Cyber - Supply Chain Risk Management

This Loss Prevention Standard provides guidance on cyber supply chain risk management.

Version: 1.1
Date: 20th March 2026

Cyber - Supply Chain Risk Management

Introduction

Supply chains are the backbone of modern business operations. Organisations of all sizes rely on networks of third-party vendors, suppliers, software providers, managed service providers and contractors to deliver products and services. These relationships, while commercially essential, introduce cyber risks. Attackers who cannot breach an organisation directly can often seek to compromise it through a less secure supplier.

High-profile incidents, including the SolarWinds Orion compromise, the MOVEit Transfer exploitation, and the 3CX supply chain attack, have demonstrated that a single vulnerability in a third-party product or service can cascade across hundreds, or even thousands, of organisations simultaneously. According to Orange Cyberdefense analysis, over 58% of UK Financial services firms experienced a breach attributable to a supply chain compromise, and the consequences of such incidents continue to rise.

This Loss Prevention Standard provides structured, practical guidance to help organisations establish, operate and continually improve a Cyber Supply Chain Risk Management (C-SCRM) programme. The guidance draws upon and is aligned with internationally recognised frameworks including:

- UK National Cyber Security Centre (NCSC) — 12 Principles of Supply Chain Security and associated guidance.
- US Cybersecurity and Infrastructure Security Agency (CISA) — ICT Supply Chain Risk Management framework.
- NIST Special Publication 800-161 Revision 1 — Cybersecurity Supply Chain Risk Management Practices.
- ISO/IEC 27036 — Information Security for Supplier Relationships.
- ISO 28000 — Security and Resilience in Supply Chains.

The Nature of the Risk

The IT supply chain represents a complex, globally interconnected ecosystem. Vulnerabilities may be introduced, intentionally or unintentionally, at any stage of the product lifecycle. The principal threat actors targeting supply chains include:

- **Nation-state Actors**. Seeking long-term intelligence access, competitive advantage, or the ability to pre-position for disruptive attacks, e.g., China, Russia, North Korea, and Iran.
- **Organised Criminal Groups**. Primarily motivated by financial gain through ransomware, data theft, and fraud, increasingly leveraging supply chain access to maximise the scale of attacks.
- **Insider Threats**. Malicious or negligent employees within supplier organisations who may introduce backdoors, leak credentials, or exfiltrate data.

- **Opportunistic Attackers**. Exploiting publicly disclosed vulnerabilities in widely used software components before patches are applied.

Common Attack Vectors

Below are some of the most common and prevalent supply chain attack methods, as identified by the NCSC & CISA:

- Software Tampering: Attackers compromise build pipelines or update mechanisms to insert malicious code into legitimate software distributions, e.g., SolarWinds, XZ Utils.
- Compromised Hardware: Counterfeit or tampered hardware components introduced during manufacturing or distribution, posing a particular risk in global OT/ICS supply chains.
- Third Party Access Exploitation: Attackers leverage legitimate access granted to managed service providers (MSPs) or contractors to pivot into client environments.
- Open-source attacks: Malicious packages published to public repositories, e.g., npm, PyPI, to be inadvertently imported into software builds.
- Credential & Data theft: Suppliers with poor security hygiene acting as an entry point for credential harvesting or data exfiltration

Regulatory and Legal Drivers

Organisations also face a growing regulatory obligation to demonstrate supply chain cyber security from a range of directives and standards:

- NIS2 Directive (EU): Requires essential and important entities to address supply chain security as part of their risk management obligations.
- DORA (EU Financial Sector): Mandates ICT third-party risk management, including contractual provisions and concentration risk assessment.
- UK Cyber Resilience Bill (anticipated): Expected to extend NIS2-equivalent obligations to UK organisations post-Brexit.
- GDPR / UK GDPR: Processor agreements must address technical and organisational security measures, including supply chain controls.

