

# STANDARDISED SECURE PROCUREMENT PRACTICES AND CYBERSECURE SUPPLY CHAIN GUIDELINES FOR THE LATIN AMERICA AND CARIBBEAN (LAC) REGION

A LAC4 and EU CyberNet Guidelines by Predrag Tasevski & Florian Göhler

*Aligned with NIS2 · EU CRA · ENISA Good Practices for Supply Chain Cybersecurity (2023) · ENISA Threat Landscape for Supply Chain Attacks (2021) · CISA Vendor SCRM Template · ISO/IEC 27036 · NIST SP 800-161 Rev. 1 · DORA RTSs · EU ICT Supply Chain Toolbox ·*



ity, cybersecurity  
technology security  
the protection of  
of and networks  
disclosure,  
go to their  
site, or electronic  
from  
misdirection of the  
guide.[1]

bersecurity  
cy security  
ation of  
networks  
data,  
net  
electronic  
ation of the  
[1]

2 3 1 5 1 2 1 3 2 5 6 1 1 2 1  
2 1 3 2 3 1 5 6 2 1 3 1 2



Computer security, cyber  
or information technology  
(IT security) is the protec  
computer systems and ne  
from information disclosure  
theft of or damage to the  
hardware, software, or el  
data, as well as from  
the disruption or misdireg  
services they provide.[1]



|                                                                               |    |
|-------------------------------------------------------------------------------|----|
| Foreword -----                                                                | 4  |
| 1. Executive Summary-----                                                     | 6  |
| Structure of Recommendations-----                                             | 6  |
| Key Findings from the Regional Baseline -----                                 | 7  |
| Companion Deliverables -----                                                  | 7  |
| 2. Introduction -----                                                         | 8  |
| 2.1 Context and Objectives -----                                              | 8  |
| 2.2 Scope and Audience-----                                                   | 8  |
| 2.3 How to Use This Document-----                                             | 8  |
| 3. Methodology -----                                                          | 9  |
| 4. Country-level Findings and Regional Baseline -----                         | 10 |
| 5. Per-country Findings -----                                                 | 11 |
| 5.1 Bahamas -----                                                             | 11 |
| 5.2 Chile -----                                                               | 11 |
| 5.3 Colombia -----                                                            | 11 |
| 5.4 Dominican Republic -----                                                  | 11 |
| 5.5 Ecuador-----                                                              | 11 |
| 5.6 Guatemala -----                                                           | 12 |
| 5.7 Mexico -----                                                              | 12 |
| 5.8 Panama -----                                                              | 12 |
| 5.9 Uruguay -----                                                             | 12 |
| 6. Common Gaps, Risks and Priority Areas for Improvement-----                 | 13 |
| 6.1 Common Gaps Observed -----                                                | 13 |
| 6.2 Priority Risks-----                                                       | 13 |
| 6.3 Priority Areas for Improvement -----                                      | 14 |
| 7. Comparative Analysis: LAC4 Baseline vs. EU / International Benchmarks----- | 15 |
| 8. ENISA Threat Landscape – Implications for the LAC Region-----              | 17 |
| 9. Implementation Roadmap -----                                               | 18 |
| 9.1 Phase 1 – Foundations (months 1-6) -----                                  | 18 |
| 9.2 Phase 2 – Adoption in New Procurements (months 6-12) -----                | 18 |
| 9.3 Phase 3 – Extension to Legacy Contracts (months 12-24) -----              | 18 |
| 9.4 Phase 4 – Continuous Improvement (year 2+)-----                           | 18 |
| 9.5 Governance and Metrics for Continuous Evaluation -----                    | 19 |
| 9.6 Training Needs -----                                                      | 19 |
| 10. Security Recommendations -----                                            | 20 |
| 10.1 Planning-----                                                            | 20 |
| 10.2 Selection of suppliers and products -----                                | 27 |
| 10.3 Operations-----                                                          | 39 |
| 10.4 Vulnerability Handling -----                                             | 47 |
| 10.5 Incident Handling-----                                                   | 52 |

|                                                                           |    |
|---------------------------------------------------------------------------|----|
| 10.6 Decommissioning / End of Use -----                                   | 56 |
| 11. Definitions -----                                                     | 60 |
| 12. Annex A – Cybersecure Supply Chain Standards -----                    | 61 |
| A.1 Software Bill of Materials (SBOM) -----                               | 61 |
| A.2 Vulnerability Disclosure Policies (VDP) -----                         | 61 |
| A.3 Security Certification and Assurance Levels -----                     | 61 |
| A.4 Secure Development Lifecycle (SDL) and Build-pipeline Integrity ----- | 61 |
| A.5 Vulnerability Handling – Supplier and Entity -----                    | 62 |
| A.6 Hardware Integrity (where hardware is procured) -----                 | 62 |
| A.7 Incident Reporting and Contractual Penalties -----                    | 62 |
| 13. Annex B – How-to: Minimal Supplier Risk Assessment -----              | 63 |
| B.1 Step 1 – Characterise the Procurement -----                           | 63 |
| B.2 Step 2 – Identify the Supplier and the Supply-chain Depth -----       | 63 |
| B.3 Step 3 – Identify the Threat Scenarios (use the ENISA taxonomy) ----- | 63 |
| B.4 Step 4 – Estimate Likelihood and impact -----                         | 63 |
| B.5 Step 5 – Identify and Tier the Controls -----                         | 63 |
| B.6 Step 6 – Decide and Document -----                                    | 63 |
| B.7 Example Threats from the ENISA Threat Landscape -----                 | 64 |
| B.8 Example Mitigations from These Guidelines -----                       | 64 |
| 14. References -----                                                      | 65 |

## Foreword

Digital transformation is reshaping how governments, critical infrastructure operators and public institutions across Latin America and the Caribbean deliver services, manage information and serve their citizens. At the same time, it is making them increasingly dependent on complex digital supply chains: software providers, cloud services, managed service providers, hardware manufacturers, system integrators and subcontractors.

This interdependence creates opportunity, but it also creates shared risk. A vulnerability in a supplier, a compromised software update, inadequate oversight of subcontractors, or unclear contractual security obligations can have consequences that extend far beyond a single organisation. Secure procurement must therefore be understood not simply as an administrative process, but as an essential component of cyber resilience, continuity and public trust.

*These Standardised Secure Procurement Practices and Cybersecurity Guidelines for the Supply Chain* have been developed to help address this challenge. They provide public institutions, regulators, critical infrastructure operators and other organisations with a practical and adaptable framework to integrate cybersecurity throughout the procurement lifecycle, from planning and supplier selection to operations, vulnerability management, incident response and the end of a contractual relationship.

Their relevance for Latin America and the Caribbean is particularly significant. The baseline assessment underpinning this study shows that, while the region has made important progress in national cybersecurity strategies, governance arrangements and response capacities, cybersecurity requirements are not yet consistently embedded in procurement processes. Common gaps remain in areas such as supplier risk assessment, model contractual clauses, software transparency, incident notification, subcontractor oversight, data portability and exit planning.

The Guidelines respond to those gaps with a proportionate, risk-based approach. Their recommendations are designed to be applied according to the criticality of each procurement process, enabling institutions to establish a meaningful minimum baseline while reserving more rigorous controls for high-impact services, systems and suppliers. This approach supports practical adoption and recognises the different levels of maturity and institutional capacity across the region.

For LAC4, this tool also represents an important achievement in strengthening cooperation and harmonisation between the European Union and Latin America and the Caribbean. The Guidelines draw upon leading European frameworks, including NIS2, the Cyber Resilience Act, DORA, the EU Cybersecurity Act and ENISA good practices, while connecting them with internationally recognised standards and tools, including ISO, NIST and CISA references.

This is not an exercise in simply reproducing European rules in another context. Rather, it is an effort to translate proven good practices into a regional reference that can be adapted to national legal frameworks, institutional priorities and operational realities. By creating a common language around secure procurement and supply-chain cybersecurity, these Guidelines can help reduce fragmentation, promote interoperability and enable both public institutions and suppliers to work towards clearer, more consistent and verifiable security expectations.

LAC4 extends its sincere appreciation to Florian Göhler and Predrag Tasevski, technical experts and consultants whose knowledge, rigorous analysis and commitment made this study possible. We also thank the members of the LAC4 community and the institutions that contributed their perspectives, experience and continued engagement throughout this process. Their collaboration has been essential in ensuring that the Guidelines are grounded in regional needs while aligned with global and European good practices.

We hope that this publication will serve as more than a reference document. It should be a practical starting point for national authorities, procurement bodies, cybersecurity teams, legal advisers and decision-makers to strengthen the security of the digital services on which our societies increasingly depend.

Supply-chain cybersecurity is a cross-border challenge. Addressing it requires shared responsibility, sustained cooperation and a commitment to building trust across our digital ecosystem. LAC4 is proud to support this collective effort and looks forward to working with our members and partners throughout the region to turn these Guidelines into lasting improvements in cyber resilience.

***César Moliné Rodríguez***

*Regional Manager*

*Latin America and Caribbean Cyber Competence Centre (LAC4)*

# 1. Executive Summary

Government entities and critical-infrastructure operators across the Latin America and Caribbean (LAC) region rely on increasingly complex digital supply chains: software, hardware, cloud services, managed services and a long tail of sub-processors. The same ecosystem that enables efficiency also enables compromise. The ENISA Threat Landscape for Supply Chain Attacks (2021) recorded a fourfold increase in supply-chain incidents from 2020 to 2021, with 66% of attacks targeting suppliers' code or processes and 62% leveraging the trusted relationship between supplier and customer.

This document delivers standardised, actionable and locally adaptable guidelines that embed cybersecurity into the full procurement lifecycle and strengthen supply chain risk management across public bodies and critical sectors. It also includes the regional baseline assessment that motivated the design choices made in the Guidelines.

Across the nine LAC4 member states for which sufficient public information was available, the dominant pattern is consistent: cybersecurity is rarely embedded in procurement processes, and supply-chain risk is not addressed in a structured way. Two countries – Bahamas and Uruguay – have partial coverage limited to specific scopes (critical infrastructure or supplier access to information). The other countries either reference supply chain implicitly through general risk-management language, or do not address it at all.

The Guidelines are aligned with the EU NIS2 Directive, the EU Cyber Resilience Act, the ENISA Good Practices for Supply Chain Cybersecurity (June 2023), the ENISA Threat Landscape for Supply Chain Attacks (July 2021), the EU ICT Supply Chain Toolbox, the EU cybersecurity certification schemes EUCC and EUCS, and the DORA technical standards. They incorporate the question categories of the CISA / ICT SCRM Task Force Vendor SCRM Template and reference international standards ISO/IEC 27036, ISO/IEC 27001:2022 and NIST SP 800-161 Rev. 1.

## Structure of Recommendations

Chapter 10 – Security recommendations contain the 63 standardised recommendations across six sections, mirroring the procurement lifecycle:

- 10.1 – Planning (10 recommendations): governance, scope, restrictions, roles, stakeholder participation, integration plan, risk assessment, policy, register.
- 10.2 – Selection of suppliers and products (18): jurisdiction, audit, location, ISMS, SDL, build integrity, SBOM, vulnerabilities, updates, VDP, portability, certifications, supplier risk, personnel security, sub-processors, change of control, tender requirements, OEM / anti-counterfeit.

