Making a positive difference for energy consumers

Consultation

Supply Chain Security: Proposed Guidance

Publication date:	2 June 2026
Response deadline:	29 June 2026
Team:	Cyber Strategy
Email:	CyberStrategy@ofgem.gov.uk

Contents

1. Introduction

This consultation supports the delivery of Ofgem's Forward Work Programme outcome themes by promoting resilient and secure supply chains that help protect the continuity, reliability, and resilience of energy services for consumers.

Purpose of this consultation

This consultation seeks views on Ofgem's draft Supply Chain Security Guidance for the Downstream Gas and Electricity (DGE) sector, and to inform refinement of the guidance prior to publication.

The consultation invites feedback on whether the proposed principles, outcomes, and supplier criticality model are sufficiently clear and usable, and whether they enable appropriate and proportionate, outcome-focused management of supply chain security risks in practice.

Ofgem is also seeking evidence on how the draft guidance aligns with existing operational, engineering, assurance, and commercial practices, including where further clarification or illustrative examples may be helpful.

The questions in this consultation relate to organisations delivering, supporting, or enabling essential services within the DGE sector. This includes suppliers whose products or services could affect the capability, control, stability, or resilience of essential energy functions.

Context and related publications

Supply chain security risks in the DGE sector may arise from the failure, compromise, or disruption of suppliers supporting operational technology, information systems, engineering services, data and analytics, or other critical capabilities. The nature and potential impact of these risks vary depending on supplier roles, levels of access, and the extent to which services are integrated into essential operations.

The intention is to follow this guidance with the development of overlays with indicators of good practice, working with stakeholders.

The guidance is intended to support these sources by providing a supply chain-specific, outcome-focused approach to encourage consistent appropriate and proportionate application within the DGE sector.

1.1 Ofgem and sector-specific regulatory guidance

- NIS Supplementary Guidance and CAF Overlay for the Downstream Gas and Electricity Sector

- Cybersecurity guidance and publications

1.2 UK regulatory and policy framework

- Implementation of the Network and Information Systems (NIS) Regulations 2018 – Energy sector (DESNZ)
- DESNZ policy guidance for the implementation of the NIS Regulations

1.3 NCSC frameworks and guidance

- Cyber Assessment Framework (CAF)
- NCSC Supply Chain Security Guidance

Overview

The DGE sector relies on a wide and dynamic range of third party suppliers to deliver, maintain, and operate essential energy functions. These relationships support everything from core operational technologies and digital platforms to engineering services, analytics, and specialist expertise. As the energy system becomes more digitalised and interconnected, the way organisations understand and manage supply chain security risk has become increasingly important.

Ofgem has developed draft Supply Chain Security Guidance to support a consistent, appropriate and proportionate outcome-focused approach to identifying and managing supplier-related security risks across the sector. The guidance is intended to help operators and suppliers establish shared expectations, while recognising the diversity of supplier roles, levels of access, and operational impact.

The consultation aligns with wider government policy development, and is consistent with the strategic objectives of the Cyber Security and Resilience Bill (CSRB), by supporting improved understanding and management of supply chain risks affecting Critical National Infrastructure (CNI) within the energy sector.

This guidance does not introduce new legal obligations but is informed by the competent authority's approach to supervision, which may inform supervisory, assessment, and engagement activities.

The draft guidance is structured around a set of outcome focused principles, supported by outcomes, broadly aligned in approach and style to the NCSC Cyber Assessment Framework (CAF), while remaining specific to supply chain security.

These elements are designed to support dialogue and transparency rather than replace organisational risk assessment, or act as a checklist or minimum compliance baseline. Equivalent or alternative approaches may be appropriate where they achieve the intended outcomes.

Ofgem intends for the guidance to evolve over time. This initial version is intended to establish a shared direction of travel and baseline clarity, with future iterations informed by stakeholder feedback, operational experience, and changes in technology, supplier models, and threat conditions.

Through this public consultation, Ofgem is seeking views from operators, suppliers, and other stakeholders on the clarity, proportionality, and usefulness of the draft guidance. Responses will help to identify areas that may benefit from refinement, additional explanation, or further examples, and to ensure the guidance supports good security outcomes without creating unnecessary burden or unintended consequences.

Consultation stages

Stage 1 Consultation open: 29th May 2026

Stage 2 Consultation closes (awaiting decision). Deadline for responses: 26th June 2026

Stage 3 Responses reviewed and published: August 2026

Stage 4 Consultation outcome (decision or policy statement): August 2026

Subsequent to publication, we will be developing draft overlays to provide additional guidance and will engage with stakeholders as appropriate.

How to respond

We want to hear from anyone interested in this consultation. Please send your response to the person or team named on the front page of this document.

We have asked for your feedback in each of the questions throughout. Please respond to each one as fully as you can.

We will publish non-confidential responses on our website.

Your response, data, and confidentiality

You can ask us to keep your response, or parts of your response, confidential. We will respect this, subject to obligations to disclose information. For example, under the Freedom of Information Act 2000, the Environmental Information Regulations 2004, statutory directions, court orders, government regulations, or where you give us explicit permission to disclose. If you do want us to keep your response confidential, please clearly mark this on your response and explain why.

If you wish us to keep part of your response confidential, please clearly mark those parts of your response that you do wish to be kept confidential and those that you do not wish to be kept confidential. Please put the confidential material in a separate

appendix to your response. If necessary, we will contact you to discuss which parts of the information in your response should be kept confidential and which can be published. We might ask for reasons why.

If the information you give in your response contains personal data under the General Data Protection Regulation (Regulation (EU) 2016/679) as retained in domestic law following the United Kingdom's withdrawal from the European Union ("UK GDPR"), the Gas and Electricity Markets Authority will be the data controller for the purposes of GDPR. Ofgem uses the information in responses in performing its statutory functions and in accordance with section 105 of the Utilities Act 2000. Please refer to our Privacy Notice on consultations, see Appendix 2.

If you wish to respond confidentially, we will keep your response confidential, but we will publish the number, but not the names, of confidential responses we receive. We will not link responses to respondents if we publish a summary of responses, and we will evaluate each response on its own merits without undermining your right to confidentiality.

How to track the progress of a consultation

1. Find the web page for the call for input you would like to receive updates on.
2. Click ‘Get emails about this page’, enter your email address and click ‘Submit’.
3. You will receive an email to notify you when it has changed status.

A consultation has three stages: ‘Open’, ‘Closed (awaiting decision)’, and ‘Closed (with decision)’.

2. Draft Supply Chain Security Guidance

How to use this guidance

This section explains how operators of essential services and their suppliers are encouraged to interpret and apply the principles and outcomes in a consistent, appropriate and proportionate way.

It introduces the supplier criticality assessment framework as a structured approach to understanding how different suppliers can affect essential functions, and how this should inform the level of oversight, assurance, and control.

Outcome-based

The guidance describes principles and outcomes illustrating typical ways an organisation may achieve those outcomes. Alternative approaches may be used where they achieve the same outcomes with equal or greater rigour.

