INDUSTRIAL CONTROL SYSTEMS
Community of Interest

Guidance for developing supply chain incident response and management within your organisation.

This guidance supports Critical National Infrastructure (CNI) operators and their third parties in establishing robust incident response and management capabilities across the supply chain. It caters for Information Technology (IT) and Industrial Control Systems/Operational Technology (ICS/OT) environments and helps organisations prepare for, detect, respond to, and recover from cyber-related incidents that impact shared services and dependencies. It aligns to NCSCs Cyber Assessment Framework (CAF) 4.0 principles, a summary of which can be found at the end of this guidance.

Security, resilience, and risk professionals, as well as procurement, legal, engineering, and incident response teams, can benefit from this guidance, as would Managed (Security) Service Providers (MSPs/MSSPs), system integrators, and vendors supporting ICS/OT operations.

This document enables you to consider how your organisation or those you work with can address incident management in the supply chain context. It builds upon current Supply Chain Risk Management (SCRM) guidance and bridges a current gap by incorporating incident response and management into current SCRM programmes and vice versa. It is not prescriptive, as each organisation will have risks and control objectives pertinent to its individual business objectives.

Important Note: *While the ICS COI is supported by the NCSC, and NCSC staff are involved in a range of its activities, no formal review of this guidance article has been undertaken by the NCSC. The ICS COI and its members strive to produce relevant ICS/OT specific cyber security guidance to supplement principle based cyber security guidance published by NCSC and have taken care to reference this guidance where applicable. This guidance article will be reviewed every 18 months to ensure that it*

has not been superseded by guidance published by NCSC, relevance and that any references are still accurate. The ICS COI and its activities are purely voluntary, with guidance articles produced that are deemed needed by UK Operators and their supportive industry partners. The fact that this guidance article has been published by the ICS COI has no relevance to the priority and focus of guidance published by NCSC.

This guidance uses the ROSE taxonomy [Fig 1] for Supply Chain Risk Management. (Topping, et al. 2021). ROSE (Risk, Ownership, Service, and End-2-End) is broken down into subcategories that, in turn, have attributes that are detailed in Annex A.

Technologies and services can also make a supplier a crucial partner in effective incident prevention, detection, response, and recovery. This is often especially true for Managed Security Service Providers (MSSPs), security vendors, security consultants, and IT/OT[1] service providers.

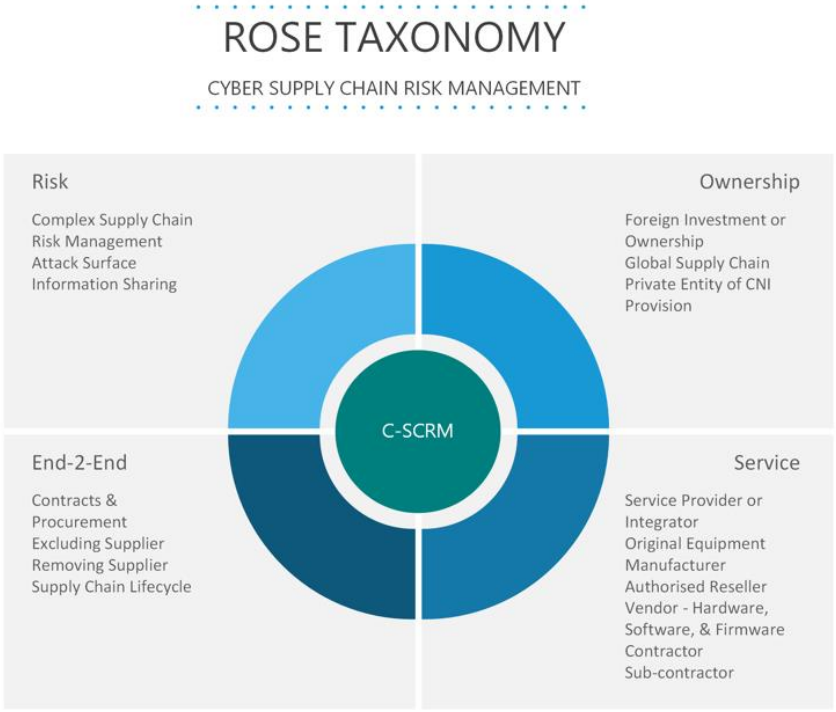


Figure 1: ROSE Taxonomy [Adapted from Beware Suppliers Bearing Gifts]

Structure of this Guidance

The guidance follows the structure of other ICS COI publications and includes:

- Introduction and Context
- Key guidance sections on supply chain incident management
- CAF Indicators of Good Practice
- Annex A – ROSE Taxonomy
- Annex B – References and Further Reading

[1] OT (Operational Technology) is also used to cover ICS (Industrial Control Systems), CPS (Cyber-Physical Systems), and IIOT (Industrial Internet of Things).

