	Strength of public key authentication	B3.b, B3.c
SR 1.10	Authenticator feedback	B4.a, B4.b
SR 1.11	Unsuccessful login attempts	B4.b
SR 1.12	System use notification	B1.b
SR 1.13	Access via untrusted networks	B2.a

Foundational Requirement 2 - Use Control

SR 2.1	Authorization enforcement	B2.a, B2.d
SR 2.2	Wireless use control	B2.a, B4.b
SR 2.3	Use control for portable and mobile devices	B2.a, B4.b
SR 2.4	Mobile code	B4.b, B4.c
SR 2.5	Session lock	B2.a, B4.b
SR 2.6	Remote session termination	B2.c
SR 2.7	Concurrent session control	B4.b
SR 2.8	Auditable events	B2.d, C1.a
SR 2.9	Audit storage capacity	
SR 2.10	Response to audit processing failures	C1.c
SR 2.11	Timestamps	C1.b
SR 2.12	Non-repudiation	

Foundational Requirement 3 – System Integrity

SR 3.1	Communication integrity	B3.b
SR 3.2	Malicious code protection	B4.a, B4.c



SR 3.3	Security functionality verification	B4.d, C1.b
SR 3.4	Software and information integrity	B3.c, B4.b
SR 3.5	Input validation	B4.b
SR 3.6	Deterministic output	
SR 3.7	Error handling	
SR 3.8	Session integrity	B2.a, B2.d
SR 3.9	Protection of audit information	C1.b
Foundational Requirement 4 – Data Confidentiality		
SR 4.1	Information confidentiality	B3.b, B3.c
SR 4.2	Information persistence	B3.e
SR 4.3	Use of cryptography	B3.b, B3.c
Foundational Requirement 5 – Restricted Data Flow		
SR 5.1	Network segmentation	B4.a
SR 5.2	Zone boundary protection	B4.a
SR 5.3	General purpose person-to-person communication restrictions	B2.b, B2.c, B4.b
SR 5.4	Application partitioning	B4.a
Foundational Requirement 6 – Timely Response to Events		
SR 6.1	Audit log accessibility	C1.b
SR 6.2	Continuous monitoring	C1.a
Foundational Requirement 7 – Resource Availability		
SR 7.1	Denial of service protection	B4.d, D1.b
SR 7.2	Resource management	D1.b
SR 7.3	Control system backup	B3.c, B5.c

---

SR 7.4	Control system recovery and reconstitution	
SR 7.5	Emergency power	D1.b
SR 7.6	Network and security configuration settings	B4.b
SR 7.7	Least functionality	B4.b
SR 7.8	Control system component inventory	A3.a, B4.b

© Crown copyright 2023

The text of this document may be reproduced (excluding logos) under and in accordance with the terms of the [Open Government Licence](#).

Without prejudice to the generality of the terms of the Open Government Licence the material that is reproduced must be acknowledged as Crown copyright and the document title of this document must be specified in that acknowledgement.

Any enquiries related to the text of this publication should be sent to Ofgem at:

10 South Colonnade, Canary Wharf, London, E14 4PU. Alternatively, please call Ofgem on 0207 901 7000.

This publication is available at [www.ofgem.gov.uk](http://www.ofgem.gov.uk). Any enquiries regarding the use and re-use of this information resource should be sent to: [psi@nationalarchives.gsi.gov.uk](mailto:psi@nationalarchives.gsi.gov.uk)