Outcomes are not intended to represent a checklist or a set of required controls, and do not replace the need for informed expert judgement. They are non-exhaustive and should be interpreted as examples of the types of practices or evidence that may support confidence that outcomes are being achieved.

Outcomes provide a useful starting point for assessment but should be applied flexibly, taking into account the specific context, risks, and characteristics of the organisation and its supplier relationships. Conclusions should be based on a holistic view, including relevant operational, technical, and organisational factors.

Proportionate application based on supplier criticality

Expectations should be applied proportionately to how a supplier's products or services could affect essential functions. This guidance introduces a structured approach to assessing supplier criticality (Appendix 1) to support consistent and repeatable judgment considering relevant factors.

In general:

1. **Limited Impact suppliers** are typically substitutable and have limited potential to affect essential functions.
2. **Moderate Impact suppliers** may influence specific systems or workflows and could create contained disruption
3. **High Impact suppliers** may materially affect system capability, stability, control, or restoration, including where there is deep integration or persistent access.

Supplier criticality should inform how strongly the principles and outcomes are applied, including the level of oversight, assurance, and governance.

How operators can use this guidance

Operators should use the principles and outcomes to support a consistent, appropriate and proportionate approach to managing supply chain security risks. In practice, this may include:

- Informing procurement and contract development
- Supporting supplier assessment, oversight, and assurance activities
- Enabling consistent treatment of suppliers across business units
- Supporting internal decision-making on risk acceptance, mitigation, and escalation

How suppliers can use this guidance

Suppliers are encouraged to use the principles and outcomes to understand sector expectations and to support transparent and proportionate engagement with operators. This may include:

- Understanding expectations of lifecycle security, transparency, and operational practices
- Preparing appropriate evidence aligned to the supplier's role and criticality
- Structuring internal processes to demonstrate security maturity and accountability
- Supporting operator risk assessment, incident coordination, and continuous improvement

In many cases, existing certifications, standards, or engineering practices may be leveraged to demonstrate these are being achieved.

Using outcomes and the supplier criticality framework together

outcomes and the supplier criticality framework (Appendix 1) are intended to be used together to support appropriate and proportionate, outcome-focused judgement.

In practice:

- Outcomes should be considered selectively, following professional judgment and based on the supplier relationship and criticality
- Outcomes illustrate typical known-good approaches and should not be treated as required controls
- The criticality framework supports understanding how a supplier may affect essential functions and informs the level of expectation

- Different dimensions of the criticality framework should be considered individually, not combined into a single score
- Insights from the framework may indicate where additional controls, evidence, or governance may be appropriate

Professional judgment should be applied when using the supplier criticality framework (Appendix 1). The framework is intended to support structured and repeatable assessment but does not replace expert evaluation. Where assessments are adjusted or classifications are overridden, the rationale should be clearly documented.

Overview of the Supply Chain Security Principles

The guidance is structured around eight supply chain security principles describing outcomes for managing risks affecting essential functions.

To support consistency with established approaches, each principle is aligned at a high level to relevant elements of the Cyber Assessment Framework (CAF), together with indicative references to selected international frameworks and standards.

This alignment is intended to support understanding and interoperability. It is indicative rather than exhaustive, and does not imply a one-to-one correspondence between principles.

Supply chain security principle	**NCSC CAF alignment**	**Reference to standards/framework**
Governance and Impact-Driven Risk Management	A1 Governance A2 Risk Management	EU CRA (risk management obligations) IEC 62443-2-1 (organisational security management)
Framework-Aligned Defence and Foundational Security	B1 Policies and Processes B2 Identity and Access Control B3 Data Security	EU CRA (baseline security requirements) IEC 62443-2-4 (security requirements for IACS service providers) Cyber Essentials and Cyber Essentials + ISO/IEC 27001 Annex A control sets

		ISO/IEC 27002 guidance on control implementation
Secure Design, Product Security, and Technical Lifecycle Management	A3 Asset Management B4 System Security	EU CRA (secure development and lifecycle requirements) IEC 62443-4-1/4-2 (secure product development and technical security requirements)
Service Delivery Security and Managed Service Risk	A4 Supply Chain B2 Identity and Access Control B4 System Security	IEC 62443-2-4 (security requirements for IACS service providers) ISO IEC 27001 (Annex A - supplier relationships)
Transparency, Trust, and Assurance	A1 Governance A2 Risk Management A4 Supply Chain	EU CRA (technical documentation and conformity assessment) ISO/IEC 27001 (Annex A – supplier relationships) ISO/IEC 27036 (Information security for supplier relationships) NIST SP 800-161 (Cybersecurity Supply Chain Risk Management)
Proactive Vulnerability and Dependency Management	A2 Risk Management B4 System Security	EU CRA (vulnerability handling and disclosure obligations) ISO/IEC 29147 (vulnerability disclosure) ISO/IEC 30111 (vulnerability handling processes)

		Software Bill of Materials (SBOM) frameworks (e.g. SPDX, CycloneDX)
Incident Response and Coordination	C1 Security Monitoring C2 Threat Hunting D1 Response and Recovery Planning	EU CRA (incident reporting obligations) ISO/IEC 27035 (incident management) NIST SP 800-61 (computer security incident handling) ISO/IEC 29147 (vulnerability disclosure, coordination aspects)
Business and Operational Resilience	D1 Response and Recovery Planning D2 Lessons Learned	ISO 22301 (business continuity management systems) ISO 22316 (organisational resilience principles) NIST SP 800-34 (contingency planning) IEC 62443-2-1 (security program requirements, including resilience aspects)

Supply Chain Security Principles

This section sets out the supply chain security principles and assorted outcomes. Each principle describes an outcome that supports the secure and resilient delivery of essential functions.

For each principle, this section outlines the principle, describes how operators and suppliers can contribute to achieving it, and provides outcomes scaled according to supplier criticality.

Principle 1 – Governance and Impact-Driven Risk Management

Supply chain risks are continuously understood, owned, and managed through governance and risk management arrangements that reflect how supplier failure, compromise, or dependency could affect the capability, control, stability, or resilience of essential energy functions.

Operator considerations

Operators should consider:

- Assigning clear accountability for supply chain security at an appropriate level within the organisation
- Integrating supplier risk into existing governance and risk management processes, including clear escalation paths and criteria for use in relation to exceeding risk tolerances
- Assessing supplier criticality using Appendix 1 (or an equivalent approach) to support appropriate and proportionate oversight
- Ensuring that supply chain risks inform investment, design, and operational decision-making
- Reviewing supply chain risks where services, suppliers, or threat assumptions change

Supplier considerations

Suppliers are encouraged to consider:

- Understanding how their products or services support essential functions
- Assessing and communicating how failure or compromise could affect operator capability
- Maintaining internal governance for managing risks associated with their delivery
- Supporting operator risk assessment through the provision of accurate and timely information

Outcomes by supplier criticality

The following are provided for illustrative purposes only and are non-exhaustive.