Introduction and Context

Current guidance can often be used as a high-level framework for IT and OT environments. Most advice suggests that organisations should incorporate the supply chain in their Incident Response Plan (IRP) but does not provide specific guidance on how this can be done. Actions required for incident response may also be considered for other third parties[2], such as partners, subsidiaries, joint ventures, customers, etc.

Current Risk Management Guidance

The NCSC provides guidance and e-learning modules on supply chain cyber security. It includes a five-stage approach [Fig 2] that details the through-life actions to consider in assessing cyber security in the supply chain. It doesn't, however, consider how to prepare for or respond to a cyber incident in the supply chain or address the specific context of ICS/OT.

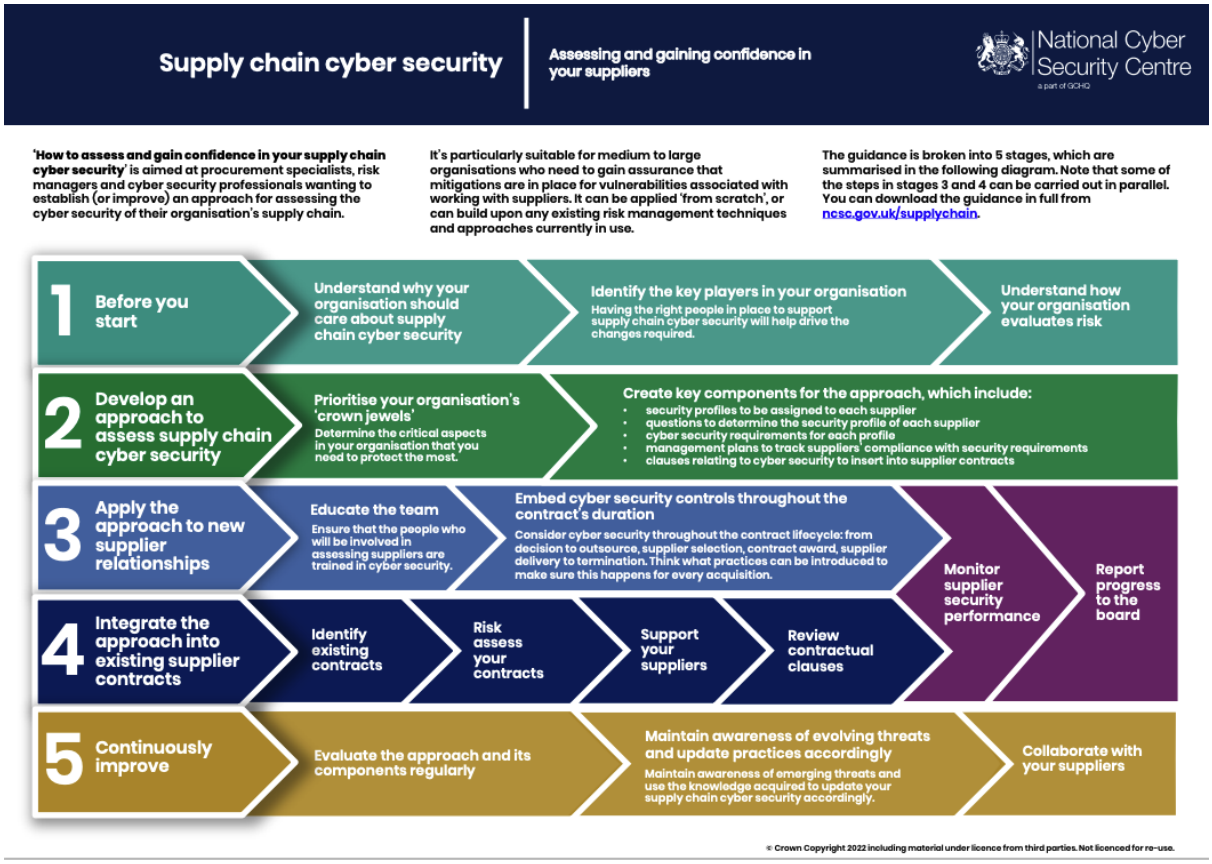


Figure 2: 5 Stages of the NCSC Guidance. (Approval received to reuse)

In more general guidance, the NCSC Board Toolkit Principle A (Risk Management) has a section on "collaborating with your supply chain and partners" to enhance your cyber

[2] Supplier and 3rd Party are used interchangeably in this document. The 3rd party may extend to Partners, Subsidiaries, Joint Ventures, and even Customers.

security outcomes, although incident responsibilities are largely focused on reporting requirements.

The MITRE Corporation has curated knowledge bases that model threat actors' tactics, techniques, and processes (TTPs) to provide a visual representation that organisations can use to strengthen their security posture. It is well known for its ATT&CK Matrix for Enterprise and has a corresponding Matrix for ISC/OT Systems. As well as focusing on threats, MITRE has also done work that helps manage risk mitigation. In 2022 MITRE released the Supply Chain Security System of Trust (SoT) Framework and followed it up in 2023 with a cloud-based prototype platform used for assurance called the Risk Model Manager (RMM) platform. The SoT details many aspects of SCRM and covers some of the ROSE categories too. It does include Incident Response (RF-428), but this relates to the adequacy of the training employees have received to respond to security incidents.