- 10.3 – Operations (12): annual re-evaluation, threat sharing, training, hardening, backups, RACI, contracts, identity & access, segmentation, patching, code of conduct.
- 10.4 – Vulnerability handling (8): PSIRT, vulnerability and weakness analysis, root-cause analysis, CVSS-based maintenance policy, customer notification, entity-side vulnerability management with SBOM monitoring, patch test & rollback, coordinated vulnerability disclosure.
- 10.5 – Incident handling (8): communication channels, RTO, BCP, restore tests, joint playbooks, contractual notification, penalties, post-incident review.
- 10.6 – Decommissioning / End of use (7): plan, stakeholders, data export, deletion, deactivation, NDA continuity, hardware sanitisation.

### Key Findings from the Regional Baseline

- Most surveyed LAC4 member states do not have a standardised secure procurement framework specifically addressing cybersecurity.
- Where supply-chain provisions exist (Bahamas, Uruguay), they are partial – limited to critical infrastructure or to specific aspects (supplier access to information).
- There is broad alignment with international standards in the abstract, but limited operational guidance, model clauses or vendor risk-evaluation tools at the national level.
- All studied countries would benefit from standardised model clauses, a vendor questionnaire, an SBOM requirement, build-pipeline integrity, a dedicated vulnerability-handling regime, and an exit-plan obligation.

### Companion Deliverables

- Model Clauses & Mapping (Excel) – 63-question vendor questionnaire, multi-framework crosswalk and ready-to-paste contract clauses.
- Dissemination Deck – slides for national adoption and stakeholder workshops.

## 2. Introduction

### 2.1 Context and Objectives

The LAC region has accelerated its digital transformation in the last decade. Public services, financial services, healthcare and energy operators all depend on long, opaque digital supply chains. Recent regional reports – including the IDB / OAS 2025 Cybersecurity Report – consistently identify supply-chain security and procurement security as low in maturity across the region.

EU CyberNet, through Call for Action CFA-215, requested the development of comprehensive guidelines on secure procurement and cyber-resilient supply-chain management to support the LAC4 community of practice. This document is the principal deliverable answering that request.

### 2.2 Scope and Audience

These guidelines are addressed to entities – public bodies, regulators, critical-infrastructure operators and any organisation that procures digital services and products. They focus primarily on essential and important entities in the sense of the EU NIS2 Directive but are written to be adaptable to organisations of any size.

They cover digital supply chains in the broad sense: software, hardware, cloud services, managed services and any third party that processes information of the entity or operates a system on its behalf – manufacturers, distributors, system integrators, MSPs, MSSPs and digital-service providers, in the typology used by ENISA's 2023 Good Practices.

### 2.3 How to Use This Document

Chapter 10 is a checklist of 63 recommendations. Each recommendation is phrased as a question that the entity should be able to answer. Below the question, a Criticality line indicates the procurement-criticality tier at which the recommendation becomes mandatory:

- Low – mandatory at every tier (Low, Medium and High criticality procurements).
- Medium – mandatory at Medium and High criticality procurements.
- High – mandatory only at High criticality procurements (the most demanding controls).

Each recommendation includes a Rationale, practical Examples and further information, and a Mapping to relevant standards and frameworks. Where appropriate, an illustrative case from the ENISA Threat Landscape is provided.

Entities can use the companion Mapping Excel (deliverable 4 of the Call for Action) as a vendor questionnaire – including the same tier filter that flags which questions are mandatory at Low, Medium or High criticality – and a multi-framework crosswalk.

### 3. Methodology

The methodology behind this consolidated draft followed five steps, merging the work that produced the Guidelines and the work that produced the Baseline Assessment Report.

- (i) Desk review of the national cybersecurity strategies, framework laws and procurement policies of the LAC4 member states for which public information was available, plus the regional studies (notably the IDB / OAS 2025 Cybersecurity Report on Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean).
- (ii) Comparative analysis against EU standards (NIS2, CRA, EU Cybersecurity Act, ENISA Good Practices for Supply Chain Cybersecurity (June 2023), ENISA Threat Landscape for Supply Chain Attacks (July 2021), ENISA Technical Implementation Guidance for Reg. (EU) 2024/2690, DORA RTSs 1773, 1774 and 532) and complementary international references (ISO/IEC 27036, ISO/IEC 27001:2022, NIST SP 800-161 Rev. 1, NIST SSDF, CISA Vendor SCRM Template).
- (iii) Content analysis to extract recurring control families and the five focus areas of the ENISA Good Practices (Strategic corporate approach, Supply chain risk management, Supplier relationship management, Vulnerability handling, Quality of products and practices).
- (iv) Mapping of the eight question categories of the CISA SCRM Template – Qualifying, SCM & Governance, Secure Design, Information Security, Physical, Personnel, Supply-Chain Integrity, Resilience – to the chapter structure of the Guidelines, to ensure that no SCRM Template category is left uncovered.
- (v) Consolidation into a question-based, mapping-anchored guideline format, with a per-question criticality tier (Low / Medium / High) used by the companion Mapping Excel as a vendor questionnaire.

Coverage limitations: this assessment relies on publicly available information. Three LAC4 countries – Antigua & Barbuda, El Salvador and Costa Rica – could not be analysed within the project timeframe and are flagged as wave-2 of the validation phase.

## 4. Country-level Findings and Regional Baseline

The recommendations in this document are calibrated to the current maturity of the LAC4 member states. This section summarises the baseline assessment carried out across nine of the twelve LAC4 member states.

| Country                   | Region    | Coverage                       | Findings                                                                                                                                                                                                                                                          |
|---------------------------|-----------|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Bahamas</b>            | Caribbean | Partial – CI only              | Objective 8 of national strategy addresses supply chain / third-party relationships, scoped to government and CI. No standardised procurement framework or general-purpose supply-chain guidelines.                                                               |
| <b>Chile</b>              | Southern  | Not defined                    | National Cybersecurity Policy 2023-2028 and Cybersecurity Framework Law (ANCI) do not explicitly cover secure procurement. Per NCSI, no standardised national framework formally established.                                                                     |
| <b>Colombia</b>           | Andean    | Not addressed                  | National strategy and recent digital agenda do not address cybersecurity in procurement, acquisitions or supply chain.                                                                                                                                            |
| <b>Dominican Republic</b> | Caribbean | Indirect / partial             | Strategy improves regulatory framework and ICT governance, which can implicitly drive minimum security standards. No detailed standardised framework (no SBOM, certification or supplier vetting). Supply chain limited to CI references.                         |
| <b>Ecuador</b>            | Andean    | Not addressed                  | Procurement security not a distinct component of strategy. Supply chain implicit through risk-management language but not formalised.                                                                                                                             |
| <b>Guatemala</b>          | Central   | Not addressed                  | National strategy makes no operational provision. No evidence of cybersecurity-related standards used in procurement processes.                                                                                                                                   |
| <b>Mexico</b>             | Central   | Not addressed                  | National Cybersecurity Strategy does not mention supply chain or procurement. Cybersecurity regulation is splintered across sectors and largely focused on data protection.                                                                                       |
| <b>Panama</b>             | Central   | Not addressed (treaty)         | No relevant national supply-chain regime documented (NCSI). Bilateral arrangement with U.S. SOUTHCOM covers supply-chain aspects but public information is limited.                                                                                               |
| <b>Uruguay</b>            | Southern  | Most developed (still partial) | AGESIC framework includes a Supplier Relations Policy (concise, focused on supplier access to information) and software-vendor security requirements (mostly technical). Exit plans, SBOM, fourth-party risk and joint incident response remain mostly untouched. |

## 5. Per-country Findings

### 5.1 Bahamas

The National Cybersecurity Strategy contains an Objective 8 that addresses supply chain and third-party relationships, but only in the scope of government and critical infrastructure. The strategy does not include standardised secure procurement practices or comprehensive cybersecurity supply-chain guidelines applicable across sectors. There are consequently no model clauses, no SBOM requirement and no exit-plan obligation. For these Guidelines, Bahamas is in the upper half of the regional baseline by virtue of explicit recognition of the topic, but it lacks operational tools.

### 5.2 Chile

Chile's National Cybersecurity Policy 2023-2028 and the Cybersecurity Framework Law (granting powers to ANCI) define general cybersecurity governance but do not explicitly cover secure procurement. Per NCSI, no standardised national framework on secure procurement is yet formally established. The combination of an emerging regulator (ANCI) and a national policy update creates a window of opportunity to embed these Guidelines in subordinate regulation.

### 5.3 Colombia

Colombia's national cybersecurity strategy and the digital / AI agenda recently issued by MinTIC do not address cybersecurity in procurement, acquisitions or supply chain in a structured way. Public-sector procurement is governed by Law 80/1993 and successors, with cybersecurity addressed only indirectly through general data-protection requirements. The lack of a structured supply-chain dimension is the principal gap.

### 5.4 Dominican Republic

Coverage is partial and indirect. The strategy strengthens the legal and regulatory framework for cybersecurity and improves governance across government ICT systems, which can implicitly drive minimum security standards in procurement. However, the strategy does not contain a detailed standardised secure procurement framework comparable to the EU model – there is no requirement for SBOMs, supplier certification or formal vetting. Supply chain guidelines are limited to references in critical-infrastructure protection and incident response, rather than to general procurement processes.

### 5.5 Ecuador

Procurement security is not a distinct component of the national cybersecurity strategy. Supply chain issues are implicit through general risk-management language but not formalised. There are no published national vendor questionnaire and no national catalogue of model security clauses. The opportunity here is to anchor the Guidelines into the national procurement law via a circular issued by the central procurement authority.

## 5.6 Guatemala

There is no evidence of the use of cybersecurity-related standards in guiding procurement processes. The national strategy makes no operational provision for secure procurement or supply chain cybersecurity. The Guidelines can be adopted as a foundational document on which to build a national approach.

## 5.7 Mexico

The National Cybersecurity Strategy does not mention supply chain or procurement. Cybersecurity regulation in Mexico is splintered across sectors (financial regulator CNBV, telecommunications regulator IFT, INAI for data protection) and largely focused on data protection rather than on cybersecurity, with no uniform regime. A cross-sectoral, tier-based application of the Guidelines is the most realistic path.

## 5.8 Panama

No relevant national supply-chain security regime is documented in NCSI. A bilateral cooperation arrangement with the United States Southern Command covers supply-chain aspects, but public information is limited. The CSIRT under the Government Innovation Authority (AIG) is the most likely operational counterpart for adoption of these Guidelines.

## 5.9 Uruguay

Uruguay has the most developed national framework in the surveyed group. The national cybersecurity framework managed by AGESIC features a Supplier Relations Policy (concise – about a single page of content – focused mainly on supplier access to information rather than on the security of procured services or products) and a set of security requirements for software vendors / providers (mostly technical, with a few organisational requirements). Other supply-chain topics – exit plans, SBOM, fourth-party risk and joint incident response – remain mostly untouched. Uruguay is therefore the natural pilot adopter of the full Guidelines, building on existing instruments.

