

Ofgem Competent Authority

NIS Check-in Report| [OES]



[DATE]

Use this slide to confirm the relevant contacts and any changes that have occurred since the last report.

Role	Named contact	Email address	Changed since previous report (Yes/NO)?	Enter date of change
CEO				
CIO				
CISO				
NIS Responsible Officer ("NRO")				
Deputy NIS Responsible Officer ("NRO")				
Cyber Operational Lead (OT)				
Cyber Operational Lead (IT)				

Table 1: NIS Communication Counterparts and Responsible Officers

- 1. Has the scope changed since the last report period** (e.g. consider functions, systems and sites view points)¹? **[YES/NO]**
(Changes to scope should be highlighted on the list and figure 1 below, and explained on the next slide).

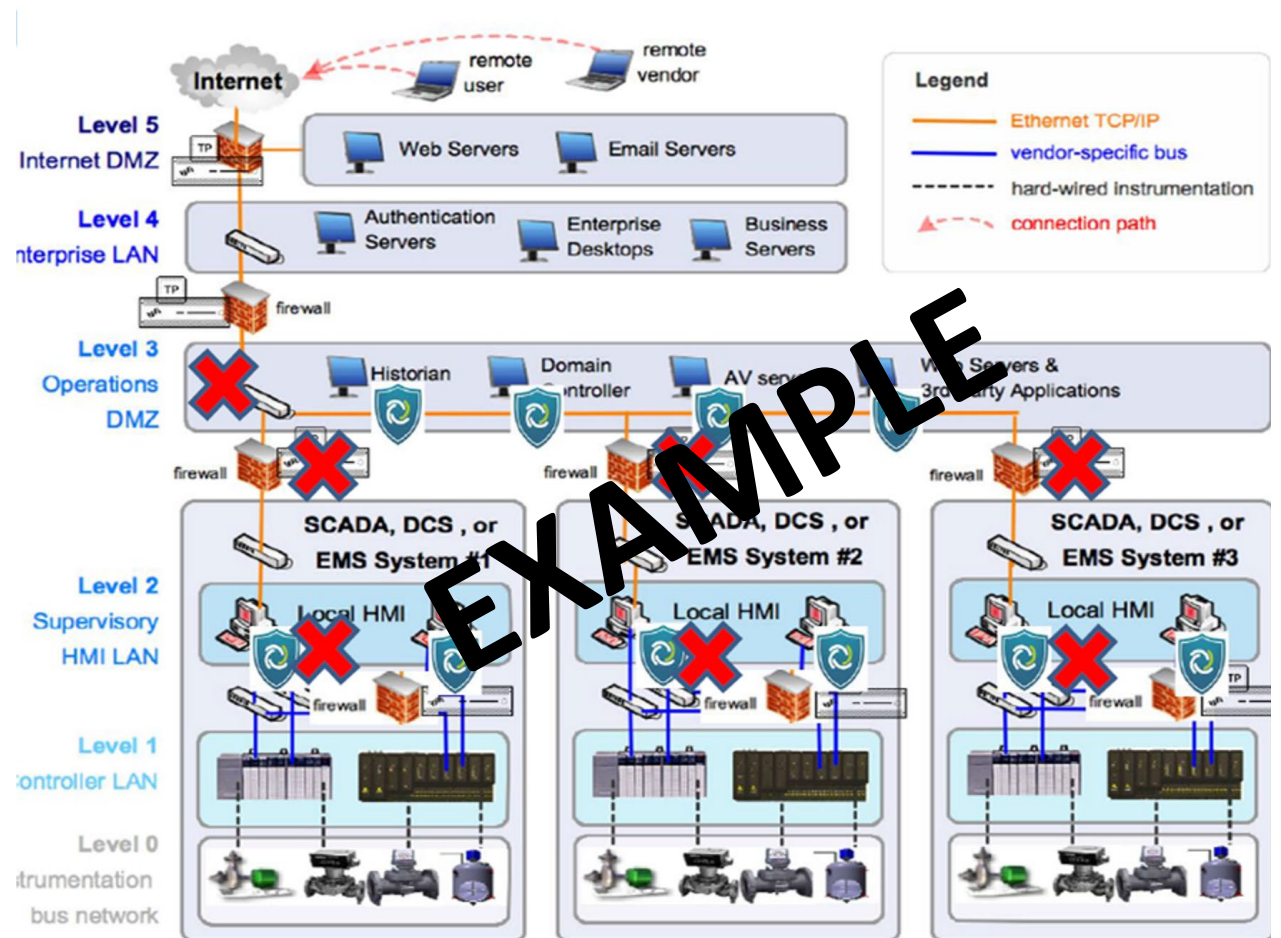
High-level list of systems within scope:

- Component 1
- Component 2
- Component 3
- Component 4
- Component 5
- Component 6
- Component 7
- Component 8

Note: This should remain the same after completing once, unless there are changes.