The National Institute of Standards and Technology (NIST) has six laboratories. One of these is the IT Laboratory (ITL) which delivers research and guidelines under the 800-series of Special Publications. NIST SP 800-53 covers the Risk Management Framework, and it was enhanced under revision 5 to include several controls and enhancements related to C-SCRM, including Incident Handling and Reporting relating to supply chain coordination. This contains assessment objectives and potential assessment methods and objectives to examine, interview, and test against, but no specific guidance on what good looks like.

NIST Cybersecurity Framework (CSF) 2.0 includes specific SCRM outcomes, which are primarily found in the new Govern function as the category SCRM (GV.SC-01 to 08), as well as in other categories, under Identity (ID.AM-06), Protect (PR.AA-05), Detect, Respond, and Recover. (Fig 3)

Category	Outcome ID	Description
GV.SC	GV.SC-01 to 08	Dedicated SCRM controls covering strategy, contracts, monitoring, etc.
ID.AM	ID.AM-06	Cataloging of external/third-party systems
PR.AA	PR.AA-05	Controlling and limiting access by third parties
DE, RS, RC	Various	Broader incident detection and response outcomes that may involve third parties

Figure 3: NIST CSF 2.0 Functions and supplier/third party-related categories

Current Incident Management Guidance

Incident management guidance promotes a standardised approach that captures the proactive element of planning and preparing for an incident through to identifying the areas to address when an incident occurs. This involves detecting and analysing a potential

incident through to containment actions that need to occur before eradication activities can happen. The post-incident activity will include a lessons-learnt aspect.

The two principal guidance documents are NIST SP 800-61r3 (2025) and ISO/IED 27035:2023. NIST documents are free, whereas ISO charges for their publication. This may be a factor when considering compliance/guidance for smaller organisations within the extended supply chain with limited funds. NCSC and the US Cybersecurity & Infrastructure Security Agency (CISA) have also released detailed guidance that is freely available and covers both IT and OT, while the ICS/COI also has specific incident response guidance for OT environments.

The following advice builds on this guidance to focus on the supply chain. It signposts how the threat has increased exponentially as organisations have become more reliant on the extended supply chain referenced in the ROSE taxonomy, as threat actors have seen the opportunity for a greater return on investment in targeting the trusted relationship between client and supplier. It then offers some contractual opportunities for procurement to consider before promoting the sharing of cyber awareness to develop a mature cyber culture within the organisation and out to the supply chain.

Risk and Threat

Your organisation may wonder how important your supply chain is when considering cyber security risk, and the answer will be that every company, no matter how large or small, is finding that this is a critical issue, particularly in the context of OT. The global digital supply chain is complex and offers a broad and deep attack surface for threat actors to target. The inherent trust that businesses have in their supply chain has been used to circumvent the controls businesses have at a local level. Mandiant highlighted this in their M-Trends 2022 report, identifying that the initial attack vector positioned the supply chain as the second most prevalent vector (after exploits), accounting for 17% of intrusions they investigated in 2021, compared to less than 1% the previous year.

Another example of threat actors looking to compromise managed service providers was illustrated by the international 5-Eyes community issuing a joint alert with recommendations that included "*understanding and proactively managing supply chain risk*" and "*developing and exercising incident response and recovery plans*".

Because suppliers have touchpoints with multiple customers, commercial software, and software-as-a-service (SaaS) are increasingly viewed as the weapon of choice for threat actors to compromise multiple organisations. Targeting a single entity to compromise many offers a greater return on investment. For example, this was used to significant effect by Russia in a political and destructively motivated attack on Ukraine, an attack that became known as the "NotPetya" attack. The attackers compromised accounting software, MeDoc, used by 90% of Ukrainian businesses. Malware was injected at the source and was distributed by the software supplier as part of trusted updates. This proved devastating to software users when the malware was activated on 27 June 2017. The software provider was as ignorant of the problem as the customers infected with the destructive ransomware.

This compromise transcended the Ukrainian international borders and compromised multiple global organisations, resulting in estimates of $10 Billion in costs [Wired].

NTT has also reported a significant shift of attacks to critical infrastructure and supply chains in their 2022 Global Threat Intelligence Report. Technology accounted for 21% of attacks, with manufacturing accounting for 14% of attacks. Researchers published a record 21,957 new vulnerabilities in 2021, an average of a new vulnerability every 24 minutes of the year. Much of this was against the software supply chain, which NTT splits into *Incorporated Threats* (exploiting originally built-in vulnerabilities) and *Insertion Threats* (intentionally implementing malicious artefacts into the software).

The number of new vulnerabilities per year has now risen to 42,595, according to the European Union Agency for Cybersecurity (ENISA) Threat Landscape 2025. That's almost double the number in 2021 and a 27% increase from the previous year.