Establishing a C-SCRM Policy

Effective supply chain cyber security begins with a clearly articulated policy that defines the organisation's appetite for supply chain risk, its expectations of suppliers, and the accountability structure for managing those risks. The policy should be reviewed at least annually.

NCSC guidance recommends that C-SCRM policy should address:

- The scope of third-party relationships subject to security oversight.
- The risk-tiering approach applied to different supplier categories.
- Minimum security standards suppliers are expected to meet.
- Consequences of non-compliance or breach of security obligations.
- The process for escalating supply chain security concerns to senior management.

C-SCRM Roles and Responsibilities

Supply chain risk management is a cross-functional responsibility. Some common roles and responsibilities within a C-SCRM programme could consider the following:

Function	Responsibilities
Board / Executive	Set risk appetite and receive regular C-SCRM reporting. Approve policies and ensure adequate resources are allocated.
Risk / Information Security	Own the C-SCRM programme, maintain the supplier risk register. Conduct assessments and report on risk posture.
Procurement / Commercial	Embed security requirements in RFPs and contracts & enforce due diligence at supplier onboarding.
Legal / Compliance	Ensure contractual obligations address cyber security & monitor regulatory developments.
IT / Technology	Manage technical controls for supplier access, maintain software inventories and patch management.
Business Owners	Identify and classify third-party dependencies, accept residual risk within their domains and engage with supplier relationships.
HR / People	Support vetting requirements and address insider risk through training and awareness.

The UK NCSC and CISA both also emphasise that C-SCRM requires visible sponsorship from senior leadership. Boards should receive, **at a minimum**:

- An annual review of the organisation's C-SCRM maturity and risk posture.
- Immediate escalation of significant supply chain security incidents.
- Reporting on the security posture of critical and strategic suppliers.
- Updates on material regulatory changes affecting supply chain obligations.

Identifying and Classifying the Supply Chain

An organisation cannot manage risks it cannot see. The first practical step in any C-SCRM programme is to establish a comprehensive inventory of all suppliers providing products, software, or services. This inventory should capture:

- Supplier name, contact, and location.
- Nature of the product or service provided.
- Business criticality to the organisation.
- Level and type of access to the organisation's data, systems, or networks.
- Whether the supplier is cloud-hosted, on-premises, or hybrid.
- Key sub-contractors or fourth parties where known.

The NCSC acknowledges that supply chains are often large and complex, and mapping them comprehensively can be challenging. A pragmatic approach is to prioritise initially by business impact, focusing on suppliers whose compromise would cause the greatest harm.

Not all suppliers carry equal risk. A tiered classification model allows proportionate application of due diligence and controls.

The following example four-tier model is aligned with NIST SP 800-161r1 and NCSC guidance:

Tier	Classification	Criteria	Due Diligence Level
1	**Critical**	Supplier access to core systems, sensitive data, or critical infrastructure. Single-source dependency.	Full assessment, contractual controls, continuous monitoring, annual on-site or detailed review.
2	**High**	Significant access to systems or data. Disruption would have material business impact. Some alternates available.	Detailed questionnaire assessment, contractual provisions, periodic review (annual or biennial).
3	**Medium**	Limited access to non-sensitive data or systems. Disruption manageable. Alternatives available.	Streamlined questionnaire, standard contract terms, periodic review (biennial).
4	**Low**	No direct access to systems or sensitive data. Commodity supplier. Readily replaceable.	Basic security confirmation, standard terms, review on contract renewal.

Assessing the Supply Chain

The depth and frequency of supplier security assessments should be proportionate to the risk tier assigned. Assessments serve to validate that a supplier's security posture is consistent with the risk they represent to the organisation and that contractual security obligations are being met.