## 6. Common Gaps, Risks and Priority Areas for Improvement

### 6.1 Common Gaps Observed

- No standardised, sector-agnostic procurement security framework – coverage where it exists is partial (CI only) or single-aspect.
- No model security clauses or tender templates available at the national level for procuring entities to reuse.
- No requirement for a Software Bill of Materials (SBOM) in tenders or contracts.
- Vulnerability disclosure obligations on suppliers are not standardised and rarely embedded in contracts.
- Code-and-build-pipeline integrity expectations on software suppliers are not articulated, despite the well-known SolarWinds and Codecov incidents.
- Supplier risk-evaluation methodologies are not harmonised; entities re-invent questionnaires per tender, with significant variance in coverage.
- Exit and decommissioning obligations are largely absent, exposing entities to vendor lock-in and continuity risk.
- Fourth-party risk (sub-processors, supply chain of the supplier) is rarely addressed in any country's framework.
- Incident notification timelines and contractual penalties are not standardised across procurement contracts.
- Personnel security obligations on supplier staff are not consistently enforced via contractual clauses.
- Vulnerability handling – supplier-side (PSIRT, formal vulnerability and weakness analysis, root-cause feedback into the SDL) and entity-side (internal VM programme, SBOM monitoring, patch test & rollback, CVD participation) – is treated as a single line item, when ENISA Good Practices identifies it as a distinct focus area.

### 6.2 Priority Risks

From the gaps above, the most material risks for entities in the region are:

- Supply-chain attacks via compromised software updates or compromised open-source dependencies (mitigated by SBOM, SDL, build-pipeline integrity, VDP, PSIRT).
- Lock-in and continuity risk – inability to migrate critical workloads, especially when suppliers operate from outside the region (mitigated by data portability, exit plans).
- Unmanaged sub-processor risk – entity cannot enumerate or control its fourth-party exposure (mitigated by sub-processor approval and notification clauses).

- Slow incident notification – entity cannot meet its own NIS2-equivalent obligations because the supplier did not notify in time (mitigated by contractual notification timelines).
- Compromised privileged access by supplier staff (mitigated by personnel screening, named accounts, MFA, JIT elevation, segmentation).
- Hardware integrity (counterfeit / non-OEM components) for procurements in transport, energy and defence sectors (mitigated by OEM-only sourcing and tamper-evident packaging).

### 6.3 Priority Areas for Improvement

- Adopt these Guidelines as a national reference – published by the national cybersecurity authority – for the public sector and critical sectors.
- Issue standardised model clauses (security, audit, incident notification, data portability, sub-processor approval, exit, NDA continuity, build integrity, OEM-only sourcing).
- Mandate the vendor questionnaire from the Mapping Excel as part of pre-qualification for any procurement above a national threshold.
- Require an SBOM, a published Vulnerability Disclosure Policy and a PSIRT-equivalent function from suppliers of software / digital services.
- Adopt a risk-tiered approach: stronger controls for suppliers of critical / essential services, lighter controls for low-risk procurement – the tier badge on each recommendation in this document already implements this.
- Enable regional information sharing on suppliers with repeated cybersecurity issues (LAC4 community of practice).

## 7. Comparative Analysis: LAC4 Baseline vs. EU / International Benchmarks

The following table maps each control area of the Guidelines to the relevant EU / international benchmark, the expected baseline, and the aggregate status across the LAC4 member states. The control-area column is anchored on the five focus areas of the ENISA Good Practices for Supply Chain Cybersecurity (2023) – strategic corporate approach, supply chain risk management, supplier relationship management, vulnerability handling, and quality of products and practices – to facilitate alignment with EU policy.

| Control area / ENISA GP focus                                  | EU / int'l benchmark                                                      | Expected baseline                                                                                                                                                                                                                                  | LAC4 status (aggregate)                                                                                                  |
|----------------------------------------------------------------|---------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Strategic corporate approach (ENISA GP 3.1)</b>             | NIS2 Art. 21(2)(d), ISO 27036-2 cl. 6, CISA SCRM Q. 2.3                   | Set policy, scope, banned-vendor list, named role, RACI                                                                                                                                                                                            | Largely absent; Uruguay partial. ENISA 2023 study: 76% of EU organisations also lack dedicated supply-chain roles.       |
| <b>Supply chain risk management (ENISA GP 3.2)</b>             | ISO 27005, ENISA TIG 2024/2690                                            | Per-supplier risk record with criticality tier and review cadence                                                                                                                                                                                  | Not standardised in any LAC4 strategy. ENISA 2023 study: only 37% of EU organisations conduct supplier risk assessments. |
| <b>Supplier relationship management – Audit (GP 3.3)</b>       | DORA RTS 1773; ISO 27036-2; CISA SCRM Q. 4.17, 7.9                        | Right to audit; ISO 27001 / SOC 2 / EUCC / EUCS where applicable                                                                                                                                                                                   | Audit clauses appear ad hoc; certification-based assurance not embedded in tenders.                                      |
| <b>Vulnerability handling (GP 3.4) – SBOM</b>                  | EU CRA Annex I Part II; CISA / NTIA SBOM; CISA SCRM Q. 2.5                | Machine-readable SBOM (CycloneDX / SPDX) at delivery and on each major release                                                                                                                                                                     | No country requires it.                                                                                                  |
| <b>Vulnerability handling (GP 3.4) – VDP</b>                   | EU CRA Art. 13-14; ISO 29147 / 30111                                      | Public VDP; advance-notice security update obligations                                                                                                                                                                                             | Not standardised regionally.                                                                                             |
| <b>Vulnerability handling (GP 3.4) – Programme &amp; PSIRT</b> | ENISA GP 3.4; CISA SCRM §3.14-3.17, §4.14-4.23; FIRST.org PSIRT framework | Supplier-side PSIRT, formal vuln/weakness analysis, root-cause feedback, CVSS-based maintenance policy, proactive customer notification – paired with entity-side internal VM programme, SBOM monitoring, patch test & rollback, CVD participation | No LAC4 country mandates a supplier PSIRT or an SBOM-based entity-side VM programme. CVD regimes are mostly absent.      |
| <b>Quality of products (ENISA GP 3.5) – Secure development</b> | NIS2 Art. 21(3); NIST SSDF; CISA SCRM Q. 3.10                             | Documented SDL with peer review, threat modelling, security testing                                                                                                                                                                                | Absent from procurement frameworks.                                                                                      |

| Control area / ENISA GP focus                           | EU / int'l benchmark                          | Expected baseline                                                        | LAC4 status (aggregate)                                            |
|---------------------------------------------------------|-----------------------------------------------|--------------------------------------------------------------------------|--------------------------------------------------------------------|
| Quality of products (GP 3.5) – Build-pipeline integrity | CISA SCRM Q. 3.6, 3.7, 3.13; Google SLSA      | Code signing, reproducible builds, controlled build environments         | Not addressed – even though SolarWinds and Codecov are well known. |
| Sub-processor / 4th party                               | DORA RTS 532; NIS2 Art. 22; CISA SCRM Q. 2.10 | List, prior approval, flow-down clauses, audit rights                    | Not addressed.                                                     |
| Personnel security                                      | ISO 27001 Annex A.6; CISA SCRM Q. 6.1-6.6     | Screening, onboarding, offboarding processes contractually flowed down   | Not standardised via procurement clauses.                          |
| Incident notification (GP 3.3)                          | NIS2 Art. 23; CISA SCRM Q. 4.25               | Contractual timeline aligned with the entity's own NIS2 obligations      | Country regimes vary; not flowed into supplier contracts.          |
| Data portability / exit                                 | EU Data Act; ENISA Cloud RA                   | Non-proprietary export format, validated exit plan                       | Largely absent (Uruguay partial).                                  |
| Continuity & exit testing                               | DORA Art. 28; ISO 22301; CISA SCRM Q. 8.3     | Exit plan tested at least every 24 months; supplier diversity considered | Not standardised.                                                  |

## 8. ENISA Threat Landscape – Implications for the LAC Region

The ENISA Threat Landscape for Supply Chain Attacks (July 2021) catalogued 24 supply-chain incidents reported between January 2020 and early July 2021. The principal findings, and the way they shape these Guidelines, are summarised below.

- 66% of attacks targeted suppliers' code or processes (e.g., SolarWinds Orion, Codecov) – embedded in S-08 (SDL) and S-18 (build-pipeline integrity).
- 62% of customer compromises leveraged the trusted relationship with the supplier (automatic update channels, signed certificates, etc.) – addressed by S-06 (SBOM), S-09 (VDP and security updates), I-05 (joint playbooks), O-10 (segmentation) and the whole Chapter 4 (Vulnerability handling).
- 66% of suppliers either did not know how they were compromised or were not transparent about it – directly motivating O-02 (information sharing), V-05 (customer notification), V-08 (CVD), I-06 (notification) and I-08 (post-incident review).
- More than 50% of incidents were attributed to APT groups – making the case that even mature supplier ecosystems require defensive depth (O-09 named accounts / MFA / JIT, O-10 segmentation, O-06 independent backups).
- ENISA recommends that customers identify and document types of suppliers, define risk criteria, manage suppliers across the lifecycle, and define obligations on protection, sharing, audit, business continuity, personnel screening and incident handling – every one of these recommendations is operationalised in the Guidelines.

## 9. Implementation Roadmap

These guidelines are designed to be adopted progressively. A phased implementation reduces the risk of disruption to ongoing procurements and allows for capacity building.

### 9.1 Phase 1 – Foundations (months 1-6)

- National coordinator (cybersecurity authority or CSIRT) endorses the guidelines and publishes them as official guidance.
- Each adopting entity appoints a Cybersecurity Officer with a supply-chain mandate and identifies a procurement security focal point.
- Each adopting entity establishes a supply-chain security policy and a procurement governance group (legal, IT/security, procurement, business owners).
- Each adopting entity builds an inventory of existing critical suppliers and tiers them by criticality (using the same Low / Medium / High scheme as this document).

### 9.2 Phase 2 – Adoption in New Procurements (months 6-12)

- Apply section 10.1 (Planning) and 10.2 (Selection) to all new tenders.
- Embed model clauses (audit rights, incident notification, data portability, exit, NDA continuity, sub-processor approval, build integrity, OEM-only) in standard contract templates.
- Mandate the vendor questionnaire (Mapping Excel) for any procurement above a national threshold or any procurement related to a critical or essential entity.
- Mandate SBOM, VDP and a supplier PSIRT for any software / digital-service procurement.

### 9.3 Phase 3 – Extension to Legacy Contracts (months 12-24)

- Apply section 10.3 (Operations) and section 10.4 (Vulnerability handling) to existing supplier relationships through contract amendments at renewal.
- Implement annual supplier risk re-evaluation.
- Develop joint incident playbooks with critical suppliers.
- Validate exit / decommissioning plans with the most critical suppliers.

### 9.4 Phase 4 – Continuous Improvement (year 2+)

- National authority publishes annual maturity assessment.
- Sectoral specialisations are added (financial-sector annex aligned with DORA, healthcare annex).
- Cross-LAC sharing of supplier intelligence (de-identified) is set up via LAC4.

- Integration with existing national strategies and digital-transformation initiatives is reviewed every 12 months.