Dragos's latest ICS/OT Cybersecurity year review highlights ICS-specific malware (PIPEDREAM) developed by a new threat group (CHERNOVITE), which they view as a supply chain risk as the methods target key vendor systems. They also identified the manufacturing sector as the most targeted sector, at 72% of all ransomware-related incidents.

The European Union Agency for Cybersecurity (ENISA) published its view on the top 10 cybersecurity threats likely to emerge by 2030 [Fig 4]. It shows the supply chain compromise of software dependencies at #1, with cross-border Information and Communication Technology (ICT) service providers as a single point of failure at #9[3].

[3] ENISA updated their report in 2024. Supply chain compromise of software dependencies retained their position at number 1, while cross border ICS service providers as a single point of failure moved up from 9 to 6.

Figure 4: [ENISA Cybersecurity Threats for 2030]

Key Guidance

Identifying High-Risk Suppliers

Not all suppliers will present you with the same levels of risk. Your cyber security team will need to appreciate the suppliers with the highest risk levels to enable them to afford the correct levels of response and prioritisation. The business stakeholders should provide this information in conjunction with the risk management team and make it available to authorised and authenticated stakeholders, centrally hosted, and keep it current. Things for you to consider when determining the cyber/business risks include the following:

1. Safety of product, or threat to life to customers/consumers/employees, or threat to the environment
2. Network, System, or Data access the third party may have.
3. Critical service provision and the impact of the loss of that service
4. Manufacture of a critical component and the impact on production or onward customer delivery
5. Hosting of business data:
    a. Compromise of intellectual property
    b. Compromise of Personal Identifiable Information
    c. Compromise of operational data (configuration settings of OT equipment)

When assessing your supply chain, you must consider how far down the supply chain you go. Critical vulnerabilities and/or compromises further down your supply chain ultimately make your organisation vulnerable. For instance, the SolarWinds compromise affected their Orion network management system. Managed Service Providers (MSPs) use such products to manage client networks. Therefore, you may need to appreciate the implications of such incidents on your suppliers and proactively seek assurances. The OT environment may be particularly vulnerable if legacy systems are end-of-life (EOL) and not supported by the vendor or if it is not part of the vulnerability management process (patching policy)

Contractual Considerations and Obligations[4]

Once you have identified the critical parts of your supply chain, you can then become a more informed buyer. This may include adding SCRM requirements into your contracts; where suppliers do not already have a mature incident response and reporting process that aligns with your business requirements, it will be incumbent upon you to contractually oblige them to satisfy your needs. Aspects to consider include:

1. Identify critical suppliers based on their risk profile to your organisation.
2. Define appropriate requirements for each contract, and do not simply list off standards. Also, ensure that any controls flow down their supply chain, if appropriate. That said… (see 3)
3. Contract minimum security requirements that are justified, proportionate, and repeatable. This may include adhering to specific certifications (Cyber Essentials/+, ISO 27000 series, NIST 800 series, NIS2 Directive, CAF 4.0, CMMC 2.0). If this cannot be currently fulfilled, a contracted remediation plan is defined and agreed upon, or the use of cyber assurance questionnaires that include open questions requiring a detailed reply beyond a simple “Yes/No” response.
4. Do they have governance provisions for cybersecurity incident management? Is resilience built into their infrastructure? What is their Business Continuity Plan (BCP)?
5. A process for reporting cyber or information security incidents that may directly or indirectly impact your business. Unilateral external reporting by either party may harm the other if an agreed process isn’t in place.
6. A standardised incident reporting template addressed to the appropriate department would allow for sufficient incident detail and reporting timeliness.
7. A process for the timely reporting of vulnerabilities within products and services, together with timely patching or mitigation that may be contracted to specific service level agreements (SLAs).
8. Where appropriate, they have a Software Bill of Materials (SBOM) and can provide current and complete access for understanding associated vulnerabilities within the software product.

[4] The supplier of services or products does not include Cloud Services, which is outside the scope of this guidance but should be considered in parallel. There is plenty of guidance relating to this area of the supply chain readily available. The Cloud Security Alliance (CSA)is a good resource that includes the Cloud Controls Matrix (CCM) and the Security, Trust, Assurance, and Risk (STAR) Registry. NCSC’s Cloud Security Guidance Principle 8 relates to Supply Chain Security, whilst CISA has release the Cloud Security Technical Reference Architecture Version 2.

9. A right to audit or to make results of 3rd-party audits available.
10. MSPs are required to report within defined SLAs against an agreed set of security metrics.

Sharing is Caring

Cybersecurity Awareness done right can help build a cyber culture that will help deliver a strong and secure posture within your organisation. Key business stakeholders and departments such as procurement and legal need to be embedded in that culture so that cybersecurity is seen as a business enabler and not a blocker.