Limited Impact Suppliers	**Moderate Impact Suppliers**	**High Impact Suppliers**
Supply chain risks are consistently incorporated into organisational risk assessments and influence overall risk posture. Responsibilities for delivery and security result in consistently reliable service performance and controlled risk exposure. Operators have sufficient visibility of supplier roles and substitutability to maintain service continuity under disruption.	Includes all Limited Impact Supplier outcomes Supplier-specific risks are actively managed such that they do not lead to unanticipated service degradation or disruption. Supply chain risk ownership at appropriate management levels results in timely and effective mitigation decisions. Dependencies and assumptions are well understood and enable continuity of service when conditions change. Risk review practices ensure that emerging changes or events do not introduce unmanaged risk to service delivery.	Includes all Limited and Moderate Impact Supplier outcomes Supply chain risks are effectively governed at senior levels, resulting in sustained service resilience under stress or attack. Escalation and ownership arrangements lead to rapid and effective response to supply chain risk events. Threat modelling and assumptions enable the organisation to anticipate and withstand realistic supply-chain-driven failures and attacks. Supply chain risk insight drives design and operational decisions that measurably improve resilience, reduce exposure, and maintain critical service delivery.

Principle 2 – Framework-Aligned Defence and Foundational Security

Suppliers maintain organisational and technical security measures appropriate to the level of access, influence, and capability impact their products or services may have on essential functions, and operators assess these measures appropriately and proportionately.

Operator considerations

Operators should consider:

- Defining baseline security expectations for suppliers, reflecting supplier criticality and established good practice frameworks
- Assessing whether supplier security measures are appropriate for the level of access and influence involved
- Identifying and applying compensating controls where supplier controls are limited or constrained
- Ensuring that security expectations are clearly communicated through procurement and contractual arrangements

Supplier considerations

Suppliers are encouraged to consider:

- Maintaining organisational and technical security practices appropriate to their role and level of access
- Applying security controls consistently across products and services used by operators
- Demonstrating how security measures reduce the risk of compromise or misuse
- Addressing gaps or weaknesses identified through assessment, assurance, or operational experience

Outcomes by supplier criticality

The following are provided for illustrative purposes only and are non-exhaustive.

Limited Impact Suppliers	**Moderate Impact Suppliers**	**High Impact Suppliers**
Supply chain security arrangements reduce the likelihood of accidental or opportunistic compromise affecting the operator's systems or services, as a result of consistent application of basic organisational security practices.	Includes all Limited Impact Supplier outcomes Security controls are applied consistently and at sufficient breadth and depth to prevent systemic weaknesses from leading to service compromise or degradation.	Includes all Limited and Moderate Impact Supplier outcomes Security controls are effective against targeted and capable adversaries, ensuring that critical services remain resilient under deliberate attack.

Access to operator systems and environments is constrained such that exposure is minimised and only necessary interactions occur, limiting the potential impact of misuse or compromise. Supplier environments are operated in a way that prevents unintentional or low-effort attacks from propagating to or affecting the operator's services.	Access to sensitive systems and data is controlled and monitored such that misuse, whether accidental or malicious, is detected and does not result in significant impact. Supplier environments are secured to a level that prevents compromise from spreading to operator systems, including through appropriate segregation and hardening measures. Operators have sufficient confidence in the effectiveness of supplier controls to make informed risk decisions and maintain service assurance.	Privileged access arrangements minimise the risk of abuse or compromise and enable rapid detection and response to anomalous or unauthorised activity. Constraints or limitations in supplier environments do not introduce unmanaged risk, as compensating measures ensure overall security outcomes are maintained. Security weaknesses with the potential to materially affect system capability are identified and resolved in a timely manner, preventing disruption to critical services.

Principle 3 – Secure Design, Product Security, and Technical Lifecycle Management

Products and technologies supporting essential functions are designed, implemented, and maintained to support secure and dependable operation throughout their lifecycle, with known dependencies, manageable risks, and appropriate ongoing support.

Applicability

This principle applies to suppliers providing products or technologies including hardware, software, platforms, and integrated technical components. Suppliers providing services only may be more appropriately assessed against Principle 4. Where suppliers provide both products and services, both principles may be relevant.

Operator considerations

Operators should consider:

- Assessing how product design and lifecycle decisions may affect system capability, control, and resilience
- Defining security and support expectations during procurement and design activities
- Reviewing and explicitly accepting risks associated with design constraints, legacy technologies, or unsupported components
- Planning for end-of-support and end-of-life impacts on essential functions
- Ensuring that dependencies, update mechanisms, and lifecycle constraints are sufficiently understood to support risk management and operational decision-making

Supplier considerations

Suppliers are encouraged to consider:

- Applying secure design practices appropriate to the product's role, impact, and connectivity
- Providing transparency over product architecture, dependencies, and update mechanisms where relevant to operational risk
- Supporting secure implementation, operation, and maintenance of products in operator environments
- Communicating lifecycle constraints, including support timelines, upgrade paths, and residual risks
- Maintaining processes for identifying, prioritising, and addressing vulnerabilities in line with the operational impact of the product

Outcomes by supplier criticality

The following are provided for illustrative purposes only and are non-exhaustive.

Limited Impact Suppliers	**Moderate Impact Suppliers**	**High Impact Suppliers**
Products are designed and configured such that they operate securely in their intended environments without introducing avoidable risk	Includes all Limited Impact Supplier outcomes Products are developed using consistent secure design practices, resulting in reduced likelihood of	Includes all Limited and Moderate Impact Supplier outcomes Products are demonstrably resilient to realistic and targeted

to the operator's systems or services. Deployed product configurations minimise exposure by avoiding unnecessary access, services, or dependencies, thereby reducing the likelihood of compromise or misuse. Operators are able to deploy products safely and consistently, supported by sufficient guidance to prevent common configuration errors that could lead to security weakness.	systemic vulnerabilities affecting essential functions. Dependencies and design assumptions are sufficiently understood to prevent unforeseen weaknesses from undermining secure operation in live environments. Products support effective maintenance practices, ensuring that vulnerabilities and misconfigurations can be addressed in a timely manner without disrupting essential services. Operators are able to deploy and operate products securely in their environments, with clear guidance that enables sustained secure use over time.	threats as a result of comprehensive and evidenced secure-by-design practices applied throughout development. Product architecture and dependency transparency enable effective risk assessment, informed decision-making, and timely incident response when issues arise. Vulnerabilities are managed proportionately to their operational impact, ensuring that issues affecting essential functions are prioritised and remediated before they can cause material harm. Risks arising from legacy or unsupported components are actively managed such that they do not lead to unmanaged exposure or disruption to critical services. Operators have sufficient visibility of product lifecycle information to plan, adapt, and maintain secure and resilient services over time.

Principle 4 – Service Delivery Security and Managed Service Risk

Services supporting essential energy functions are delivered securely and predictably, with controlled access, defined operational practices, and appropriate visibility of

dependencies, so that service delivery does not adversely affect system capability, control, stability, or resilience.