## 9.5 Governance and Metrics for Continuous Evaluation

Adopting authorities should track at least the following metrics:

- Percentage of new tenders that include the standard security clauses.
- Percentage of suppliers who have completed the vendor questionnaire.
- Percentage of software/digital procurements that include an SBOM.
- Number of supply-chain incidents notified by suppliers within contractual timelines.
- Mean time to revoke supplier access at contract end.
- Number of critical suppliers with a tested exit plan.

## 9.6 Training Needs

- Procurement officers: secure procurement basics, model clauses, vendor questionnaire interpretation.
- Cybersecurity officers / CISOs: supplier risk assessment methodology, SBOM analysis, vulnerability handling (PSIRT, CVD, root-cause analysis), incident handling with suppliers, build-pipeline integrity assessment.
- Legal counsel: contractual mechanisms for cross-border audits, sub-processor approval, data localisation, cooperation with regulators.
- Senior management: oversight of supply-chain risk; risk-appetite setting.

## 10. Security Recommendations

This section contains the 63 standardised recommendations across six sections, mirroring the procurement lifecycle. Each recommendation is phrased as a question that the entity should be able to answer. The Criticality line below the question indicates the procurement-criticality tier at which the recommendation becomes mandatory: Low (mandatory everywhere), Medium (mandatory at Medium and High), or High (mandatory only at High). Each question is followed by a Rationale, practical Examples and further information, an optional illustrative case from the ENISA Threat Landscape, and a Mapping to relevant standards and frameworks.

Sections 10.1 to 10.6 below correspond to the six sections of the Guidelines:

- 10.1 – Planning (10 recommendations)
- 10.2 – Selection of suppliers and products (18 recommendations)
- 10.3 – Operations (12 recommendations)
- 10.4 – Vulnerability handling (8 recommendations)
- 10.5 – Incident handling (8 recommendations)
- 10.6 – Decommissioning / End of use (7 recommendations)

### 10.1 Planning

Planning sets the scope, the governance and the constraints under which any procurement will be carried out. Decisions taken at the planning stage shape what can – and cannot – be procured, who is accountable, and which minimum requirements apply. NIS2 Article 21(2)(d) and the ENISA Good Practices for Supply Chain Cybersecurity (2023) both require entities to define supply-chain security as a managed activity, not as a one-off task.

#### **P-01 Is there a management-approved strategy that determines what services and products may be procured from third parties?**

**Tier: Low** · *Mandatory at all criticality tiers (Low, Medium, High).*

##### **Rationale**

Nearly every digital activity can be procured from suppliers and vendors. However, in some instances an activity is so sensitive that it should not be carried out on third-party infrastructure – for example when an entity determines some business data highly confidential, or when data protection laws or existing contracts prohibit certain actions.

Without an explicit strategy, individual procurement decisions are taken in isolation and may end up exposing data or capabilities that the entity intended to keep in-house. ENISA's Good Practices for Supply Chain Cybersecurity identify a strategic corporate approach as the first of five focus areas for essential and important entities.

##### **Examples and further information**

Senior management should adopt a binding policy that defines (i) which categories of data and which mission-critical activities cannot be outsourced, (ii) which

categories may be outsourced only under restrictive conditions (e.g., onshore only, certified supplier only), and (iii) which categories are open to standard procurement.

The policy should be reviewed at least annually and after any major change in the regulatory environment.

- Categories of data that must remain in-house (e.g., classified, judicial, intelligence).
- Categories of data that may be processed by third parties only under specific conditions (e.g., personal data of citizens – onshore, certified provider).
- Activities that may be outsourced freely (e.g., generic office productivity, public-facing websites).

### Mapping

| Framework                                                  | Reference / clause                                                        |
|------------------------------------------------------------|---------------------------------------------------------------------------|
| NIS2 Directive                                             | Art. 21(2)(d) – supply chain security as part of risk-management measures |
| ENISA Good Practices for Supply Chain Cybersecurity (2023) | Area 3.1 – Strategic corporate approach                                   |
| ISO/IEC 27036-2                                            | Clause 6 – Information security in supplier relationships                 |
| NIST SP 800-161 Rev. 1                                     | Section 2.3 – C-SCRM strategy                                             |
| CISA SCRM Template                                         | Q. 2.3 – Organisation-wide end-to-end strategy                            |

### P-02 Are external and internal restrictions for procurement (sanctions, banned vendors, country of origin, data protection, contradictory contracts) considered and documented?

**Tier: Low** · *Mandatory at all criticality tiers (Low, Medium, High).*

#### Rationale

Entities may need to avoid certain third parties for legal or strategic reasons: sanctions regimes, prior incidents involving a vendor, data-protection rules limiting cross-border transfers, contradictory contracts with other parties, or national-security restrictions on technology origin.

If procurement officers do not have access to a current list of restrictions, issues are discovered late – typically at contract review – leading to wasted effort and delays. The CISA Vendor SCRM Template (Q. 2.4 / 4.9) makes a banned list check a standalone control.

#### Examples and further information

The procurement function, working with legal counsel and the cybersecurity officer, should maintain a list of restrictions and circulate it to all relevant employees. The list should be reviewed each time international sanctions are updated and each time a national authority issues an advisory on a vendor.

- Vendor with known and repeated cybersecurity issues
- Sanctions and embargoes

- Data-protection laws restricting cross-border transfers
- Existing contradictory contracts with other parties
- National-security restrictions on the origin of technology
- Existing entity policies on banned vendors

### Mapping

| Framework                   | Reference / clause                                                        |
|-----------------------------|---------------------------------------------------------------------------|
| EU ICT Supply Chain Toolbox | Risk scenarios – strategic dependency on high-risk vendors                |
| NIS2 Directive              | Art. 22 – coordinated security risk assessments of critical supply chains |
| CISA SCRM Template          | Q. 2.4 banned components, Q. 4.9 banned assets                            |
| NIST SP 800-161 Rev. 1      | Section 3 – Foreign ownership, control or influence                       |

## P-03 Has the entity appointed a cybersecurity officer with an explicit supply-chain mandate?

**Tier:** **Low** · *Mandatory at all criticality tiers (Low, Medium, High).*

### Rationale

Cybersecurity is a day-to-day activity for IT staff, but the strategic management of cybersecurity – including supply-chain aspects – needs to be assigned to a dedicated role.

ENISA's 2023 study found that 76% of surveyed organisations did not have dedicated roles and responsibilities for ICT/OT supply-chain cybersecurity. Without such a role, supply-chain risk falls between procurement (focused on cost and timeline) and IT (focused on operational stability) and is rarely addressed proactively.

### Examples and further information

The cybersecurity officer (CISO or equivalent) should have a written mandate that explicitly includes supply-chain cybersecurity. The role should sit at a level high enough to challenge procurement decisions and report to senior management.

### Mapping

| Framework                   | Reference / clause                                                  |
|-----------------------------|---------------------------------------------------------------------|
| ENISA Good Practices (2023) | Area 3.1 – designated supplier-risk role                            |
| ISO/IEC 27001:2022          | Clause 5.3 – Organisational roles, responsibilities and authorities |
| NIS2 Directive              | Art. 20 – management bodies' accountability                         |
| DORA – Reg. (EU) 2024/1773  | Art. 4 – governance arrangements for ICT third-party risk           |

## P-04 Are responsibilities and competences for the supply chain assigned in a documented manner (RACI)?

**Tier:** **Low** · *Mandatory at all criticality tiers (Low, Medium, High).*

### Rationale

The entity needs to assign all supply-chain related responsibilities so that no unwanted services are procured and so that ongoing supplier oversight has clear ownership. Diffused responsibilities – "someone in IT" or "someone in legal" – lead to gaps in due diligence and to incidents that are not handled coherently.

### Examples and further information

Maintain a RACI-style matrix that covers, at minimum, the items below. The matrix should be reviewed when there are organisational changes and at least once a year.

- Who is allowed to sign procurement contracts.
- Whether there is a threshold above which management approval is required for a new procurement.
- Who is responsible for evaluating existing contracts and for ensuring that new contracts are entered into the entity's licence-management system.
- Who validates supplier security posture before contract signature.
- Who is the operational point of contact with each supplier during the contract.
- Who validates incident notifications received from suppliers.
- Who authorises sub-processor changes and supplier ownership changes.
- Who approves contract termination and the exit plan.

### Mapping

| Framework              | Reference / clause                                                 |
|------------------------|--------------------------------------------------------------------|
| ISO/IEC 27036-2        | Clause 6.2 – Roles and responsibilities for supplier relationships |
| ISO/IEC 27001:2022     | Clauses 5.1, 5.3 – Management commitment and roles                 |
| NIST SP 800-161 Rev. 1 | Section 2.3.3 – C-SCRM PMO and roles                               |

## P-05 Are all relevant stakeholders included in the procurement process from an early stage?

**Tier: Medium** · *Mandatory at Medium and High criticality procurements.*

### Rationale

New procurements, especially for larger systems, may result in widespread discussions among stakeholders. Such discussions can bring useful insights that help decision-makers identify the right supplier, but they may also cause unrest among employees, customers or authorities. To prevent unforeseen issues, all relevant stakeholders should be included early and proactively.

### Examples and further information

Stakeholders depend on the context of the entity and the procurement at hand.

- IT personnel and operations
- Cybersecurity officers / CISO
- Employees (or their representatives) and union representatives
- Customers and citizens (where applicable)

- Existing suppliers or vendors that might be affected
- Competent authorities and regulators
- Partner entities
- Legal counsel

### Mapping

| Framework                  | Reference / clause                          |
|----------------------------|---------------------------------------------|
| ISO/IEC 27036-1            | Clause 5 – Multidisciplinary engagement     |
| DORA – Reg. (EU) 2024/1773 | Three-lines-of-defence in third-party risk  |
| NIST SP 800-161 Rev. 1     | Section 2.3.3 – Cross-functional engagement |

### P-06 Is the integration of the procured product or service planned in advance, including timeframes for installation, training, transition and start of use?

**Tier: Low** · Mandatory at all criticality tiers (Low, Medium, High).

### Rationale

New services or products should be integrated with a plan, not without consideration of all relevant aspects. A planned approach helps to ensure that procurement can be conducted within the foreseen time and cost frame and reduces the room for mistakes that affect cybersecurity.

### Examples and further information

An integration plan should at least include the following considerations:

- Point of contract signing
- Time until the service or product is ready to be installed
- Timeframe for installation
- Timeframe for training of personnel, including security training
- Transition period if an old system gets replaced, including data transfer
- Time for start of usage
- Strategic policy and management decisions taken at each milestone
- Stakeholder participation at each milestone

### Mapping

| Framework              | Reference / clause                             |
|------------------------|------------------------------------------------|
| ISO/IEC 27036-2        | Clause 7 – Initiation of supplier relationship |
| NIST SP 800-161 Rev. 1 | Section on lifecycle integration               |
| CISA SCRM Template     | Q. 2.3 – End-to-end lifecycle                  |

## P-07 Are risk assessments conducted by the entity for newly procured services and products?

**Tier: Low** · Mandatory at all criticality tiers (Low, Medium, High).

### Rationale

A risk assessment helps identify and reduce risks to the business operations of the entity. Risks are threats combined with their likelihood of occurrence. If the entity uses a formal risk-management framework, it should fold new procurement projects into that framework.