Your supply chain will likely comprise businesses of varying sizes and cybersecurity capabilities. Ensuring your less mature suppliers maintain a base level of understanding of the risk associated with providing products and/or services to you will strengthen your security posture and theirs. Therefore, you may wish to consider the following:

1. Providing a central repository for sharing best practices and guidance. This may be content created by your organisation or signposting out to trusted 3rd parties. Ensure that various teams regularly review all material to ensure its relevance and that it remains current.
2. Similarly, make available cyber threat intelligence (CTI). Your organisation may have a contracted service with a professional CTI provider, so the information you can share with your supply chain will likely be restricted to Open-Source Intelligence (OSINT) and sent without prejudice and in good faith. This information may include tactics, techniques, and processes (TTP) of threat actors operating globally or in your sector and might contain indicators of compromise (IOCs). This information can be used by your 3rd parties to implement mitigation measures or scan their environment for potential compromises or weaknesses.
3. Consider inviting suppliers to join appropriate Information Sharing & Analysis Centres (ISACs). These are international communities of members within specific critical infrastructures, such as finance, oil & gas, and aviation.
4. Encourage suppliers to sign up for the NCSC Active Cyber Defence program[5]. This is free at the point of use and was established to "*protect the majority of people in the UK from the majority of the harm caused by the majority of the cyber-attacks the majority of the time*." Services include the Early Warning threat-notification service, Exercise in a Box, and the Cyber Action Toolkit, specifically for small businesses
5. You may contract or offer the opportunity for your suppliers to share in joint cyber-related exercises.
    a. This is likely to be desktop-based and will look to develop a mutual appreciation of the people, process, and technology capability. This can also help build relationships with key suppliers, potentially satisfying commercial or regulatory requirements.
    b. Technology suppliers can help develop the exercise to validate key capabilities to enhance technical skills or awareness of current capabilities.

[5] CISA offers a similar Cyber Hygiene Service at no cost that is limited to federal, state, local, tribal, and Territorial governments, as well as public/private sector critical infrastructure organisations.

c. The type of exercise will vary depending on the significance of the supplier to the business and their level of access to the networks, the sensitivity of data held, or the criticality of the product or service they deliver.
d. Exercises should include key business stakeholders from within your organisation. This may be particularly important if it involves the ICS/OT environment, as the cyber team may not have a broader appreciation of the exercise area.

Incident Response

For incidents within the supply chain that potentially affect your organisation, your operational security team must have business-supplied information to understand the business impact from the outset to enable them to prioritise their incident response and management. The types of business impact to consider are outlined above under the Risk and Threat area.

You should always be aware that the compromised party may have multiple customers and be dealing with a possible major incident. Therefore, pragmatism encourages them to focus on their priorities and appreciate that reporting may be generic initially before it can become more targeted. However, If the incident impacts safety or service delivery, the requirements for updates may be crucial to manage your response.

If the supplier calls in a 3rd party incident response team, the tactical cybersecurity relationship may transfer to that team, whilst the business impact relationship will remain between the supplier and your organisation.

Communication and incident response plans should be created for internal and external (client) use, aligned with the governance approach to establish an end-to-end coordination and ownership. This would help develop a specific incident response training plan and awareness campaign for those business areas involved in SCRM and incident response.

A mature understanding of vendor deployment across IT/OT services would introduce a degree of agility into the initial response with knowledge of the extent of exploited services to focus resources only towards impacted systems.

Communications

We have already recommended that you consider contracting suppliers to an agreed process for reporting cyber or information security incidents that may directly or indirectly impact your business. As with all significant cybersecurity incidents, the response is a team effort bringing together the security teams and business stakeholders. When the incident is related to the supply chain, the operational security team won't necessarily appreciate the business impact of the incident unless it has been furnished with the details to make an informed decision. Still, the security team should know from the development of a playbook the questions to ask of the supplier and recommend mitigation actions to be considered.

This business impact may evolve as further details are released, but recorded supplier risk assessments will assist with initial impact assessments.

Engagement may occur at various levels in the organisation and supply chain, depending upon the incident's size and criticality. A transparent and inclusive line of communication between all areas becomes essential while distinct roles and responsibilities are established and understood.

The information relating to a third-party compromise is likely very sensitive, and they may have informed you due to contractual obligations but have yet to make the compromise public. Therefore, all such instances **must be treated in the strictest confidence** unless advised otherwise. This may include signing a non-disclosure agreement or using Traffic Light Protocols (TLP)[6] to make confidentiality requirements explicit.

Regulatory/Contractual reporting responsibilities

If the 3rd party compromise can potentially affect your data or the service offered, you need to work with the supplier to agree on any onwards reporting responsibilities. This could be very sensitive to both parties, whilst other customers of the supplier may also be considering what to report, to whom, and when to report it. This will likely be a conversation between the supplier and your business stakeholders, but the security team should be informed appropriately and in line with transparent and inclusive communications objectives.

If your organisation is assured or accredited by your customer(s), this is also an area to consider for onwards reporting. Managing the narrative and timing of its release can be necessary for maintaining customer relations.

UK-based 3rd parties should be encouraged to report a significant cyber security incident to the NCSC.