Applicability

This principle applies to suppliers providing services, including managed services, operational support, maintenance, monitoring, and professional services, particularly where these involve logical or physical access to operator environments. Suppliers providing products only may be more appropriately assessed against Principle 3. Where suppliers provide both products and services, both principles may be relevant.

Operator considerations

Operators should consider:

- Defining security expectations for service delivery, reflecting supplier criticality and the level and type of access provided
- Controlling and approving the level and method of supplier access to systems, environments, and sites
- Ensuring that service delivery risks are considered alongside product and system risks
- Maintaining visibility of subcontracted or upstream service dependencies
- Ensuring that service arrangements support effective incident response, coordination, and recovery

Supplier considerations

Suppliers are encouraged to consider:

- Delivering services in a manner consistent with agreed security and operational expectations
- Ensuring that staff, tooling, and access methods are appropriate to the sensitivity and impact of the service
- Maintaining oversight and assurance of any subcontractors involved in service delivery
- Supporting operator visibility, assurance, and incident coordination activities
- Managing changes to service delivery methods or access arrangements in a controlled and transparent manner

Outcomes by supplier criticality

The following are provided for illustrative purposes only and are non-exhaustive.

Limited Impact Suppliers	**Moderate Impact Suppliers**	**High Impact Suppliers**
Service delivery is carried out within clearly defined and controlled boundaries, resulting in predictable outcomes and reduced risk of unintended impact on operator systems or services. Access to operator systems and sites is constrained to only what is necessary, ensuring that exposure is minimised and opportunities for misuse or compromise are limited. Service activities are conducted in a manner that prevents accidental disruption or misuse, maintaining the stability and integrity of operator services during delivery.	Includes all Limited Impact Supplier outcomes Service delivery is performed through consistent and repeatable processes, reducing the likelihood of errors, inconsistencies, or unmanaged risks affecting service outcomes. Logical and physical access arrangements ensure that only authorised, time-bound access occurs, limiting the risk of unauthorised activity and enabling effective oversight. Use of subcontractors does not introduce unknown or unmanaged risks, as their involvement is visible and understood where it could affect service delivery or security. Operators have sufficient visibility of how services are delivered and controlled, enabling them to assess risk and maintain confidence in service integrity.	Includes all Limited and Moderate Impact Supplier outcomes Service delivery is actively governed and overseen, resulting in sustained control and assurance even under complex or high-risk conditions. Access with the potential to cause significant impact is tightly controlled and monitored, ensuring that inappropriate or malicious activity is detected and does not result in material harm. Subcontractors with the ability to affect critical services operate to equivalent security and delivery standards, ensuring that their involvement does not weaken overall assurance. Service delivery arrangements support effective incident response, recovery, and continuity, ensuring that disruption can be managed without loss of critical capability. Changes to service delivery methods or

		access do not introduce unmanaged risk, as impacts are understood and agreed in advance, maintaining service stability and resilience.

Principle 5 – Transparency, Trust, and Assurance

Outcome

Operators and suppliers maintain appropriate transparency over dependencies, architectures, risks, and security practices, supported by appropriate and proportionate assurance, so that supplier-related risks to essential functions can be understood and managed effectively.

Operator considerations

Operators should consider:

- Defining expectations for transparency and assurance, reflecting supplier criticality and the potential impact on essential functions
- Assessing and, where appropriate, challenging assurance evidence to support confidence in supplier practices
- Avoiding over-reliance on supplier assertions without appropriate supporting evidence
- Sharing relevant assurance findings with suppliers to support risk management and continuous improvement
- Treating gaps in transparency or assurance as a factor in risk assessment and decision-making

Supplier considerations

Suppliers are encouraged to consider:

- Providing accurate and timely information about their products, services, and dependencies where relevant to operational risk
- Supporting assurance activities appropriate and proportionate to their role and criticality
- Disclosing material changes that could affect risk, dependencies, or service delivery
- Engaging constructively with operators on assurance, risk management, and improvement activities

- Ensuring that internal processes support the generation and maintenance of reliable assurance evidence

Outcomes by supplier criticality

The following are provided for illustrative purposes only and are non-exhaustive.

Limited Impact Suppliers	**Moderate Impact Suppliers**	**High Impact Suppliers**
Service delivery is carried out within clearly defined and controlled boundaries, resulting in predictable outcomes and reduced risk of unintended impact on operator systems or services. Operators have sufficient insight into the supplier's resilience and security posture to understand potential risks to service delivery at a basic level. Where assurance is requested, operators are able to rely on reasonable attestations to support confidence that services are being delivered without introducing unmanaged risk.	Includes all Limited Impact Supplier outcomes Operators receive sufficient architectural or service-level information to enable meaningful assessment of risks associated with service delivery. Assurance arrangements provide credible evidence beyond self-assertion, enabling operators to form a reliable view of control effectiveness and associated risks. Changes that could materially affect service delivery, dependencies, or risk posture are identified and communicated in a timely manner, preventing unexpected impacts to operator services.	Includes all Limited and Moderate Impact Supplier outcomes Operators have visibility of key dependencies and subcontractors sufficient to ensure that risks to service capability are understood and managed across the supply chain. Assurance provided is robust enough to support high-impact decisions, enabling confident operation of critical services under conditions of elevated risk. Assurance findings actively inform joint risk management, design, and operational decisions, resulting in improved resilience and reduced exposure to supply chain threats. Gaps in transparency or assurance do not result in unmanaged risk, as they are identified, treated explicitly, and addressed

		to maintain confidence in service delivery and security.

Principle 6 – Proactive Vulnerability and Dependency Management

Vulnerabilities and dependency-related risks that could affect essential functions are identified, assessed, and managed in a timely and coordinated way, reducing the likelihood and impact of supplier-related disruption or compromise.

Operator considerations

Operators should consider:

- Defining expectations for vulnerability and dependency identification, disclosure, and communication, reflecting supplier criticality
- Assessing reported vulnerabilities and dependency issues for potential operational and systemic impact
- Integrating supplier-related vulnerabilities and dependencies into wider risk management, assurance
- Agreeing mitigation actions or compensating controls where risks cannot be addressed immediately
- Maintaining awareness of upstream dependencies and how issues could propagate across systems or services

Supplier considerations

Suppliers are encouraged to consider:

- Maintaining processes to identify and assess vulnerabilities and dependency risks in their products or services
- Communicating vulnerabilities and emerging risks that could materially affect operator capability in a timely and actionable way
- Supporting operators in understanding impact, mitigation options, and remediation timelines
- Monitoring upstream dependencies and assessing how issues could affect delivered services or products
- Prioritising the management of vulnerabilities and dependency risks in line with their potential impact on essential functions

Outcomes by supplier criticality

The following are provided for illustrative purposes only and are non-exhaustive.