NCSC guidance on supply chain security identifies several assessment mechanisms that can be used in combination:

- Security questionnaires: Structured questionnaires aligned to recognised frameworks (Cyber Essentials, ISO 27001, NIST CSF). These provide a cost-effective baseline but rely on self-attestation.
- Certification validation: Verification of third-party certifications (ISO 27001, Cyber Essentials/Plus, SOC 2 Type II, PCI DSS etc). Certifications provide independent validation but have defined scope limitations.
- Penetration testing and security audits: Particularly valuable for Tier 1 (Critical) suppliers. May be conducted by the organisation or a trusted third party.
- Continuous monitoring: Automated monitoring of supplier cyber posture using attack surface/open-source intelligence tools and threat intelligence feeds.
- On-site review: For the highest-risk suppliers, direct inspection of security controls, processes, and evidence.

The NCSC also states that organisations should **set minimum security requirements** for suppliers which are “justified, proportionate and achievable”. This can be through “passing” questionnaires provided, or by validation of a certification achieved (e.g., requiring key suppliers to hold a valid Cyber Essentials certificate).

Procurement and Contractual Controls

Security requirements should be embedded at the earliest stage of the procurement process, not bolted on after contract award. The NCSC recommends that supply chain security requirements are included in Requests for Proposal, Invitations to Tender, and pre-qualification questionnaires. This establishes security as a core selection criterion, not just an afterthought.

Additionally, when drawing up contracts with critical suppliers, considerations should be made to include the following security provisions as a minimum:

- Compliance with applicable security standards and frameworks (e.g., ISO 27001, Cyber Essentials, NIST CSF).
- Obligation to notify the organisation of security incidents within defined timeframes (typically less than 72 hours) in line with regulatory obligations.
- The right to conduct security audits or assessments of the supplier, either directly or through a designated third party.
- Data protection and processing requirements consistent with applicable law (UK GDPR, EU GDPR).
- Obligation for the supplier to apply equivalent or greater security standards to their own sub-contractors.
- Requirement for regular independent security testing of systems and services provided.
- Obligations for the secure return or destruction of the organisation's data upon contract termination.
- Minimum service continuity standards and testing requirements.
- Vetting requirements for supplier staff with access to the organisation's systems or data.

Contracts should also be reviewed periodically, to ensure that clauses are updated to reflect evolving threats and regulatory requirements.

Third Party Access Management and Incident Response

Third-party access to systems, data, and networks is one of the most significant vectors for supply chain compromise. The principle of least privilege requires that suppliers are granted only the access strictly necessary to perform their contracted function — no more.

Effective management of third-party access should include:

- Formal access request and approval process for all supplier access requests.
- Time-limited access: Access provisioned for the minimum necessary period and revoked promptly upon expiry or contract termination.
- Multi-factor authentication (MFA): Mandatory for all third-party remote access, particularly to privileged systems.
- Privileged Access Management (PAM): Use of PAM tools to monitor, record, and control privileged supplier access.
- Network segmentation: Third-party access confined to dedicated network segments; no direct access to core systems without explicit justification.
- Regular access reviews: Periodic audit of all active third-party access accounts, with prompt revocation of unnecessary or dormant accounts.

The increase in remote and managed services has expanded the attack surface associated with third-party connections. The NCSC advises that organisations should treat third-party remote access as a significant risk requiring dedicated controls, including:

- Use of organisation-controlled VPNs or Zero Trust Network Access (ZTNA) solutions rather than supplier-controlled remote access tools.
- Session recording and monitoring for privileged remote sessions.
- Just-in-time access provisioning, in which access activated only when required and deactivated immediately upon task completion.

Organisations **should assume that supply chain security incidents will occur** and plan accordingly. A supply chain-specific addendum to the organisation's broader incident response plan should address:

- How the organisation will be notified of a supplier security incident and what information should be requested.
- The criteria for triggering an internal incident response when a supplier reports a breach.
- Procedures for immediate containment of a compromised supplier's access.
- Communication protocols for internal and external stakeholders, including regulators.
- Business continuity measures to maintain operations if a critical supplier is unavailable.