Playbooks and Questions

A playbook can help create a standardised and repeatable approach to managing a cyber incident within the supply chain. This can evolve as lessons are learnt from any post-incident activity or following any joint exercises. Such activity would seek input from all business stakeholders and, if you are creating supplier-specific playbooks, may even extend to consulting the 3rd party.

Relevant content to include in supplier-specific playbooks may include:

1. The location of details relating to the supplier

[6] TLP is a commonly accepted set of designations created by FIRST to restrict the sharing of sensitive information to intended recipients. It comprises of four TLP labels (TLP:RED, TLP:AMBER, TLP:GREEN, and TLP:CLEAR.

a. Their risk profile. This relates to the list outlined under the Risk and Threat area and is established by the risk management department with business stakeholder engagement.
b. Business stakeholders. To be informed of a cyber incident with this supplier
c. Points of contact of the 3rd party for the security team to engage with.

2. A set of questions that can be used to glean further details. Their use will vary depending on the nature of the compromise and what information has already been received. Suggested questions include:
    a. Is there a potential compromise and/or loss of your organisation/customer data?
        i. What is the nature/sensitivity of the compromised data (if any)?
    b. Do they have trusted connections into your organisation?[7]
        i. What connections do they have?
            1. VPN Access. Is there MFA and/or access via proxy?
            2. Data feed (ingress/egress)?
            3. IT accounts (if so, can you provide a list of users)?
                a. Privileged accounts?
            4. Vendor connections within the OT environment and how updates are transmitted into the environment?
    c. Has the attack affected the service or products they provide?
        i. Do they have an estimated timeline for the service return?
    d. Is the attacker still active within the network?
    e. Do they have a detailed timeline of the attack?
    f. What type of systems were affected?
    g. What actions have been taken with compromised assets (accounts/software/etc.)?
    h. Can they provide details of any indicators of compromise, including any malware, command & control infrastructure, the attacker's techniques, and attribution?
    Note that the TTP/IoCs used by a threat actor to compromise the 3rd party may be different from any they use to pivot over to your environment if this is their intention.
    i. What are the current remediation/recovery plans and expected timeline?

Critical Vulnerabilities

Some vulnerabilities might be deemed significant enough to require action outside the "business as usual" patching or mitigation process. This could require you to create an incident to manage the patching or mitigation through to resolution.

CISA provides a searchable and complementary resource for ICS-related vulnerabilities through its ICS Advisory service, which complements their other advisory services and the Known Exploit Vulnerability (KEV) catalogue. The types of advisories provided are:

[7] Ideally, this information would be available to the security team prior to any future incident, but there is value in asking the question to ensure that both parties have the same view. Also, not all organisation will have this level of detail about their full supply chain, whilst things 'evolve' over the duration of a contract and this is an opportunity to capture any such changes.

1. Alert
2. Analysis Report
3. Cybersecurity Advisory
4. ICS Advisory
5. ICS Medical Advisory

Public and private sector contributors have developed the OASIS Common Security Advisory Framework (CSAF) Version 2.0. It includes Vulnerability Exploitability eXchange (VEX), which has been developed as a security advisory to support the release of vulnerabilities related to SBOM data. It delivers machine-readable content to allow both suppliers and users to understand the risk and mitigate accordingly.

ENISA manages the EU Vulnerability Database (EUVD), while VulnCheck is a free commercial resource that is also increasingly adopted as part of organisations' blended vulnerability management solutions.

Supply Chain Resilience

Your organisation should have a Business Continuity Plan (BCP) in the event of a significant incident within the supply chain. This may include ensuring that there are sufficient spares/replacement equipment that are maintained and ready to replace components that have been compromised or are not available. This is informed by the risk assessment of both the supplier and the part of the business they support.

This risk assessment may also determine whether the service or component can be acquired from another 3rd party or if multiple sources already provide it to safeguard against a single point of failure.

Lessons Learned

All significant incidents should include lessons learned as part of the post-incident activity. This opportunity to reflect and critically assess the incident's people, process and technology elements can help drive improvements while validating areas that worked well. Such activity would seek input from all business stakeholders and may even extend to the affected 3rd party.

Output from this stage can help drive continuous service improvement of both incident management and the onboarding/contracting of suppliers and other 3rd parties. It can also influence future desktop exercises. It allows time to reflect on the engagement between the 3rd party, the security team, and the business stakeholders to understand any conflicting priorities and how mature the incident management process is within and between the different corners of this triangle.

Summary

The drive to acknowledge and secure the supply chain is fast-paced as the threat has become more apparent, and governments look to bring in regulatory and contractual requirements to shore up their C-SCRM plans. Advice and guidance from government entities, academia, industry, and vendor specialists are becoming a regular occurrence.

NCSC has released e-learning packages for supply chain mapping that are freely available, whilst CISA has an extensive resource library that will allow agencies and other stakeholders to explore practical C-SCRM information assets like pull-down templates, checklists, guides, and other tools.