Further Information: See the following reference for further information on the different scope viewpoints - Part A: Overview and Scope. NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in Great Britain.

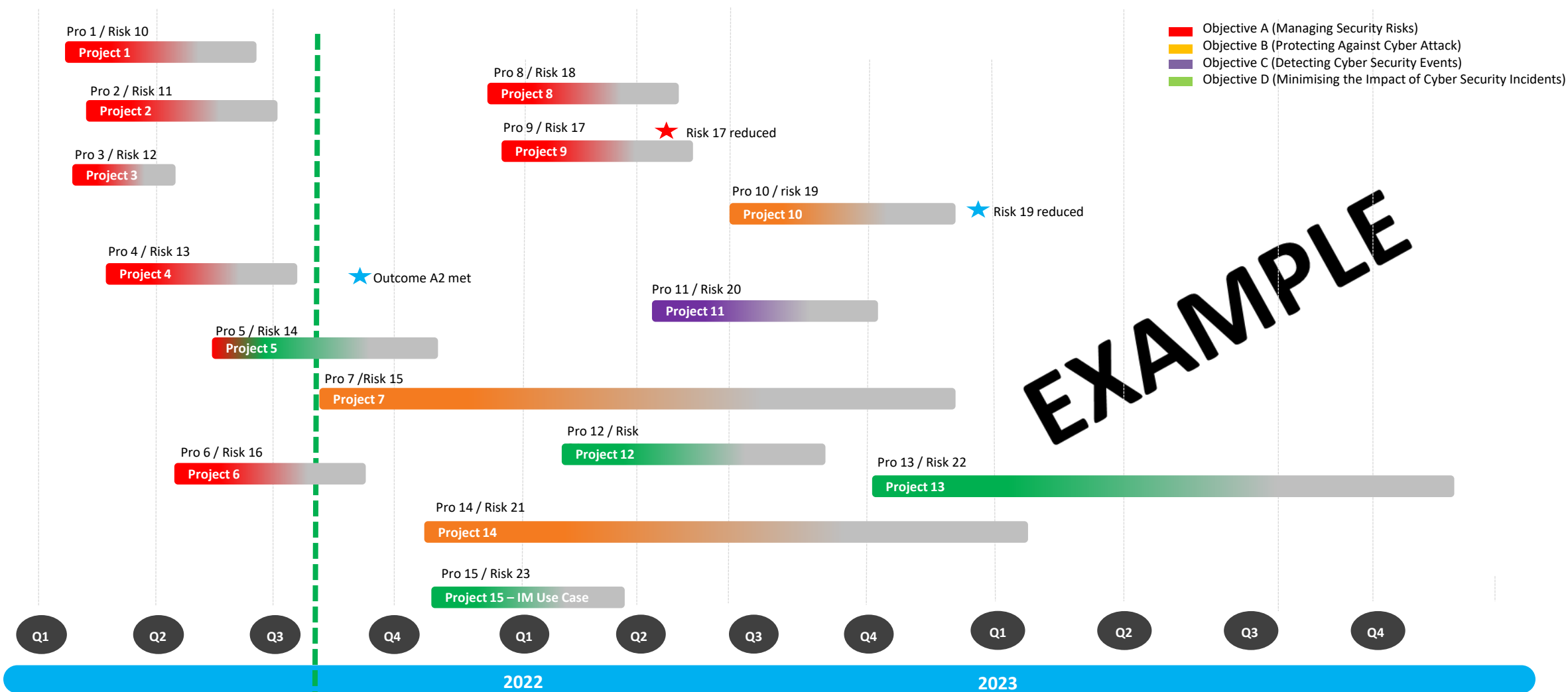
Figure 1: [OES] Purdue Model of System Scope



Scope change	Change type (e.g. Addition/descope/decommission)	Addition details (e.g. justification of a descope, decommissioning details)	Impact (e.g. in terms of impact to risk exposure, CAF target profile attainment and improvement plan status)	Date of change

Table 2: Change in NIS Scope

Further Information: OES should declare and confirm all changes to the NIS scope. If there is a reduction or de-scope, justifications are to be detailed. Decommissioning of an asset which is in-scope must still be reported upon with details of the decommissioning and risk exposure changes to the essential service documented. Also consider the impact to the CAF target profile attainment and improvement plan progress .



Further Information: This is a suggested format for a Gantt Chart.