ENISA's 2023 study found that only 37% of organisations demonstrate due diligence or risk assessments of suppliers, and 9% do not evaluate supply-chain risk at all – a notable gap.

### Examples and further information

ISO/IEC 27005 is a risk assessment framework focused on cybersecurity. NIST SP 800-30 is the U.S. equivalent. The how to annex of these guidelines walks through a minimal six-step methodology.

Threats to consider for new procurements may include, but are not limited to:

- Failure of service at the third party
- Information leak at the third party (e.g. Verkada 2021 – credentials found online granted access to 150,000 customer cameras)
- Software vulnerability in the procured product (e.g. Kaseya VSA 2021 – zero-day used to push ransomware to managed customers)
- Spreading of malicious code or software via the vendor (e.g. SolarWinds 2020 – malware injected into Orion build process)
- Compromise of a sub-processor
- Misconfiguration in the supplier's environment (e.g. Codecov 2021 – Docker image bug exposed credentials, used to modify customer-facing bash script)

*ENISA Threat Landscape – illustrative case: Verkada (March 2021): credentials allegedly found online (OSINT) gave attackers access to 150,000 customer cameras. SolarWinds (2020) and Kaseya VSA (July 2021) are reference cases for the supply-chain attack pattern.*

### Mapping

| Framework                   | Reference / clause                      |
|-----------------------------|-----------------------------------------|
| ISO/IEC 27005               | Information security risk management    |
| NIST SP 800-30              | Guide for conducting risk assessments   |
| NIST SP 800-161 Rev. 1      | Appendix C – Risk exposure framework    |
| ENISA Good Practices (2023) | Area 3.2 – Supply chain risk management |

## P-08 Is there a published procurement security policy approved by senior management?

**Tier: Low** · Mandatory at all criticality tiers (Low, Medium, High).

### Rationale

A policy makes the entity's expectations explicit, both internally and to bidders. It supports consistent decision-making and provides legal cover for rejecting bids that do not meet minimum cybersecurity requirements.

### Examples and further information

The policy should reference these Guidelines as the source for minimum requirements, define the risk-tiering of suppliers, list the model clauses, and define escalation paths. It should be approved by the highest executive level and published, at minimum, on an internal portal.

### Mapping

| Framework                   | Reference / clause                                                        |
|-----------------------------|---------------------------------------------------------------------------|
| NIS2 Directive              | Art. 21(2)(a) – policies on risk analysis and information system security |
| ISO/IEC 27001:2022          | Clause 5.2 – Information security policy                                  |
| ENISA Good Practices (2023) | Area 3.1 – Policy and framework                                           |
| CISA SCRM Template          | Q. 4.3 – company-wide policies                                            |

## P-09 Is there a multidisciplinary procurement governance group (legal, IT/security, procurement, business)?

**Tier: High** · Mandatory at High criticality procurements only.

### Rationale

Supply-chain cybersecurity decisions cut across functions – legal, technical, financial and operational dimensions. A standing group, rather than ad-hoc consultation, is the only sustainable mechanism.

### Examples and further information

The group should meet at least quarterly and on demand for decisions on critical procurements. It should review the supplier risk register, approve material risk acceptances and validate the use of model clauses.

### Mapping

| Framework                  | Reference / clause                      |
|----------------------------|-----------------------------------------|
| ISO/IEC 27036-1            | Overview – multidisciplinary engagement |
| DORA – Reg. (EU) 2024/1773 | Provisions on management body           |
| NIST SP 800-161 Rev. 1     | Section 2.3.3                           |

## P-10 Does the entity maintain a supply-chain risk register that is reviewed periodically?

**Tier: Medium** · Mandatory at Medium and High criticality procurements.

### Rationale

A register of supplier risks – and not only of suppliers – is the operational instrument that translates the policy into day-to-day decisions. It enables tiering of controls, prioritisation of monitoring, and traceability of risk-acceptance decisions.

ENISA's Technical Implementation Guidance on Reg. (EU) 2024/2690 details how supplier-related risks should feed into the entity's overall risk-management measures.

### Examples and further information

The register should be linked to the entity's broader information-security risk management process, but specific enough to capture supplier-by-supplier risk. Each entry should include the supplier, the service/product, the criticality tier, the residual risk, the risk owner and the next review date.

### Mapping

| Framework                                                     | Reference / clause                               |
|---------------------------------------------------------------|--------------------------------------------------|
| ENISA Technical Implementation Guidance – Reg. (EU) 2024/2690 | Section on supply chain security risk management |
| ISO/IEC 27005                                                 | Information security risk management             |
| NIST SP 800-161 Rev. 1                                        | Appendix C – Risk exposure framework             |
| NIS2 Directive                                                | Art. 21(2)(d), Art. 22                           |
| ENISA Good Practices (2023)                                   | Area 3.2 – Supply chain risk management          |

## 10.2 Selection of suppliers and products

Selection is the stage at which the entity acquires its information about the supplier and locks in contractual obligations. The recommendations in this section cover legal enforceability, technical due diligence on the supplier and the product, minimum cybersecurity controls, contract clauses and product integrity. They draw on ENISA's Good Practices, the ENISA Threat Landscape for Supply Chain Attacks (2021) – from which several incident-based examples are taken – the EU CRA, ISO/IEC 27036, the CISA Vendor SCRM Template and NIST SP 800-161 Rev. 1.

### S-01 Can a contract with the third party be enforced in the jurisdiction the third party operates from?

**Tier:** **Low** · *Mandatory at all criticality tiers (Low, Medium, High).*

### Rationale

When forming a contract with a third party, the entity should consider whether the contract can be enforced by legal means. This is especially relevant for contracts with third parties that operate from a different jurisdiction or country, and where governmental access regimes may override commercial confidentiality.

### Examples and further information

Legal counsel should review the choice of governing law, the choice of forum, and the practical enforceability against the supplier's group structure. Where the supplier is part of a multinational group, an in-region contracting party should be required.

### Mapping

| Framework                             | Reference / clause                                       |
|---------------------------------------|----------------------------------------------------------|
| ISO/IEC 27036-2                       | Clause 6.3 – Legal and regulatory requirements           |
| DORA – Reg. (EU) 2024/1773            | Provisions on contractual arrangements and governing law |
| ENISA Cloud Computing Risk Assessment | Legal risks – jurisdiction                               |
| NIST SP 800-161 Rev. 1                | Section 3.4 – Foreign legal jurisdiction                 |

## S-02 Does the contract grant the entity (or its appointed auditor or competent authority) audit rights over the supplier and its sub-processors?

**Tier: Low** · *Mandatory at all criticality tiers (Low, Medium, High).*

### Rationale

Without audit rights, the entity has no independent means to verify that the supplier actually implements the security controls it claims. Audit rights also enable regulator-mandated audits when the entity is itself supervised.

ENISA's Good Practices identify audit rights as a routine obligation that customers should expect. The CISA SCRM Template (Q. 7.9) makes regularly scheduled audits a standalone item.

### Examples and further information

Audit rights should cover: the right to receive standard third-party audit reports (e.g., ISO/IEC 27001, SOC 2 Type II); the right to request additional information; the right of the entity, a third-party auditor or a regulator to conduct on-site or remote audits with reasonable notice; and the right to audit sub-processors via the supplier.

DORA RTS 1773 provides a strong reference point for financial-sector audit clauses; the same model can be used by other sectors.

### Mapping

| Framework                   | Reference / clause                             |
|-----------------------------|------------------------------------------------|
| DORA – Reg. (EU) 2024/1773  | Audit and inspection rights                    |
| ISO/IEC 27036-2             | Clause 7 – Verification of supplier            |
| ENISA Good Practices (2023) | Area 3.3 – Supplier relationship management    |
| CISA SCRM Template          | Q. 4.17, 7.9 – Contractual audit and assurance |

### S-03 Are third-party facilities necessary for the service or product located in secure locations?

**Tier: Medium** · *Mandatory at Medium and High criticality procurements.*

#### Rationale

Cloud and managed services rely on physical facilities. The location determines exposure to natural disasters, political instability, governmental access regimes and operational risks. Lack of transparency about locations is a red flag.

#### Examples and further information

The supplier should disclose the primary and disaster-recovery locations of the facilities used to provide the service. The entity should assess political stability, exposure to natural disasters, the presence of an export-control or governmental access regime, and the physical security of the site (typically through ISO/IEC 27001 or SOC 2 reports).

*ENISA Threat Landscape – illustrative case: Verkada (March 2021): the supplier's production server was compromised – physical location was not the issue, but lack of segmentation between facilities was.*

#### Mapping

| Framework                             | Reference / clause                  |
|---------------------------------------|-------------------------------------|
| ENISA Cloud Computing Risk Assessment | Physical and environmental risks    |
| ISO/IEC 27001:2022                    | Annex A.7 – Physical controls       |
| EU ICT Supply Chain Toolbox           | Risk scenarios on data localisation |
| CISA SCRM Template                    | Q. 5.1-5.7 – Physical security      |

### S-04 Does the third party operate an Information Security Management System (ISMS) covering the procured service or product?

**Tier: Low** · *Mandatory at all criticality tiers (Low, Medium, High).*

#### Rationale

An ISMS demonstrates that the supplier manages information security as a systematic activity rather than as ad-hoc fixes. ISO/IEC 27001 certification by an accredited body is the most widely recognised assurance form.

The entity should verify that the procured product or service is actually inside the certified scope, since an ISMS may cover only certain areas of a company. ENISA's 2023 study found 61% of organisations require security certification from suppliers, but the scope check is often missing.

### Examples and further information

The entity should ask for the certificate, the Statement of Applicability and the most recent surveillance audit report. For sectors with stricter expectations, equivalent or stronger assurance – SOC 2 Type II, sector-specific certifications, EU CC EUCC for products, EUCS for cloud services – should be required.

### Mapping

| Framework                                 | Reference / clause                                          |
|-------------------------------------------|-------------------------------------------------------------|
| ISO/IEC 27001:2022                        | Full standard                                               |
| EU Cybersecurity Act – Reg. (EU) 2019/881 | Cybersecurity certification framework                       |
| ENISA EUCS scheme                         | Cloud services certification                                |
| ENISA EUCC scheme                         | ICT product certification – Implementing Reg. (EU) 2024/482 |
| CISA SCRM Template                        | Q. 4.1, 4.2 – Certification / framework                     |

### S-05 Does the third party have a documented cybersecurity incident-handling plan, including notification obligations toward customers?

**Tier: Medium** · *Mandatory at Medium and High criticality procurements.*

### Rationale

In case of a security incident or detected vulnerability, the supplier should have pre-planned incident-handling procedures. This significantly reduces time to react and ensures that affected entities are informed and advised on the actions to take.

Mimecast (2021) showed how delayed or incomplete supplier notification compounds the impact: customers needed days to discover that certificates used to authenticate to their Microsoft 365 tenants had been compromised. Pre-existing playbooks shorten this gap.

### Examples and further information

The plan should be documented, exercised, and shared with the entity to the extent necessary. The supplier should appoint a CSIRT or PSIRT contact and provide its details. ISO/IEC 27035 and the FIRST.org PSIRT Services Framework are useful references.