Note: Responding to a suspected Supply Chain Compromise
CISA recommends that organisations immediately isolate and quarantine affected systems upon identification of a supply chain compromise, assume that all credentials and secrets exposed to the compromised supplier are compromised, engage forensic investigation capability, and assess all other suppliers using similar technology for exposure. **Organisations should not wait for the affected supplier to confirm the scope or nature of a breach before initiating their own containment and investigation measures.**

Business Continuity and Supplier Resilience

Dependency on third-party suppliers also introduces business continuity risk. Where a critical supplier experiences a cyber incident that disrupts their services, the procuring organisation must have contingency arrangements in place. These should include:

- Identification and pre-qualification of alternative suppliers for critical services and components.
- Escrow arrangements for critical software: ensuring access to source code or build artefacts in the event of a supplier failure.
- Testing of continuity arrangements: Regular exercises that include scenarios involving loss of a critical supplier's services.
- Minimum recovery time objectives (RTOs) and recovery point objectives (RPOs) for critical supplier-dependent systems.

Monitoring, Review and Continuous Improvement

The cyber risk profile of a supplier can change significantly between formal assessment cycles due to organisational changes, new vulnerabilities, mergers, or incidents. Organisations should implement continuous monitoring mechanisms, particularly for critical suppliers, including:

- Automated attack surface monitoring tools that track the external-facing security posture of suppliers.
- Threat intelligence feeds covering the sectors and technologies used by key suppliers.
- Dark web monitoring for leaked supplier credentials or data.
- Monitoring of vulnerability databases (NVD, CISA KEV) for vulnerabilities in software products used by the organisation.
- Tracking of supplier financial health and organisational stability as leading indicators of emerging risk.

The C-SCRM programme should be subject to formal review annually, as a minimum, and triggered reviews should be in place following material supply chain incidents. Reviews should consider:

- Whether the supplier inventory remains accurate and complete.
- Changes to the organisation's risk appetite or regulatory environment.
- Lessons learned from supply chain security incidents — both internal and those reported by peers or national agencies.
- Emerging threat intelligence and changes to the supply chain threat landscape.
- The effectiveness of existing controls in addressing identified risks.

Organisations are encouraged to periodically assess the maturity of their C-SCRM programme against recognised frameworks. The NIST Cybersecurity Supply Chain Risk Management framework identifies six function areas (Govern, Identify, Protect, Detect, Respond, Recover) across which maturity can be assessed. The Cybersecurity Maturity Model Certification (CMMC) Level 2 requirements also address supply chain obligations for organisations in defence supply chains.

The self-assessment checklist in Appendix A of this Loss Prevention Standard provides a practical starting point for such maturity assessments.

Summary Recommendations

The following priority actions are recommended for organisations seeking to establish their own C-SCRM programme:

No.	Priority	Action	Timeframe
1	**Critical**	Establish a comprehensive inventory of all third-party IT suppliers and classify by risk tier.	Immediate
2	**Critical**	Define and document a C-SCRM policy approved at Board or Executive level.	Immediate
3	**Critical**	Assign clear ownership and accountability for supply chain risk management.	Immediate
4	**High**	Conduct baseline security assessments of all identified Tier 1 and Tier 2 suppliers.	0–3 months
5	**High**	Implement MFA and least-privilege access controls for all third-party remote access.	0–3 months
6	**Medium**	Review and update supplier contracts to include mandatory cyber security provisions.	3-6 months
7	**Medium**	Establish a supply chain incident response procedure and test it via tabletop exercise.	6–9 months
8	**Medium**	Implement continuous monitoring for Tier 1 and Tier 2 suppliers.	9-12 months
9	**Ongoing**	Embed C-SCRM into procurement processes from RFP stage onwards.	Ongoing

Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services at preferential rates via our network of Specialist Partners.

For more information please visit: Aviva Risk Management Solutions – Specialist Partners

Sources and Useful Links

- National Cyber Security Centre: https://www.ncsc.gov.uk/
- Report Fraud: https://www.reportfraud.police.uk/
- National Crime Agency: https://www.nationalcrimeagency.gov.uk/

Note: Whilst UK standards and legislation are referenced in this document, other international standards and legislation should be referenced where applicable.