Limited Impact Suppliers	**Moderate Impact Suppliers**	**High Impact Suppliers**
Known vulnerabilities relevant to delivered products or services are addressed in a timely manner, reducing the likelihood that exploitable weaknesses affect operator systems or service delivery. Operators receive timely information about issues that could reasonably affect service delivery, enabling them to take appropriate action to maintain service stability.	Includes all Limited Impact Supplier outcomes Vulnerabilities and dependency risks are consistently identified, assessed, and prioritised such that they do not result in unmanaged exposure or unexpected service impact. Operators are informed of vulnerabilities or dependency issues in sufficient time to prevent adverse effects on system behaviour, resilience, or recovery. Where immediate remediation is not possible, effective mitigation or workaround measures are implemented and communicated, ensuring that risk remains controlled.	Includes all Limited and Moderate Impact Supplier outcomes Vulnerability management activities ensure that risks are addressed in line with their potential operational impact, preventing material disruption to critical services. Dependencies with the potential to create systemic or cascading failures are actively managed such that their failure does not lead to widespread or uncontrolled service impact. Notifications regarding vulnerabilities and dependency risks enable timely, informed operational decision-making, supporting effective risk response under real-world conditions. Risks associated with legacy, unsupported, or hard-to-remediate components are actively controlled through joint understanding and

		management, preventing unacceptable exposure. Dependency-related risks are consistently incorporated into joint planning, resilience measures, and incident preparedness, resulting in improved readiness and reduced likelihood of service disruption.

Principle 7 – Incident Response and Coordination

Operators and suppliers maintain effective and compatible approaches to detecting, escalating, and managing incidents, enabling timely and coordinated action where supplier products or services contribute to, or are affected by, disruption or compromise of essential functions.

Operator considerations

Operators should consider:

- Maintaining incident response arrangements that explicitly account for supplier involvement
- Defining escalation paths, roles, and notification expectations for suppliers
- Ensuring that supplier responsibilities are understood within incident management processes
- Integrating supplier-related incidents into wider response, communication, and recovery activities
- Maintaining contact points and coordination mechanisms to support timely engagement during incidents

Supplier considerations

Suppliers are encouraged to consider:

- Maintaining incident response processes appropriate to the products or services they provide
- Notifying operators promptly where incidents could affect system capability, availability, or recovery
- Supporting operator incident response and restoration activities

- Providing information that is timely, accurate, and sufficient to support operational decision-making
- Participating in post-incident review and improvement activities where relevant

Outcomes by supplier criticality

The following are provided for illustrative purposes only and are non-exhaustive.

Limited Impact Suppliers	**Moderate Impact Suppliers**	**High Impact Suppliers**
Basic incident management arrangements ensure that issues affecting service delivery are reliably communicated to the operator, enabling awareness and appropriate response. Defined contact points and escalation routes enable timely communication, reducing the risk that incidents remain unreported or unmanaged.	Includes all Limited Impact Supplier outcomes Incident response capabilities ensure that events are managed in a structured and effective manner, reducing the likelihood of prolonged disruption or uncontrolled impact. Escalation arrangements provide operators with timely awareness of incidents, enabling informed decision-making and appropriate response actions. Information provided during incidents enables operators to understand the nature, impact, and recovery options, supporting effective management of service continuity.	Includes all Limited and Moderate Impact Supplier outcomes Incident response approaches are aligned and coordinated with operator processes, ensuring that incidents are managed effectively across organisational boundaries without gaps or delays. Incident notifications are timely, prioritised, and actionable, enabling operators to respond proportionately to the operational impact and maintain critical service delivery. Joint incident response activities ensure that both supplier and operator are prepared to respond effectively to complex or high-impact scenarios. Post-incident learning results in measurable improvements to systems, processes, and controls, reducing the

		likelihood or impact of future incidents.

Principle 8 – Business and Operational Resilience

Operators and suppliers are prepared for disruption or failure within the supply chain and are able to maintain, restore, or safely degrade essential functions, taking account of how supplier-related issues could affect wider systems or the sector.

Operator considerations

Operators should consider:

- Understanding where supplier failure could create single points of failure or wider systemic risk
- Exercising resilience arrangements to review and enhance relevant capability
- Incorporating supplier-related disruption scenarios into resilience and recovery planning
- Identifying alternative arrangements, workaround, or compensating controls where substitution is limited
- Ensuring that restoration priorities reflect operational, safety, and consumer impact considerations
- Considering how supplier disruption could propagate across systems and affect interconnected services or operators

Supplier considerations

Suppliers are encouraged to consider:

- Understanding how failure, degradation, or disruption of their products or services could affect operator capability and recovery
- Maintaining continuity and recovery arrangements appropriate and proportionate to their role and criticality
- Supporting restoration activities during supplier-related disruption
- Communicating constraints, dependencies, and recovery timelines clearly during disruption
- Incorporating lesson from disruption, incidents, or near-misses into improvements to design, delivery, or operational practices

Outcomes by supplier criticality

The following are provided for illustrative purposes only and are non-exhaustive.

Limited Impact Suppliers	**Moderate Impact Suppliers**	**High Impact Suppliers**
Disruption to the supplier's service does not result in material impact to the operator, as effects can be absorbed or effectively worked around to maintain service continuity. Basic continuity arrangements ensure that the supplier can continue to support service delivery or recover without introducing unmanaged disruption.	Includes all Limited Impact Supplier outcomes The effects of supplier disruption on operator systems and workflows are understood, ensuring that impacts are anticipated and do not result in unexpected service degradation. Continuity and recovery arrangements enable the supplier to restore service within a timeframe that avoids significant operational impact to the operator. Recovery dependencies and constraints are sufficiently understood and communicated to prevent delays or failures in restoring service.	Includes all Limited and Moderate Impact Supplier outcomes Supplier failure scenarios are incorporated into resilience planning, ensuring that critical services can continue or be restored under severe but plausible disruption conditions. Recovery and restoration arrangements enable the timely reinstatement of essential functions, preventing prolonged loss of critical capability. Dependencies that could delay or prevent restoration are actively managed, reducing the risk of systemic or cascading failure. Supplier-related disruption scenarios are considered jointly with operators, ensuring that wider system impacts are understood and mitigated. Lessons from disruptions and near-misses result in measurable improvements to resilience, reducing the

		likelihood and impact of future service failures.

Roles and ownership across the principles

While the guidance sets out operator and supplier considerations for each principle, effective supply chain security relies on shared responsibility and coordination between both parties.

The roles outlined below provide a consolidated view of how principle ownership is typically distributed across governance, delivery, and operational activities. The level of ownership and depth of expectation should be interpreted proportionately, reflecting supplier criticality, and are illustrative and non-exhaustive.