The size of your organisation and the industry sector that you are in may determine where you seek such advice, although you are unlikely to find a single source document that will cover all areas identified within the ROSE taxonomy.

Incident response and management within the supply chain is a shared responsibility. By embedding collaborative planning, information sharing, and post-incident learning, CNI operators and their suppliers can significantly enhance their resilience.

CAF Indicators of Good Practice Summary

This article discusses measures that contribute to the following CAF Indicators of Good Practice (IGP):

- A2.a. Risk Management Process: Your organisation has effective internal processes for managing risks to the security and resilience of network and information systems related to the operation of your essential function(s) and communicating associated activities.
- A4.a Supply Chain: You understand and effectively manage the risks associated with suppliers to the security of network and information systems supporting the operation of your essential function(s).
- A4b Secure Software Development and Support: You actively maximise the use of secure and supported software, whether developed internally or sourced externally, within network and information systems supporting the operation of your essential function(s).
- B1.a Policy, Process, and Procedure Development: You have developed and continue to improve a set of cyber security and resilience policies, processes and procedures that manage and mitigate the risk of adverse impact to network and information systems supporting your essential function(s).
- B3.a Understanding Data: You have a good understanding of data important to the operation of network and information systems supporting your essential function(s), where it is stored, where it travels and how unavailability or unauthorised access, uncontrolled release, modification or deletion would adversely impact the essential function(s). This also applies to third parties storing or accessing data important to the operation of your essential function(s).

- B4.d Vulnerability Management: You manage known vulnerabilities in network and information systems to prevent adverse impact on your essential function(s).
- C1.d Triage of Security Alerts: You contextualise alerts with knowledge of the threat and your systems, to identify security incidents as well as responding to all alerts appropriately.
- D1.a Response Plan: You have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of network and information systems supporting the operation of your essential function(s) and covers a range of incident scenarios
- D1.c Testing and Exercising: 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.
- D2.a Post Incident Analysis: When an incident occurs, your organisation takes steps to understand its causes, informing appropriate remediating action.
- D2.b Using Incidents to Drive Improvements: Your organisation uses lessons learned from incidents to improve your security measures.