*ENISA Threat Landscape – illustrative case: Mimecast (Jan 2021): attackers used a compromised supplier certificate to authenticate to Microsoft 365 tenants of customers – emphasising the value of fast supplier disclosure.*

### Mapping

| Framework                   | Reference / clause                                   |
|-----------------------------|------------------------------------------------------|
| ISO/IEC 27035               | Incident management                                  |
| NIS2 Directive              | Art. 21(2)(b) – incident handling                    |
| ENISA Good Practices (2023) | Area 3.3 – Supplier obligations on incident handling |
| CISA SCRM Template          | Q. 4.25 – CSIRT and customer notification            |

## S-06 Has the supplier provided a Software Bill of Materials (SBOM)?

**Tier:** **Low** · *Mandatory at all criticality tiers (Low, Medium, High).*

### Rationale

An SBOM is a machine-readable list of components contained in a software product. Without an SBOM, neither the supplier nor the entity can rapidly determine whether the product is affected by a newly disclosed vulnerability – as Log4Shell illustrated globally.

The EU Cyber Resilience Act establishes SBOM as a horizontal expectation for products with digital elements. The CISA / NTIA SBOM Minimum Elements provide a useful operational reference, and the CISA SCRM Template (Q. 2.5) makes BOM provision a standalone supplier check.

### Examples and further information

Require an SBOM in CycloneDX or SPDX format at the moment of acceptance and at every major update of the product. The SBOM should cover the supplier's first party code, and all included open-source and third-party components. Integrate the SBOM into vulnerability management so that, when a new vulnerability is disclosed, the entity can determine within hours which deployed products are affected.

### Mapping

| Framework                                     | Reference / clause                                                         |
|-----------------------------------------------|----------------------------------------------------------------------------|
| EU Cyber Resilience Act – Reg. (EU) 2024/2847 | Annex I, Part II – Vulnerability handling: SBOM in machine-readable format |
| CISA / NTIA SBOM Minimum Elements             | Format, depth and required fields                                          |
| ENISA Good Practices (2023)                   | Area 3.4 – Vulnerability handling – software supply-chain transparency     |
| NIST SP 800-161 Rev. 1                        | Section 2.5 – Information sharing and SBOM                                 |
| CISA SCRM Template                            | Q. 2.5 – BOM coverage and change tracking                                  |

### S-07 Has it been verified that the procured service or product does not suffer from known security vulnerabilities?

**Tier: Low** · *Mandatory at all criticality tiers (Low, Medium, High).*

#### Rationale

Before procuring a service or product, the entity should verify that there are no known security vulnerabilities. The simplest way is to scan the SBOM (S-06) against vulnerability databases.

Independent of the SBOM check, the entity should review reports about unsolved security issues – Cybersecurity journals, CVE databases, vendor advisories, sectoral CSIRTs.

#### Examples and further information

Use CVE / NVD search, OSS Index, GitHub Security Advisories or commercial SCA tools against the SBOM. Reject products that depend on unpatched components without a documented compensating control.

#### Mapping

| Framework                   | Reference / clause                                                          |
|-----------------------------|-----------------------------------------------------------------------------|
| ENISA Good Practices (2023) | Area 3.4 – Vulnerability handling                                           |
| ISO/IEC 30111               | Vulnerability handling processes                                            |
| CISA SCRM Template          | Q. 4.14, 4.22 – Vulnerability identification and scanning before acceptance |
| NIST SSDF (SP 800-218)      | Practices PO and PW                                                         |

### S-08 Does the third party follow a Secure Development Lifecycle (SDL) and protect the integrity of its build pipeline?

**Tier: Low** · *Mandatory at all criticality tiers (Low, Medium, High).*

#### Rationale

Software development should follow procedures that consider product security. Developers that use a standardised SDL produce fewer vulnerable releases. NIS2 Art. 21(3) explicitly requires entities to take into account the secure development practices of their suppliers.

The SolarWinds (2020) attack injected malicious code into the Orion build process – making build-pipeline integrity (CISA SCRM Q. 3.6, 3.7, 3.13) as important as the SDL itself. Codecov (2021) was a similar build-environment compromise. ENISA's analysis found that 66% of attacks targeted suppliers' code or processes.

#### Examples and further information

Evidence: secure coding standards, mandatory peer review, threat modelling, security testing (SAST, DAST, dependency scanning), security training of developers, and a formal release / approval process. ISO/IEC 27034, BSIMM, the Microsoft SDL and NIST SP 800-218 (SSDF) are common references.

Build-pipeline controls: source-code integrity (signed commits), reproducible builds, signed releases, SLSA-aligned provenance, restricted access to the build infrastructure.

*ENISA Threat Landscape – illustrative case: SolarWinds Orion (Dec 2020): malware injected during the supplier's build process; ~18,000 customers received the compromised update. Codecov (Apr 2021): credentials stolen from a Docker image were used to modify a customer-facing bash script – same pattern of build-environment compromise.*

### Mapping

| Framework               | Reference / clause                                     |
|-------------------------|--------------------------------------------------------|
| NIS2 Directive          | Art. 21(3) – secure development practices of suppliers |
| EU Cyber Resilience Act | Annex I – secure development requirements              |
| ISO/IEC 27034           | Application security                                   |
| NIST SSDF (SP 800-218)  | Secure Software Development Framework                  |
| CISA SCRM Template      | Q. 3.6, 3.7, 3.10, 3.13 – Code & build integrity       |
| Google SLSA             | Supply chain Levels for Software Artifacts             |

### S-09 Does the third party commit to providing security updates throughout the planned period of use, with a published Vulnerability Disclosure Policy?

**Tier: Low** · Mandatory at all criticality tiers (Low, Medium, High).

#### Rationale

If a security issue is identified after a product is considered out-of-life, the entity may need to operate it in a vulnerable state. Entities must select products that will receive security updates throughout their planned use period – this should be specified in the contract.

A published Vulnerability Disclosure Policy (VDP) creates a safe channel for security researchers to report vulnerabilities responsibly. EU CRA Art. 13-14 imposes specific obligations on manufacturers regarding vulnerability handling and coordinated disclosure.

#### Examples and further information

The supplier should disclose: the planned support period and end-of-life date; the patching SLA for critical vulnerabilities; the channel for receiving advisories; and the VDP point of contact (typically a security.txt file or dedicated security page).

The supplier's VDP should commit to acknowledging reports within a stated timeframe and define the triage, mitigation and coordinated-disclosure process.

### Mapping

| Framework                                     | Reference / clause                                       |
|-----------------------------------------------|----------------------------------------------------------|
| EU Cyber Resilience Act – Reg. (EU) 2024/2847 | Art. 13-14 – vulnerability handling and security updates |
| ISO/IEC 29147                                 | Vulnerability disclosure                                 |
| ISO/IEC 30111                                 | Vulnerability handling processes                         |
| ENISA Good Practices (2023)                   | Area 3.4 – Vulnerability handling                        |
| CISA SCRM Template                            | Q. 3.16 – PSIRT                                          |

### S-10 Does the third party provide data portability to prevent vendor lock-in?

**Tier: Low** · Mandatory at all criticality tiers (Low, Medium, High).

#### Rationale

Many services and products use proprietary data formats. Data created with the service can only be viewed or edited with that service. Some services do not provide an export option at all. In this case, data cannot be transferred to other services, which can result in data loss if the service is taken out of operation.

#### Examples and further information

Any service or product should provide export options. At minimum it should be possible to obtain a human-readable export that can be processed manually. A better option is a machine-readable export into an open format that can be used by other products without much effort. The contract should fix the export format, the export frequency and the maximum delivery time.

EU Data Act (Reg. (EU) 2023/2854) introduces switching and portability obligations for data-processing services that can be referenced.

### Mapping

| Framework                                                     | Reference / clause                     |
|---------------------------------------------------------------|----------------------------------------|
| ENISA Technical Implementation Guidance – Reg. (EU) 2024/2690 | Continuity and data portability        |
| ENISA Cloud Computing Risk Assessment                         | Lock-in risks                          |
| EU Data Act – Reg. (EU) 2023/2854                             | Switching and portability obligations  |
| ISO/IEC 19941 / 22123                                         | Cloud interoperability and portability |

### S-11 Are the third party's cybersecurity certifications validated, current, and in scope of the procured service?

**Tier: Low** · Mandatory at all criticality tiers (Low, Medium, High).

#### Rationale

Certifications are only meaningful when current, in scope and from an accredited body. Certifications also need to certify a relevant subject – a quality-management

certificate is not useful to determine cybersecurity maturity, and a cybersecurity certificate that does not cover the data centre but only the administrative area of a third party is of limited use.

### Examples and further information

Validate the certificate with the issuing body or its public registry; verify that the scope covers the procured service; review the most recent surveillance / recertification audit report; and record the expiry date to re-check before contract renewal.

### Mapping

| Framework                                 | Reference / clause                                 |
|-------------------------------------------|----------------------------------------------------|
| EU Cybersecurity Act – Reg. (EU) 2019/881 | European cybersecurity certification framework     |
| ENISA EUCC                                | Common Criteria-based scheme – Reg. (EU) 2024/482  |
| ENISA EUCS                                | Cloud services scheme                              |
| ISO/IEC 17021                             | Conformity assessment – accreditation requirements |
| CISA SCRM Template                        | Q. 4.1 / 4.2 – third-party attestation             |

## S-12 Has the supplier provided their own risk assessment for the product or service in question, including residual risks accepted?

**Tier: Medium** · *Mandatory at Medium and High criticality procurements.*

### Rationale

The supplier sees risks that the entity cannot – internal architecture, history of vulnerabilities, dependencies on sub-processors. Requiring the supplier's risk assessment makes those risks transparent and informs the entity's own risk management.

### Examples and further information

The supplier should provide a summarised risk assessment at contract signature and on each major release, indicating residual risks accepted by the supplier and any compensating controls expected from the entity.

### Mapping

| Framework                   | Reference / clause                              |
|-----------------------------|-------------------------------------------------|
| ISO/IEC 27036-3             | Guidelines for ICT supply chain – supplier-side |
| ENISA Good Practices (2023) | Area 3.2 – Supply chain risk management         |
| EU Cyber Resilience Act     | Risk-based design and conformity assessment     |
| CISA SCRM Template          | Q. 2.3 – Strategy implementation                |

## S-13 Are personnel of the supplier with access to entity systems or data subject to security screening (background checks, references) proportionate to the role?

**Tier: Medium** · *Mandatory at Medium and High criticality procurements.*

### Rationale

Insider risk in the supplier's organisation is a recurring incident vector – privileged technicians, on-call engineers, support staff. Proportionate screening reduces the probability of malicious insiders without imposing disproportionate cost.

CISA SCRM Template Q. 6.3-6.5 explicitly requires background-check policies for the supplier's own employees, the supplier's suppliers, and any subcontractors, with allowances for jurisdictions where this is not legally permitted.

### Examples and further information

Screening should be commensurate with the data classification and the access level. Typical baseline: identity verification, employment-history check, and confidentiality undertaking. For privileged or critical roles: criminal-record check (where legally permitted), references, periodic re-checks.

Onboarding: documented; covers security awareness training and asset distribution. Offboarding: documented; covers access removal and asset recovery.