Governance and Impact-Driven Risk Management

Operator	Supplier	Shared
Set risk appetite and security expectations for suppliers Assess supplier criticality using Appendix 1. Ensure supply chain risk is governed at appropriate senior levels Explicitly decide on and document risk acceptance, escalation, and mitigation	Understand how products or services support essential functions Maintain internal accountability for security and delivery risk Provide accurate information to support operator risk assessment	Agree roles and escalation paths Review supplier risk following material change or incidents

Framework-Aligned Defence and Foundational Security

Operator	Supplier	Shared
Define security and support expectations during procurement Assess design and lifecycle risks to system capability and restoration	Apply appropriate secure design practices Disclose architecture, dependencies, and lifecycle constraints	Review high-risk design decisions Manage legacy or unsupported components Plan end-of-support and transition activities

Explicitly accept or reject residual or legacy risk	Provide support, patching, and upgrade paths consistent with impact	

Secure Design, Product Security, and Technical Lifecycle Management

Operator	Supplier	Shared
Approve and control supplier access to systems and sites Define acceptable access methods and conditions Maintain oversight of service delivery risk	Deliver services in accordance with agreed security and access constraints Ensure staff, tooling, and subcontractors meet required standards Limit access to only what is necessary for delivery	Agree access models and controls Manage changes to service delivery or access arrangements Coordinate service activities affecting critical systems

Service Delivery Security and Managed Service Risk

Operator	Supplier	Shared
Define expectations for vulnerability and incident notification Assess reported issues for operational and systemic impact Integrate supplier issues into incident and recovery management	Identify and assess vulnerabilities in products or services Notify operators of issues that could materially affect capability Support incident response and restoration activities	Coordinate incident handling and communication Agree mitigations where risks cannot be immediately removed Conduct post-incident reviews and apply lessons learned

Transparency, Trust, and Assurance

Operator	Supplier	Shared
Identify where supplier failure creates single points of failure	Understand how failure or degradation affects operators	Consider supplier failure scenarios in resilience planning

Maintain contingency plans and workarounds Prioritise restoration of essential functions	Maintain continuity and recovery arrangements proportionate to criticality Communicate recovery timelines and constraints clearly	Manage dependencies that affect restoration Improve resilience based on real-world disruption or near-misses

Incident Response and Coordination

Operator	Supplier	Shared
Maintain incident response arrangements that include supplier involvement Define escalation paths and notification expectations Integrate supplier incidents into response, communication, and recovery	Maintain incident response processes appropriate to role Notify operators promptly of relevant incidents Support response and restoration activities	Coordinate incident response activities and communications Align response approaches and escalation arrangements Conduct post-incident reviews and implement improvements

Business and Operational Resilience

Operator	**Supplier**	**Shared**
Identify systemic risks and supplier-related single points of failure Incorporate supplier disruption into resilience and recovery planning Prioritise restoration of essential functions	Maintain continuity and recovery capabilities proportionate to role Understand and communicate recovery constraints and dependencies Support restoration during disruption	Plan for disruption and failure scenarios Coordinate restoration priorities and activities Improve resilience based on incidents, disruptions, and lessons learned

Consultation Questions

Principles and coverage

Q1. In your view, do the principles address the relevant aspects of supply chain security risk in the downstream gas and electricity sector? Please explain, including any areas you consider out of scope, missing, over over-represented.

Q2. To what extent do the principles clearly and distinctly describe different supply chain security outcomes? Please comment on whether there are any areas where principles overlap, duplicate, could be clarified, or are already sufficiently distinct.

Outcomes

Q3. How would you assess the level of detail provided by the outcomes in terms of supporting understanding and usability?

Q4. Are there any areas where changes to the illustrative examples used in the outcomes would be helpful, or where the current examples are sufficient?

Supplier criticality and proportionality

Q5. To what extend does the supplier criticality framework describe the factors that influence supply chain security risk in practice?

Q6. Please comment on the clarity and usefulness of the individual criticality dimensions, including whether any are missing, redundant, difficult to assess, or appropriately defined as they stand.

Q7. How effective is the criticality framework in supporting appropriate and proportionate judgment in practice? Please comment on whether, and in what ways, it supports judgment, structured classification, or a combination of both.

Practical application and existing practice

Q8. Based on your experience, how could the guidance be applied across different supplier relationships, technologies, and operating contexts? Please comment on any practical considerations, including where application may be straightforward and where challenges may arise.

Q9. How does the draft guidance relate to standards, frameworks, or assurance approaches you currently use, including any areas of alignment, complementarity, duplication, or tension?

Iterative development

Q10. What are your views on developing this guidance over time, including whether an iterative approach informed by operational experience and stakeholder feedback is appropriate? Please include any views on what should trigger future updates.

Open feedback

Q11. Are there any other issues, unintended consequences, or areas of ambiguity you consider important to highlight, or any additional observations you wish to make?

About your response

This section is optional and intended only to help us understand the context of responses.

Q12. Are you responding as:

a) An individual
b) On behalf of an organisation

Q13. If responding on behalf of an organisation, which best describes your organisation's role in relation to the downstream gas and electricity sector? Please select all that apply:

a) Operator of energy infrastructure or services
b) Supplier of products or services to the energy sector
c) Service provider, systems integrator, or managed service provider
d) Equipment or technology manufacturer
e) Trade body or industry association
f) Academia or research organisation
g) Other (please specify)

Q14. If you are replying as an operator or supplier, please indicate the subsector(s) you most closely work with or supply into:

a) Gas transmission, distribution, or system operation
b) Gas supply or shipping
c) Gas interconnection or cross-border infrastructure
d) Electricity generation
e) Electricity transmission, distribution, or system operation
f) Electricity supply
g) Smart meter or communications infrastructure
h) Carbon dioxide transport and storage
i) Other energy-related subsector (please specify)

Send us your feedback

We believe that consultation is at the heart of good policy development. We are keen to receive your comments about this consultation. We would also like to get your answers to these questions:

- Do you have any comments about the quality of this document?
- Do you have any comments about its tone and content?
- Was it easy to read and understand? Or could it have been better written?
- Are its conclusions balanced?
- Did it make reasoned recommendations?
- Do you have any further comments?

Please send your feedback to stakeholders@ofgem.gov.uk.

Appendix 1. Supplier Criticality Assessment

This appendix provides a structured framework for assessing supplier criticality based on how supplier failure, compromise, or dependency could affect essential functions.

The framework considers a set of dimensions relating to supplier stability, access and influence, impact and propagation, and supplier criticality. These dimensions are used to inform professional judgment about the level of risk posed by a supplier relationship.

The framework is not intended to produce a single composite score or automated classification. Instead, it supports consistent and repeatable assessment, enabling expectations for governance, assurance, and control to be applied proportionately.

This framework is intended to align conceptually with established approaches to assessing security and resilience, including the NCSC CAF and relevant international standards such as IEC 62443. It focuses on understanding the potential impact of supplier failure or compromise, including factors such as access, dependency, and propagation within supplier relationships, rather than providing a full assessment of risk or prescribing specific control measures.

How to Use This Model

The model should be used to:

- understand how a supplier could affect essential functions
- inform the classification of suppliers as Limited, Moderate, or High Impact justify appropriate and proportionate expectations during procurement, assurance, and oversight
- support clear communication of supplier risk internally and with suppliers

The model is not intended to produce a single composite score. Each dimension should be considered individually, with particular attention paid to high scores in dimensions relating to access, propagation, restoration difficulty, and functional impact.