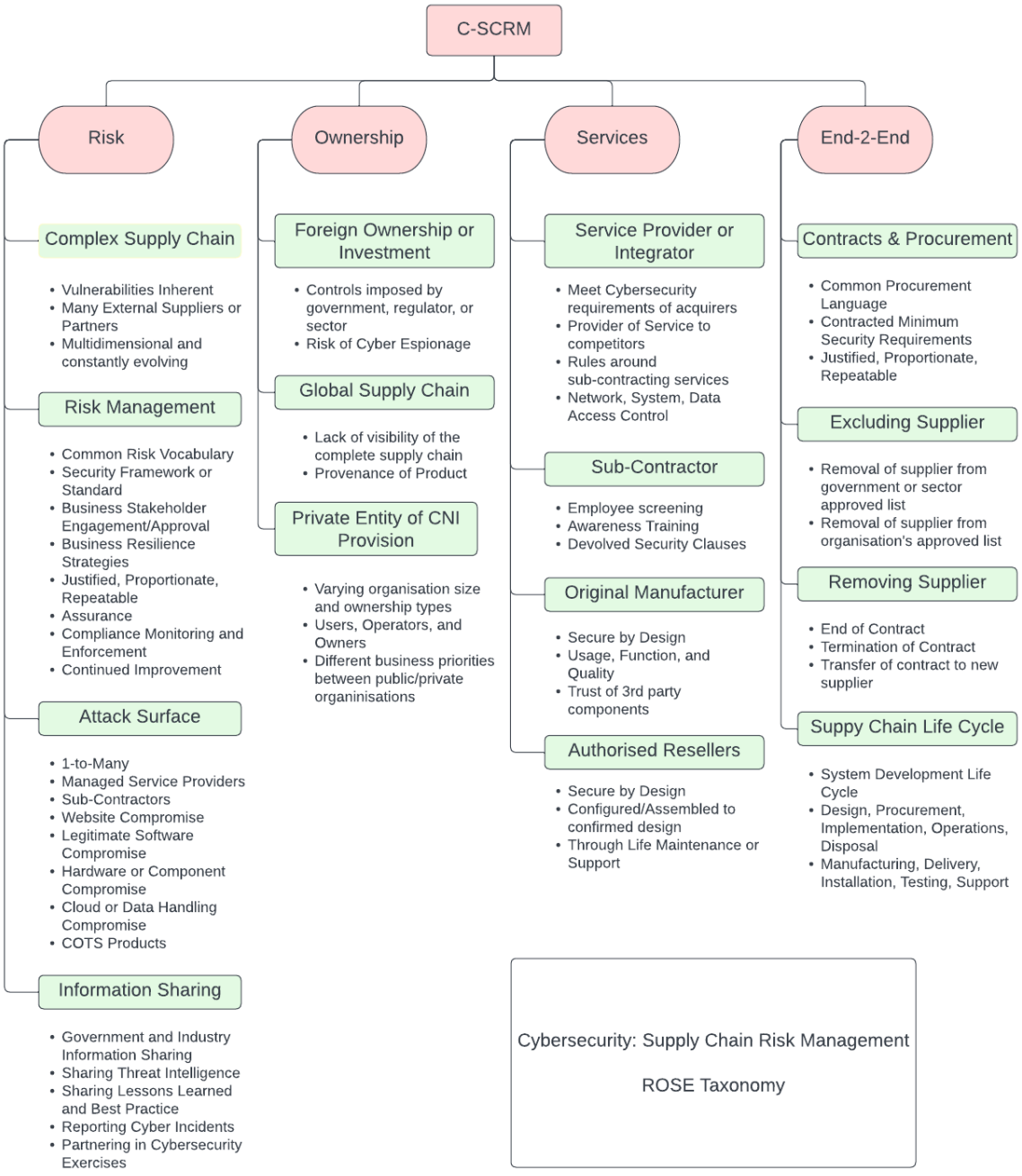
Statement of Support

This guidance has been produced with support from 26 individuals employed in a variety of roles from various organisations in a range of sectors and members of the Industrial Control System Community of Interest (ICS-COI) Supply Chain Expert Group (SCEG) for publication via the Research Institute for Trustworthy Inter-connected Cyber-Physical Systems (RITICS). This guidance is not intended to replace formal NCSC guidance where already available, and care has been taken to reference such existing guidance where applicable. The lead author is Colin Topping, with final review from Tania Wallis and Paul Dorey (SCEG).

Document Details

This document is version 2.0 and was published on 01/11/2025. It will be reviewed every 18 months.

Annex A: ROSE Taxonomy



ROSE Taxonomy [Adapted from [Beware Suppliers Bearing Gifts]]

Annex B – References and Further Reading

1. **NCSC Cyber Assessment Framework (CAF) 4.0**
   https://www.ncsc.gov.uk/collection/caf
2. **MITRE ATT&CK Matrix for Enterprise**
   https://attack.mitre.org/matrices/enterprise/
3. **MITRE ATT&CK Matrix for ICS/OT**
   https://attack.mitre.org/matrices/ics/
4. **MITRE Supply Chain Security System of Trust (SoT) Framework**
   https://sot.mitre.org/
5. **MITRE Risk Model Manager (RMM)**
   https://riskmodelmanager.mitre.org/
6. **NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations**
   https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
7. **NIST SP 800-61 Rev. 3: Computer Security Incident Handling Guide**
   https://csrc.nist.gov/publications/detail/sp/800-61/rev-3/final
8. **ISO/IEC 27035:2023 – Information Security Incident Management**
   https://www.iso.org/standard/80303.html
9. **NIST Cybersecurity Framework (CSF) 2.0**
   https://www.nist.gov/cyberframework
10. **NIS2 Directive**
    https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
11. **CISA Known Exploited Vulnerabilities (KEV) Catalog**
    https://www.cisa.gov/known-exploited-vulnerabilities-catalog
12. **CISA ICS Advisories**
    https://www.cisa.gov/ics/advisories
13. **OASIS Common Security Advisory Framework (CSAF) Version 2.0**
    https://docs.oasis-open.org/csaf/csaf/v2.0/csaf-v2.0.html
14. **Vulnerability Exploitability eXchange (VEX)**
    https://www.cisa.gov/resources-tools/resources/vulnerability-exploitability-exchange-vex
15. **ENISA Threat Landscape 2025**
    https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape
16. **ENISA Top 10 Cybersecurity Threats for 2030**
    https://www.enisa.europa.eu/publications/enisa-cybersecurity-threats-2030
17. **NCSC Active Cyber Defence (ACD) Programme**
    https://www.ncsc.gov.uk/section/products-services/active-cyber-defence
18. **NCSC Exercise in a Box**
    https://www.ncsc.gov.uk/information/exercise-in-a-box
19. **NCSC Cyber Action Plan / Cyber Action Toolkit**
    https://www.ncsc.gov.uk/cyberaware/actionplan
20. **NCSC Supply Chain Security Guidance**
    https://www.ncsc.gov.uk/collection/supply-chain-security

21. **Mandiant M-Trends 2022 Report**
https://www.mandiant.com/resources/reports/m-trends-2022
22. **Wired: NotPetya Analysis**
https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
23. **NTT Global Threat Intelligence Report 2022**
https://services.global.ntt/en-us/insights/gtir-2022
24. **CISA ICS Medical Advisories**
https://www.cisa.gov/ics/medical-advisories
25. **ENISA EU Vulnerability Database (EUVD)**
https://euvd.enisa.europa.eu/
26. **VulnCheck**
https://vulncheck.com/
27. **CISA Supply Chain Risk Management Resources**
https://www.cisa.gov/supply-chain-integrity
28. **NCSC Supply Chain Mapping eLearning**
https://www.ncsc.gov.uk/information/supply-chain-mapping-e-learning