### Mapping

| Framework              | Reference / clause                                       |
|------------------------|----------------------------------------------------------|
| ISO/IEC 27001:2022     | Annex A.6 – People controls                              |
| ISO/IEC 27036-2        | Personnel security clauses                               |
| CISA SCRM Template     | Q. 6.1-6.6 – Personnel security, onboarding, offboarding |
| NIST SP 800-161 Rev. 1 | Personnel security in supply chain                       |

## S-14 Are sub-processors / fourth parties identified and contractually controlled, with notification of changes?

**Tier: Medium** · *Mandatory at Medium and High criticality procurements.*

### Rationale

Most modern services rely on sub-processors. A breach at a fourth party can cascade up the supply chain to the entity, even though the entity has no direct relationship with that party. The recent regulatory trend (DORA RTS 532, NIS2 Art. 22) is to make fourth-party visibility and control mandatory.

CISA SCRM Template Q. 2.10 makes notification of subcontractor changes a standalone obligation.

### Examples and further information

The contract should require: an up-to-date list of sub-processors; prior approval (or at least notification with right of objection) for new sub-processors; flow-down of the entity's security obligations to sub-processors; and audit rights extending to sub-processors via the prime supplier.

### Mapping

| Framework                 | Reference / clause                          |
|---------------------------|---------------------------------------------|
| DORA – Reg. (EU) 2025/532 | RTS on subcontracting                       |
| NIS2 Directive            | Art. 21(2)(d) and Art. 22                   |
| ISO/IEC 27036-2           | Extended supply chain                       |
| CISA SCRM Template        | Q. 2.10 – Subcontractor change notification |

### S-15 Does the contract require notification of changes in ownership, control or location of the supplier?

**Tier: Medium** · *Mandatory at Medium and High criticality procurements.*

#### Rationale

Mergers, acquisitions, changes of control or relocation of operations can materially change the risk profile of a supplier – for example by bringing the supplier under a different jurisdiction, sanctions regime or governmental access regime.

#### Examples and further information

The contract should require advance notification of changes of ownership of more than a defined threshold (e.g., 25%); changes in the country of incorporation or country of operation; changes in the country of data storage. The entity should retain a contractual right to terminate without penalty if the change is unacceptable.

### Mapping

| Framework                   | Reference / clause                               |
|-----------------------------|--------------------------------------------------|
| DORA – Reg. (EU) 2024/1773  | Contractual arrangements: change of control      |
| ENISA Good Practices (2023) | Area 3.3 – Manage changes in supplier agreements |
| EU ICT Supply Chain Toolbox | Strategic dependency                             |

### S-16 Are minimum cybersecurity controls included in the tender specifications and weighted in the evaluation?

**Tier: Low** · *Mandatory at all criticality tiers (Low, Medium, High).*

#### Rationale

If cybersecurity is not a scored evaluation criterion, suppliers will compete on price and timeline alone, and the cheapest insecure offer wins. Embedding minimum controls and a security score in the evaluation grid changes that incentive.

#### Examples and further information

Tender specifications should include a clear minimum-requirement section (pass / fail) and a scored cybersecurity section. The minimum requirement section should reference these guidelines and make it explicit that any non-compliance with mandatory items disqualifies the offer. The scored section should reward suppliers with stronger assurance, broader certifications and more transparent SDL practices.

### Mapping

| Framework                        | Reference / clause                           |
|----------------------------------|----------------------------------------------|
| ENISA Good Practices (2023)      | Area 3.5 – Quality of products and practices |
| EU public-procurement directives | Use of qualitative award criteria            |
| ISO/IEC 27036-2                  | Clause on supplier selection                 |

**S-17 For hardware procurement, does the supplier source only from original equipment manufacturers (OEM) or licensed resellers, with anti-counterfeiting and tamper-evident controls?**

**Tier: High** · *Mandatory at High criticality procurements only.*

### Rationale

Counterfeit hardware is a documented attack vector – modified components, tampered packaging or fake firmware enter the supply chain through unauthorised resellers. CISA SCRM Template Q. 5.10 and Q. 2.6 / 2.7 cover OEM-only sourcing, controlled BOM, and chain-of-custody.

### Examples and further information

Require: OEM-or-authorized-reseller-only sourcing for key components; tamper-evident packaging; controlled BOM and chain-of-custody documentation in transit; supplier-side processes to detect and dispose of counterfeit parts.

### Mapping

| Framework              | Reference / clause                                                                        |
|------------------------|-------------------------------------------------------------------------------------------|
| CISA SCRM Template     | Q. 2.6, 2.7, 5.10 – OEM/Authorised resellers, BOM, tamper-evident, counterfeit prevention |
| NIST SP 800-161 Rev. 1 | Provenance and integrity                                                                  |
| ISO/IEC 27036-2        | Clause on hardware integrity                                                              |

**S-18 Does the supplier protect the integrity of code, build pipeline and software-release distribution (signed releases, controlled build environments, no unauthorised changes)?**

**Tier: High** · *Mandatory at High criticality procurements only.*

### Rationale

The SolarWinds and Codecov attacks both compromised the supplier's build environment and used the supplier's own distribution channel to push malicious code to customers. Build-environment integrity is therefore distinct from SDL practices and warrants its own check.

CISA SCRM Template Q. 3.6, 3.7 and 3.13 explicitly cover protection of code from unauthorised changes, software-release integrity verification, and hardened build / compile processes.

### Examples and further information

Evidence: code signing, reproducible builds, restricted access to build infrastructure, build-pipeline auditing, software bill of materials at release time, optional alignment with Google SLSA levels.

*ENISA Threat Landscape – illustrative case: SolarWinds Orion (2020) – malicious code injected at the supplier's build process. Codecov (2021) – bash script modified using credentials extracted from a Docker image. Both attacks bypassed customer-side controls because they originated inside the supplier's distribution channel.*

### Mapping

| Framework                   | Reference / clause                                         |
|-----------------------------|------------------------------------------------------------|
| CISA SCRM Template          | Q. 3.6, 3.7, 3.10, 3.13 – Code integrity and build process |
| Google SLSA                 | Supply chain Levels for Software Artifacts                 |
| NIST SSDF (SP 800-218)      | Practice PS – Protect the software                         |
| ENISA Good Practices (2023) | Area 3.5 – Quality of products                             |

## 10.3 Operations

Operations is the longest phase of the supplier relationship. The recommendations here cover ongoing risk monitoring, joint operations, training, configuration hardening, identity and access controls, segmentation, patching, and supplier-side personnel governance. Many breaches originating in suppliers occurred not because the contract was weak, but because the relationship was not actively managed.

### O-01 Is supplier risk and cybersecurity posture re-evaluated at least annually, and on material changes?

**Tier: Medium** · Mandatory at Medium and High criticality procurements.

#### Rationale

An initial risk assessment before acquiring a new service is not enough to ensure security over time. Cybersecurity risk needs to be evaluated on a regular basis. A usual cadence is yearly, plus on material changes (notified incident, change of control, change of criticality).

#### Examples and further information

Use the same Vendor Questionnaire used at selection, so changes are visible. Update the supplier risk register as a result.

### Mapping

| Framework                   | Reference / clause                       |
|-----------------------------|------------------------------------------|
| DORA – Reg. (EU) 2024/1774  | Periodic monitoring of ICT third parties |
| ISO/IEC 27036-2             | Ongoing relationship monitoring          |
| ENISA Good Practices (2023) | Area 3.3 – Continuous monitoring         |
| NIST SP 800-161 Rev. 1      | Continuous monitoring                    |

## O-02 Are cybersecurity threat information and incident information shared between the entity and the third party?

**Tier: Medium** · *Mandatory at Medium and High criticality procurements.*

### Rationale

When a cybersecurity threat becomes known, sharing increases the security of both parties. Threat information includes incidents, increased attacks (e.g., targeted phishing campaigns), and new vulnerabilities affecting software used by either party.

### Examples and further information

The contract should define which categories of information will be shared (vulnerabilities affecting the product, indicators of compromise observed by the supplier, suspicious activity targeting the entity), the channel (e.g., MISP, secure email, portal), and the cadence. Confidentiality and protection of shared intelligence should be addressed.

### Mapping

| Framework                   | Reference / clause                                                                       |
|-----------------------------|------------------------------------------------------------------------------------------|
| NIS2 Directive              | Art. 29 – voluntary cybersecurity information-sharing arrangements                       |
| ENISA Good Practices (2023) | Area 3.3 – Information sharing                                                           |
| ISO/IEC 27010               | Information security management for inter-sector and inter-organisational communications |

## O-03 Are administrators trained to ensure the secure operation of the procured service or product, including security-relevant configuration?

**Tier: Low** · *Mandatory at all criticality tiers (Low, Medium, High).*

### Rationale

Misconfiguration of cloud and managed services is consistently one of the top root causes of breaches. Trained administrators are the most cost-effective preventive control. CISA SCRM Q. 4.16 makes administrator cybersecurity training a standalone supplier obligation.

### Examples and further information

The contract should include initial training and a refresher cadence after major releases. Training should cover security configuration, identity and access management, logging and monitoring, and the supplier's incident-response process. Track training compliance.

- Cryptographic operations
- Identity and access management
- Network configuration
- Patch management
- Backup strategy

### Mapping

| Framework                   | Reference / clause                                  |
|-----------------------------|-----------------------------------------------------|
| ISO/IEC 27001:2022          | Annex A.6.3 – Awareness and training                |
| ENISA Good Practices (2023) | Area 3.3 – Personnel awareness                      |
| CIS Controls v8             | Control 14 – Security Awareness and Skills Training |
| CISA SCRM Template          | Q. 4.16 – Cybersecurity training for administrators |

## O-04 Are end users trained on security-sensitive aspects of the procured service or product?

**Tier:** **Low** · *Mandatory at all criticality tiers (Low, Medium, High).*

### Rationale

In many services or products not only administrators, but also regular users, can perform security-sensitive operations – sharing or editing business data, changing certain configurations that may expose or alter data in unwanted ways.

### Examples and further information

The supplier should provide standard end-user training material, and the entity should integrate the supplier's product into its general awareness programme. Phishing simulations should include the supplier's product wherever relevant.

- Data sharing and exposure to third parties
- Altering or deleting data in a non-recoverable way
- Activating functions with automatic, additional billing
- Unwanted data upload to third-party servers

### Mapping

| Framework                   | Reference / clause                                         |
|-----------------------------|------------------------------------------------------------|
| ISO/IEC 27001:2022          | Annex A.6.3                                                |
| NIS2 Directive              | Art. 21(2)(g) – basic cyber-hygiene practices and training |
| ENISA Good Practices (2023) | Area 3.3 – Personnel awareness                             |

### O-05 Is the configuration of the procured service or product hardened to a defined baseline and verified by a different person than the one configuring it?

**Tier: Low** · Mandatory at all criticality tiers (Low, Medium, High).

#### Rationale

Default configurations are typically optimised for ease of installation, not security. A documented hardening baseline aligned with the supplier's recommendations and recognised benchmarks closes known weaknesses. Configuration should be checked at regular intervals and after every update and reviewed by a different person to avoid unintentional oversight.