Re-assessment should occur when:

- supplier scope, access, or delivery model changes
- products reach end-of-support or end-of-life
- new dependencies or subcontractors are introduced
- threat conditions or system architectures change
- significant incidents or near-misses occur

The output of this model determines how strongly the expectations set out by the principles apply to a supplier. It does not introduce additional requirements, but

provides a model for assessing proportionality across governance, assurance, design, service delivery, vulnerability management, incident coordination, and resilience.

Assessment Approach

Each dimension is scored on a 1-5 scale, where higher scores indicate greater potential impact or influence. Some dimensions may not be applicable (N/A) depending on the supplier offering and relationship.

Scoring should assume credible worst-case conditions, including malicious control, not simply accidental failure or unavailability.

Dimensions

Group	Factor	Factor	Factor
Supplier Stability	A1.1 Financial Health	A1.2 Operational Stability	A1.3 Geopolitical and Jurisdictional Behaviour
Access and Influence	A1.4 Technical Access	A1.5 Physical Access	A1.6 Data Access
Impact and Propagation	A1.7 Velocity of Impact	A1.8 Propagation Potential	A1.9 Restoration Difficulty
Supplier Dependency	A1.10 Service Permanence	A1.11 Functional Criticality	A1.12 Substitutability

Supplier Stability Factors

These dimensions consider the inherent resilience of the supplier organisation and its exposure to potential systemic threats.

A1.1 Financial Health

Ability to sustain service delivery and support obligations on a continuing economic basis.

- Low scores indicate strong financial resilience.
- High scores indicate material risk of service disruption due to financial instability.

A1.2 Operational Stability

Reliability of the supplier's delivery, support, and operational capability.

- Low scores indicate a consistent record of reliable performance to a measurable standard.
- High scores indicate fragile delivery, limited operational capacity, or reliance on single points of failure (key individuals, facilities, or sub-suppliers with limited resilience).

A1.3 Geopolitical and Jurisdictional Exposure

Exposure to jurisdictions, ownership structures, or legal regimes that could introduce strategic, legal, or coercive risk.

- Not Applicable (N/A) where there is no exposure to non-UK jurisdiction, legal regimes, or ownership – i.e. fully owned and operated within the UK, and no operations in regimes with applicable extra-national legislation.
- Low scores indicate exposure only to stable, aligned regimes and jurisdictions.
- High scores indicate exposure to, ownership by, or dependency on unstable or hostile regimes and jurisdictions.

Access and Influence Factors

These dimensions describe what the supplier can access or control, and the degree of supervision applied.

A1.4 Technical Access

Level of logical or system access to operator environments, including administrative or control access.

- Not Applicable (N/A) where there is no logical or system access to operator environments.
- Low scores indicate low-privilege access, i.e. less sensitive systems, read-only access, supervised and brokered remote access, or similar.
- High scores indicate high-privilege access such as control access to critical systems, unsupervised maintenance access to OT systems, and similar.

A1.5 Physical Access

Extent of access to sites, equipment, or operational environments.

- Not Applicable (N/A) where there is no physical access to sites, equipment, or operational environments or infrastructure.
- Low scores indicate access only to non-sensitive areas, or strongly supervised access.
- High scores indicate access to sensitive areas, especially where the access is unsupervised.

A1.6 Data Access

Access to data that could enable disruption, misuse, or loss of control, where such access has a plausible path to operational impact.

- Not Applicable (N/A) where there is no access to data, or where there is no plausible path for the data to cause an operational impact to the essential services.
- Low scores indicate access to data where there are low-plausibility paths to cause an operational impact, such as where data may be useful for hostile reconnaissance.
- High scores indicate access to sensitive data with highly plausible paths to cause or enable operational impacts.

Impact and Propagation Factors

These dimensions describe how supplier issues could affect essential functions.

A1.7 Velocity of Impact

How quickly a failure or compromise could affect operations once initiated.

- Not Applicable (N/A) where there is no vector through which a failure or compromise could affect operations regardless of timeline.
- Low scores indicate slow propagation, allowing a timeline to proactively respond to any failure or compromise to prevent any impact to operations.
- High scores indicate rapid propagation, where the timeline would not allow a proactive response to any failure or compromise to prevent impact to operations.

A1.8 Propagation Potential

Extent to which the impact could spread across systems, services, operators, or the wider sector.

- Not Applicable (N/A) where there is no potential for impact to affect any level of operations.
- Low scores indicate limited scope propagation, where any impact would be tightly contained to a defined, manageable boundary and is more likely to degrade than cause failure of operations.
- High scores indicate wide scope propagation, where any impact would not be contained to an identifiable boundary or where the boundary includes a significant proportion of operations.

A1.9 Restoration Difficulty

Effort, coordination, and time required to restore capability following supplier-related failure or compromise.

- Not Applicable (N/A) where operations do not depend on restoration of the product or service, or where restoration is instant and automatic (e.g. failover to a redundant system which would not be affected by the same failure).
- Low scores indicate trivial restoration of operations following an impact, where minimal manual or diagnostic effort would be required.
- High scores indicate complex restoration following an impact, which may include up to reconstruction of facilities or replacement of highly bespoke services.

Supplier Dependency Factors

These dimensions reflect how embedded and replaceable the supplier is.

A1.10 Service Permanence

Duration and persistence of the supplier's presence in the operational environment.

- Not Applicable (N/A) where the supplier provides ad-hoc services or products and there is no long-term dependency on their offerings.
- Low scores indicate short-term relationships such as supply of largely commodity products or services which do not require a long-term commitment.
- High scores indicate long-term relationships such as products requiring maintenance contracts and services which require a long-term relationship.

A1.11 Functional Criticality

Degree to which a supplier failure could degrade or interrupt essential functions.

- Not Applicable (N/A) where there is no vector by which a supplier failure could degrade or interrupt essential functions.
- Low scores indicate that a supplier failure may cause limited degradation of essential functions but could not cause interruptions or significant degradation.
- High scores indicate that a supplier failure may cause significant degradation of essential functions, or could cause interruption or loss of control.

A1.12 Substitutability

Ease of replacing the supplier or migrating away from their product or service.

- Not Applicable (N/A) where the supplier could be replaced with little effort, such as a commodity supplier of standardised parts or services purchasable off-the-shelf from multiple suppliers.
- Low scores indicate that a supplier could be replaced with a level of effort, but the effort would be focused on identifying and securing a new supplier.
- High scores indicate where a supplier would require significant effort, especially where products and services are entrenched and would require replacement.

Interpreting Results

Supplier criticality should be determined by patterns across dimensions, not numerical aggregation.

In general:

- **Limited Impact Suppliers**: Low scores across most dimensions, high substitutability, limited access or impact.
- **Moderate Impact Suppliers:** Moderate scores in access, functional impact, or restoration difficulty, where disruption would be contained but meaningful.
- **High Impact Suppliers:** High scores in one or more of: access and influence, impact and propagation, and supplier criticality factors.