Additional Information

Relevant Aviva Loss Prevention Standards include:

- **Cyber - Incident Response Process**
- **Cyber - Respond and Recover**
- **Social Engineering - Fundamentals**
- **Cyber Governance for Boards**

To find out more, please visit Aviva Risk Management Solutions **or speak to one of our advisors.**

Email us at riskadvice@aviva.com or call 0345 366 6666.*

*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

Appendix A – C-SCRM Self-Assessment Checklist

This checklist provides a structured framework for organisations to assess the maturity and effectiveness of their Cyber Supply Chain Risk Management programme.

Instructions: For each item, indicate whether the control is fully in place (Yes), not in place (No), or partially implemented or not applicable (Partial / N/A). A score can be derived by calculating the percentage of 'Yes' responses and mapping against the risk rating table below.

Rating	Score Range (Yes)	Guidance
Significantly Below	**0 - 10**	Immediate action required. Fundamental gaps in C-SCRM controls exist. Senior management and board escalation necessary.
Below	**10 - 20**	Significant risk exposure. Remediation plan required within 30 days. Risk acceptances require Director-level sign-off.
Meets	**20 - 35**	Moderate risk. Controls exist but require strengthening. Remediation plan within 90 days.
Exceeds	**35+**	Controls broadly in place. Minor improvements recommended. Review at next scheduled cycle.

Q/s	Assessment Question	Yes	No	Partial or N/A
1	A formal Cyber Supply Chain Risk Management (C-SCRM) policy exists and has been approved at Board or senior executive level.	☐	☐	☐
2	Roles and responsibilities for C-SCRM are clearly defined and assigned across relevant functions (security, procurement, legal, IT, business).	☐	☐	☐
3	The C-SCRM policy is reviewed at least annually and updated to reflect changes in the threat landscape and regulatory environment.	☐	☐	☐
4	The Board or equivalent receives regular reporting on the organisation's supply chain risk posture.	☐	☐	☐
5	Supply chain risk is included within the organisation's enterprise risk register.	☐	☐	☐
6	A defined risk appetite for supply chain cyber risk has been established and communicated.	☐	☐	☐
7	A comprehensive inventory of all third-party ICT suppliers, vendors, and service providers is maintained and kept up to date.	☐	☐	☐
8	All suppliers are classified against a defined risk-tiering model based on access, criticality, and potential business impact.	☐	☐	☐

Q/s	Assessment Question	Yes	No	Partial or N/A
9	The supplier inventory captures the nature of each supplier's access to the organisation's data, systems, and networks.	☐	☐	☐
10	Key sub-contractors (fourth parties) of critical suppliers are identified and assessed where practical.	☐	☐	☐
11	Concentration risks (e.g., multiple critical suppliers sharing the same cloud platform or software components) have been identified and assessed.	☐	☐	☐
12	The supplier inventory is reviewed and updated at least annually and upon material changes to supplier relationships.	☐	☐	☐
13	A formal security assessment is conducted for all new Tier 1 and Tier 2 suppliers prior to onboarding.	☐	☐	☐
14	Assessments cover key security domains including governance, access management, patch management, incident response, data handling, and subcontractor controls.	☐	☐	☐
15	Third-party certifications (ISO 27001, Cyber Essentials Plus, SOC 2 Type II) are verified as part of the assessment process.	☐	☐	☐
16	Security questionnaire responses are validated against independent evidence rather than accepted solely on self-attestation.	☐	☐	☐
17	Periodic reassessments are conducted for existing suppliers at frequencies appropriate to their risk tier (at least annually for Tier 1).	☐	☐	☐
18	Assessment findings are recorded in a supplier risk register and tracked through to remediation.	☐	☐	☐
19	Software Bill of Materials (SBOMs) are requested from critical software vendors and used to support vulnerability management.	☐	☐	☐
20	The organisation has a defined process for conducting or commissioning penetration testing of critical supplier-provided systems.	☐	☐	☐
21	Security requirements are embedded in RFPs, ITTs, and pre-qualification questionnaires from the earliest stage of procurement.	☐	☐	☐
22	All Tier 1 and Tier 2 supplier contracts include mandatory cyber security provisions covering incident notification, audit rights, and data protection.	☐	☐	☐
23	Contracts specify incident notification timeframes consistent with the organisation's regulatory obligations (e.g., within 24–72 hours).	☐	☐	☐
24	Contracts include the right to audit the supplier's security controls, either directly or via a designated third party.	☐	☐	☐
25	Contracts require suppliers to apply equivalent security standards to their own sub-contractors.	☐	☐	☐