Improve ment Plan ID	Initiative / Project Name	Initiative / Project Description	Applicable Scope / Improveme nt Area	Risk Ref No	Risk Criticality	Other Industry Framework Control reference	CAF Mapping –	Basic Profile and/or Enhanced Profile Maturity alignment	Start Date	Finish Date	Risk Tolerance
The reference ID	Name of initiative	Describe the initiative and include Project Control area (primary)	What scope does this apply to? And exclusions NIS Scope (site, system, geography etc.)	Any relevant risk reference ID (Should align with the ID from the RA)	Is the Improvemen t Plan mapped to a HIGH risk etc.?	Related control outcomes including compensating controls such as Physical security controls.	Related CAF outcomes	Which Profile is the initiative looking to meet or exceed?			Is the risk now within risk appetite? Yes, No If Yes, then revised risk criticality should be stated e.g. Medium or Low for a High risk If No, then current risk criticality should be stated.
[Example] PRO 15a	Phase 1 -OT incident management use cases.	Description: Create fully test and implement incident management use cases for top 10 cyber OT incident scenarios. Control: NIST RE. 1	Only Non production environment within the same network boundaries	Risk 23	High	e.g. PE-3 Physical Access Control	D1.a, D1.b, D1.c	BP	31 Oct 21	20 Dec 23	Yes, Low
[Example] PRO 15b	Phase 2 - OT incident management use cases.	Description: Create fully test and implement incident management use cases for top 10 cyber OT incident scenarios. Control: NIST RE. 1	All NIS scope – Production systems	Risk 23	High	e.g. PE-3 Physical Access Control	C1.a, C1.b, C1.c	EP	31 Oct 21	20 October 23	No, High

Statement which summarises OES Risk Appetite and Risk response should be noted here. This can be a summary statement from NIS Self Assessment Part B. For e.g. Risk response is 'Mitigate' for all Medium and High risk criticality etc.

CAF Target Profile Changes

Use this slide to report any changes to the CAF target profile you wish to share.

Further Information: For the Check-in Report, an Indicative CAF changes should be reported – As an OES delivers their improvement plans, it may be learned through cyber risk management, programme delivery or assurance processes that indicative risk reduction or CAF change has occurred. In these instances, OES should report on the indicative risk reduction or security and resilience changes that have occurred.

CAF Objective, Principle and Contributing Outcome		CAF Outcomes Changes
Objective A: Managing security risk	Contributing Outcome	Add information to indicate status of the changes as well. E.g., planned, in progress, or complete
Principle A1 - Governance	A1.a Board Direction	
	A1.b Roles & Responsibilities	
	A1.c Decision-making	
Principle A2 - Risk management	A2.a Risk Management Process	
	A2.b Assurance	
Principle A3 - Asset management	A3.a Asset Management	
Principle A4 - Supply chain	A4.a Supply Chain	
Objective B: Protecting against cyber-attack		
Principle B1 - Service protection policies and processes	B1.a Policy & Process Development	
	B1.b Policy & Process Implementation	
Principle B2 - Identity and access control	B2.a Identity Verification, Authentication & Authorisation	
	B2.b Device Management	
	B2.c Privileged User Management	
	B2.d Identity & Access Management	
Principle 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	
Principle B4 - System security	B4.a Secure By Design	
	B4.b Secure Configuration	
	B4.c Secure Management	
	B4.d Vulnerability Management	
Principle B5 - Resilient Networks and Systems	B5.a Resilience Preparation	
	B5.b Design for Resilience	
	B5.c Backups	
Principle B6 - Staff Awareness and Training	B6.a Cyber Security Culture	
	B6.b Cyber Security Training	
Objective C: Detecting cyber security events		
Principle C1 - Security monitoring	C1.a Monitoring Coverage	
	C1.b Securing Logs	
	C1.c Generating Alerts	
	C1.d Identifying Security Incidents	
	C1.e Monitoring Tools & Skills	
Principle C2 - Proactive security event discovery	C2.a System Abnormalities for Attack Detection	
	C2.b Proactive Attack Discovery	
Objective D: Minimising the impact of cyber security incidents		
Principle D1 - Response and recovery planning	D1.a Response Plan	
	D1.b Response & Recovery Capability	
	D1.c Testing & Exercising	
Principle D2 - Lessons learned	D2.a Incident Root Cause Analysis	
	D2.b Using Incidents to Drive Improvements	

Further Information: For the Check-in Report, a risk reduction should be reported – As an OES delivers their improvement plans, it may be learned through cyber risk management, programme delivery or assurance processes that risk reduction or CAF change has occurred. In these instances, OES should report on the risk reduction or security and resilience changes that have occurred.

Use this slide to provide an update of any NIS incidents or sub-threshold NIS incidents that have occurred

Further Information: For the Check-in Report an OES should provide an update of any NIS incidents that have occurred.