A single high score in certain dimensions (for example, rapid and wide-scope propagation) may be sufficient to treat a supplier as High Impact, even if other scores are lower.

Classification Process

The following process can be used in combination with outputs of the framework to categorise suppliers as Low, Moderate, or High Impact.

It translates the individual scores into a repeatable classification outcome, without relying on composite scoring or averaging. Note that at all stages expert, professional judgement should be primary when applying classifications.

Design Principles

This framework is based on the following principles:

- Individual high-impact scores dominate classification decisions
- No scores are combined or averaged
- Some dimensions are decisive on their own

- Proportionality is through gated escalation, not totals
- Professional judgement is encouraged, but must be justified and recorded

This process assumes:

- Scoring has been completed
- Each dimension has been scored 1-5 or N/A
- Scoring reflects credible worst-case scenarios, including malicious control

Classification Flow

Step 1) If any of the following dimensions score 5, the supplier is classed as High Impact:

- Technical Access
- Physical Access
- Functional Criticality
- Propagation Potential
- Restoration Difficulty

These dimensions represent direct control, systemic propagation, or irrecoverable impact.

Step 2) If two or more of the following dimensions score 4 or higher, the supplier should normally be classed as High Impact.

- Technical Access
- Propagation Potential
- Impact Velocity
- Functional Criticality
- Substitutability

Step 3) If the supplier does not meet Critical criteria, assess the following:

If any of the following dimensions score 4, or multiple score 3, the supplier should be classified as Moderate Impact:

- Technical Access
- Physical Access
- Data Access
- Restoration Difficulty
- Service Permanence
- Functional Criticality

Step 4) A supplier may be classified as Low Impact only where all of the following conditions are met:

- No dimension scores higher than 3
- Technical Access, Physical Access, Functional Criticality, Substitutability, and Propagation Potential score 2 or below

Stability Rule

If classification would change category due to marginal score changes, the higher category should be retained until:

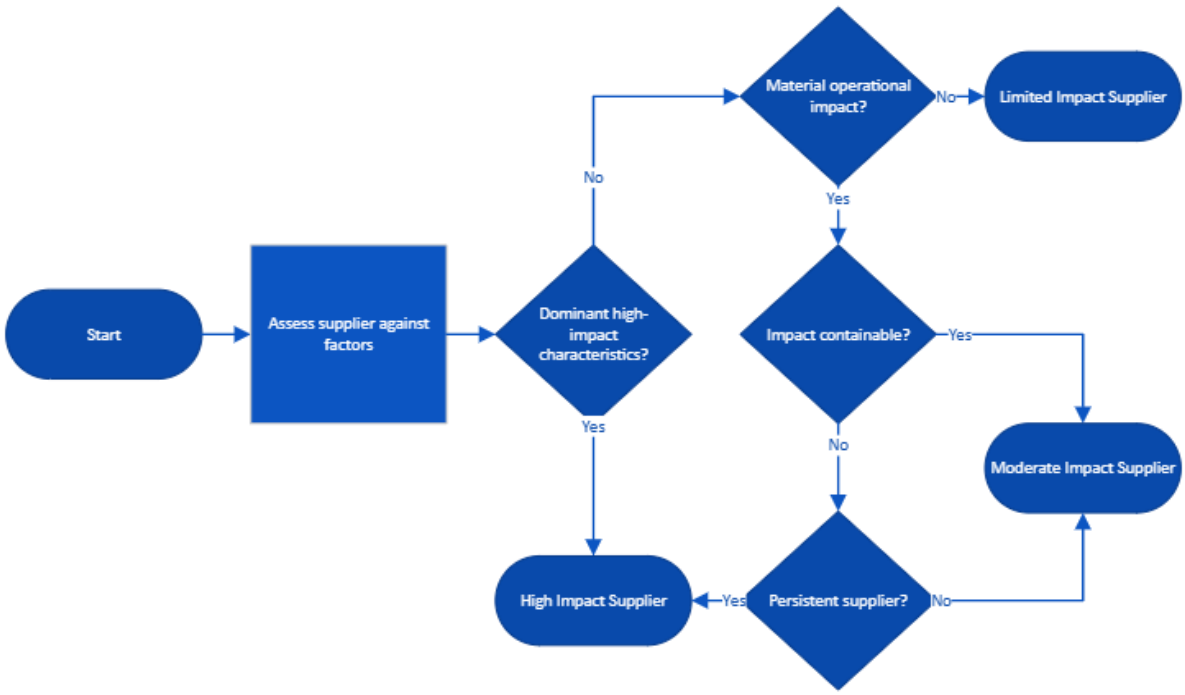
- compensating controls are in place and
- reduced risk is evidenced

Recording Output

For each supplier, organisations should record:

- Scores for each dimension
- Final classification
- Any override applied and justification
- Date of assessment and review trigger

Supplier Criticality Flow Chart



Appendix 2. Privacy policy

Personal data

The following explains your rights and gives you the information you are entitled to under the General Data Protection Regulation (GDPR).

Note that this section only refers to your personal data (your name address and anything that could be used to identify you personally) not the content of your response to the consultation.

1. The identity of the controller and contact details of our Data Protection Officer

The Gas and Electricity Markets Authority is the controller, (for ease of reference, "Ofgem"). The Data Protection Officer can be contacted at dpo@ofgem.gov.uk

2. Why we are collecting your personal data

Your personal data is being collected as an essential part of the consultation process, so that we can contact you regarding your response and for statistical purposes. We may also use it to contact you about related matters.

3. Our legal basis for processing your personal data

As a public authority, the GDPR makes provision for Ofgem to process personal data as necessary for the effective performance of a task carried out in the public interest. i.e. a consultation.

4. With whom we will be sharing your personal data

We will not share your personal data with any third parties. Anonymised summaries may be shared with organisations including the National Cyber Security Centre, the Department for Science, Innovation and Technology, the National Energy System Operator, and the Department for Energy Security and Net Zero.

5. For how long we will keep your personal data, or criteria used to determine the retention period.

Your personal data will be held for up to 12 months after the project is closed, including subsequent projects or legal proceedings regarding a decision related to this consultation.

6. Your rights

The data we are collecting is your personal data, and you have considerable say over what happens to it. You have the right to:

- know how we use your personal data

- access your personal data
- have personal data corrected if it is inaccurate or incomplete
- ask us to delete personal data when we no longer need it
- ask us to restrict how we process your data
- get your data from us and re-use it across other services
- object to certain ways we use your data
- be safeguarded against risks where decisions based on your data are taken entirely automatically
- tell us if we can share your information with 3rd parties
- tell us your preferred frequency, content and format of our communications with you
- to lodge a complaint with the independent Information Commissioner (ICO) if you think we are not handling your data fairly or in accordance with the law. You can contact the ICO at https://ico.org.uk/, or telephone 0303 123 1113.

7. Your personal data will not be sent overseas.

8. Your personal data will not be used for any automated decision making.

9. Your personal data will be stored in a secure government IT system.

10. More information For more information on how Ofgem processes your data, click on the link to our Ofgem privacy promise.