Q/s	Assessment Question	Yes	No	Partial or N/A
26	Contractual obligations for secure data disposal upon contract termination are in place.	☐	☐	☐
27	A formal process exists for requesting, approving, and provisioning third-party access to the organisation's systems and data.	☐	☐	☐
28	Multi-factor authentication (MFA) is mandatory for all third-party remote access.	☐	☐	☐
29	The principle of least privilege is applied to all third-party access — suppliers receive only the minimum access necessary for their contracted function.	☐	☐	☐
30	Third-party access is time-limited and reviewed regularly; dormant or unnecessary accounts are promptly deactivated.	☐	☐	☐
31	Privileged third-party access is managed through a Privileged Access Management (PAM) solution with session monitoring and recording.	☐	☐	☐
32	Network segmentation is used to limit third-party access to defined segments; suppliers cannot directly access core systems without specific justification.	☐	☐	☐
33	All third-party access accounts are reviewed at least quarterly, with formal sign-off for continued access.	☐	☐	☐
34	A supply chain-specific incident response plan or addendum is documented and approved.	☐	☐	☐
35	The incident response plan includes procedures for immediate isolation of a compromised supplier's access.	☐	☐	☐
36	Procedures exist for receiving and triaging security incident notifications from suppliers.	☐	☐	☐
37	The supply chain incident response plan has been tested via tabletop exercise or equivalent in the past 12 months.	☐	☐	☐
38	Alternative or backup suppliers have been identified and pre-qualified for critical dependencies.	☐	☐	☐
39	Business continuity plans address scenarios involving the unavailability of critical suppliers.	☐	☐	☐
40	Recovery time and recovery point objectives (RTOs / RPOs) are defined for critical supplier-dependent systems.	☐	☐	☐
41	Continuous or regular monitoring of the cyber posture of Tier 1 and Tier 2 suppliers is in place (e.g., attack surface monitoring, threat intelligence).	☐	☐	☐
42	The organisation subscribes to relevant threat intelligence feeds (e.g., NCSC, CISA, sector ISACs) and monitors for supply chain-specific advisories.	☐	☐	☐
43	The CISA Known Exploited Vulnerabilities (KEV) catalogue and equivalent sources are monitored for vulnerabilities in supplier-provided products.	☐	☐	☐
44	The C-SCRM programme is subject to formal review at least annually.	☐	☐	☐

Q/s	Assessment Question	Yes	No	Partial or N/A
45	Lessons learned from supply chain incidents (internal and industry-wide) are systematically incorporated into programme improvements.	☐	☐	☐
46	The maturity of the C-SCRM programme is periodically assessed against a recognised framework (e.g., NIST CSF, NCSC Cyber Assessment Framework).	☐	☐	☐
47	Senior management and the Board receive regular, meaningful reporting on the C-SCRM programme and key supply chain risks.	☐	☐	☐

20th March 2026

Version 1.1

ARMSGI4012026

Aviva Insurance Limited, Registered in Scotland Number SC002116. Registered Office: Pitheavlis, Perth PH2 0NH.
Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.