#### Examples and further information

Adopt either the supplier's hardening guide, the relevant CIS Benchmark, or an internally validated baseline. Track configuration drift and remediate. Where the procured service is configured by the supplier, the contract should oblige the supplier to apply a defined baseline.

- Cryptographic operations
- Identity and access management
- Network configuration
- Patch management
- Backup strategy

#### Mapping

| Framework                   | Reference / clause                              |
|-----------------------------|-------------------------------------------------|
| CIS Benchmarks              | Configuration baselines per technology          |
| ENISA Good Practices (2023) | Area 3.5 – Quality of products and practices    |
| NIST SP 800-53 Rev. 5       | CM family – Configuration Management            |
| CISA SCRM Template          | Q. 3.15, 4.19 – Secure-by-default and hardening |

### O-06 Are backups conducted regularly, stored independently of the supplier, and restorable without the supplier?

**Tier: Low** · Mandatory at all criticality tiers (Low, Medium, High).

#### Rationale

Data can be lost due to hardware failure, accidental deletion or ransomware attack. A solid backup strategy is necessary to restore data. Backups stored only inside the supplier are useless when the supplier is the source of disruption.

#### Examples and further information

Backups should be conducted at least daily, stored outside the supplier, in a format that can be restored without the supplier's tools, and tested at least annually. Encryption keys should be held by the entity. If the supplier does not provide automatic backups, a fixed manual procedure should be implemented and audited.

### Mapping

| Framework                             | Reference / clause                    |
|---------------------------------------|---------------------------------------|
| NIS2 Directive                        | Art. 21(2)(c) – business continuity   |
| ENISA Cloud Computing Risk Assessment | Lock-in / continuity                  |
| CIS Controls v8                       | Control 11 – Data Recovery            |
| ISO/IEC 27031                         | ICT readiness for business continuity |

### O-07 Are operative responsibilities clearly assigned between the entity and the third party (RACI)?

**Tier: Medium** · *Mandatory at Medium and High criticality procurements.*

#### Rationale

Depending on the product or service, administration may be the responsibility of the entity, the third party, or shared. To ensure no area of administration remains unhandled, all responsibilities must be clearly assigned. Misalignment is a frequent root cause of access-management failures (e.g., dormant accounts of former employees remaining active because each side believed the other was responsible).

#### Examples and further information

Use a RACI matrix that covers the items below. Review on changes to the service and at least annually.

- Patches
- Security settings
- Identity and access management
- Configuration
- Data handling
- (De)activation of functions and plug-ins
- Logging and monitoring
- Incident response steps

### Mapping

| Framework                   | Reference / clause                            |
|-----------------------------|-----------------------------------------------|
| ISO/IEC 27036-2             | Operational responsibilities                  |
| ENISA Good Practices (2023) | Area 3.3 – Operational ownership              |
| CISA SCRM Template          | Q. 4.15 – Network access control / role-based |

## O-08 Are contracts (and licences) tracked, re-evaluated, and renewed (or formally cancelled) on a regular basis?

**Tier: Medium** · Mandatory at Medium and High criticality procurements.

### Rationale

Contracts often have limited duration or automatic renewal. All procurement contracts should be tracked to ensure that no product or service becomes unusable because licences expire unexpectedly, and to avoid unintended automatic renewals on contracts the entity wishes to cancel.

### Examples and further information

Establish a fixed procedure to evaluate existing contracts on a regular basis. Track key dates: end of term, automatic-renewal trigger date, notice period, end of vendor support period.

### Mapping

| Framework                   | Reference / clause        |
|-----------------------------|---------------------------|
| ISO/IEC 27036-2             | Relationship management   |
| ENISA Good Practices (2023) | Area 3.3 – Manage changes |

## O-09 Are identity and access controls for third-party personnel enforced (named accounts, MFA, JIT elevation, periodic review, no standing privileged access)?

**Tier: Low** · Mandatory at all criticality tiers (Low, Medium, High).

### Rationale

Standing privileged access for the supplier's staff is a common compromise vector. Time-bound, named, MFA-protected access, with logging, reduces this risk substantially. The Verkada incident illustrated how the absence of such controls allowed an external actor to access privileged surveillance management consoles.

### Examples and further information

Implement: named accounts (no shared accounts) for supplier staff; multi-factor authentication; just-in-time elevation for privileged actions where technically feasible; session recording for high-risk activities; quarterly access review.

*ENISA Threat Landscape – illustrative case: Verkada (March 2021) – privileged access available remotely without strong controls allowed access to 150,000 customer cameras.*

### Mapping

| Framework                                                     | Reference / clause                            |
|---------------------------------------------------------------|-----------------------------------------------|
| NIS2 Directive                                                | Art. 21(2)(i) – access control policies       |
| ENISA Technical Implementation Guidance – Reg. (EU) 2024/2690 | Identity and access section                   |
| CIS Controls v8                                               | Controls 5, 6 – Account and access management |
| ISO/IEC 27001:2022                                            | Annex A.5.15-5.18 – Access control            |
| CISA SCRM Template                                            | Q. 4.15 – Network access control              |

### O-10 Is the procured service or product network-segmented from the rest of the entity's environment, with explicit ingress and egress allow-lists?

**Tier: High** · Mandatory at High criticality procurements only.

#### Rationale

Network segmentation limits lateral movement after a compromise – both from the supplier into the entity and vice versa. It is one of the most effective measures against the supply-chain attack pattern in which a trusted supplier component becomes the entry point.

In SolarWinds, customers that segmented Orion's outbound traffic limited exfiltration significantly compared to those that allowed broad outbound access from the management server.

#### Examples and further information

Deploy the supplier's product in a dedicated network segment with explicit egress and ingress allow-lists. Where the supplier requires connectivity into the entity's environment, allow-list at host and port level, not at IP-range level. Terminate connectivity when not required.

*ENISA Threat Landscape – illustrative case: SolarWinds (2020) – entities that restricted Orion's outbound connectivity limited the impact of the implant.*

### Mapping

| Framework                   | Reference / clause                             |
|-----------------------------|------------------------------------------------|
| CIS Controls v8             | Control 12 – Network Infrastructure Management |
| NIST SP 800-207             | Zero Trust Architecture                        |
| ENISA Good Practices (2023) | Area 3.5 – Defence-in-depth                    |
| ISO/IEC 27001:2022          | Annex A.8.20-8.22 – Network controls           |
| CISA SCRM Template          | Q. 4.19 – Network segmentation / IDS           |

## O-11 Is patching and security update management agreed contractually and monitored?

**Tier: Low** · Mandatory at all criticality tiers (Low, Medium, High).

### Rationale

EU CRA Art. 13 establishes obligations on manufacturers regarding security updates throughout the support period. The entity, on its side, must ensure those updates actually reach the deployed product within a defined timeframe.

### Examples and further information

The contract should specify: the supplier's commitment to provide security updates throughout the planned use period, the maximum time to release a patch for critical vulnerabilities, the entity's obligation to deploy patches within a defined window, and the consequences of missing those windows.

### Mapping

| Framework                                                     | Reference / clause                                                                                   |
|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| EU Cyber Resilience Act – Reg. (EU) 2024/2847                 | Art. 13 – security update obligations                                                                |
| NIS2 Directive                                                | Art. 21(2)(e) – security in network and information systems acquisition, development and maintenance |
| ENISA Technical Implementation Guidance – Reg. (EU) 2024/2690 | Patch management section                                                                             |
| CIS Controls v8                                               | Control 7 – Continuous Vulnerability Management                                                      |
| CISA SCRM Template                                            | Q. 4.23 – patch management                                                                           |

## O-12 Is there a Code of Conduct binding the supplier and its subcontractors with respect to security, privacy and confidentiality?

**Tier: Medium** · Mandatory at Medium and High criticality procurements.

### Rationale

A Code of Conduct, formally accepted by supplier personnel and sub-suppliers, makes expectations explicit and supports enforcement. CISA SCRM Q. 6.13 makes this a standalone control.

### Examples and further information

The Code of Conduct should be available and visible to employees, suppliers and subcontractors, kept up to date, and accompanied by training. A point of contact for questions / violations should be designated.

### Mapping

| Framework          | Reference / clause                  |
|--------------------|-------------------------------------|
| CISA SCRM Template | Q. 6.13 – Code of Conduct           |
| ISO/IEC 27001:2022 | Annex A.5 – Organisational policies |

## 10.4 Vulnerability Handling

Vulnerabilities are continuously discovered in the products and services the entity depends on. ENISA's Good Practices identify vulnerability handling as one of five focus areas for supply-chain cybersecurity, distinct from incident handling: a vulnerability becomes an incident only if it is exploited. The recommendations in this section cover the supplier side (PSIRT, formal vulnerability and weakness analysis, root-cause analysis, scoring and risk-based maintenance policy, customer notification) and the entity side (internal vulnerability management with SBOM monitoring, patch testing and rollback, participation in coordinated vulnerability disclosure).

### V-01 Does the third party operate a Product Security Incident Response Team (PSIRT) with a documented process to assess, prioritise and remediate reported vulnerabilities?

**Tier:** **Low** · *Mandatory at all criticality tiers (Low, Medium, High).*

#### Rationale

A PSIRT is the operational unit that turns a vulnerability report into a fix and an advisory. Without one – or with one that lacks documented triage criteria – vulnerabilities sit untreated and customers are kept in the dark.

ENISA Good Practices (Area 3.4) and CISA SCRM §3.16 both treat the existence of a PSIRT-equivalent function as a baseline expectation for any product or digital-service supplier. The FIRST.org PSIRT Services Framework provides a model for what the function should cover.

#### Examples and further information

Evidence the supplier should provide: PSIRT charter or equivalent, named point of contact (often via security.txt), triage SLA, severity matrix, and statistics on time-to-fix per severity tier from the past year.

The PSIRT should assess, prioritise and remediate vulnerabilities, ensure that fixes ship within a window proportionate to severity, and coordinate disclosure with reporters.

#### Mapping

| Framework                                 | Reference / clause                                                                       |
|-------------------------------------------|------------------------------------------------------------------------------------------|
| <b>ENISA Good Practices (2023)</b>        | Area 3.4 – Vulnerability handling: monitoring, scoring, treatment, customer notification |
| <b>FIRST.org PSIRT Services Framework</b> | Function definitions and maturity                                                        |
| <b>ISO/IEC 30111</b>                      | Vulnerability handling processes                                                         |
| <b>CISA SCRM Template</b>                 | Q. 3.16 – Product Security Incident Reporting and Response (PSIRT)                       |
| <b>EU Cyber Resilience Act</b>            | Art. 13 – Manufacturer vulnerability handling                                            |

## V-02 Does the third party perform formal vulnerability and weakness analysis on every release (SAST, DAST, software composition analysis, fuzzing)?

**Tier: Medium** · *Mandatory at Medium and High criticality procurements.*

### Rationale

Pre-release vulnerability analysis is the cheapest place to fix problems. Suppliers without a documented programme will discover the same classes of bugs over and over – and customers will pay the operational cost.

CISA SCRM §3.14 makes this a standalone supplier control, distinct from the broader SDL (S-08), and asks whether the analysis is automated and whether executable code is tested before release. NIST SSDF practice PW (Produce Well-Secured Software) covers the same ground.

### Examples and further information

Evidence: tooling list (e.g., Semgrep / SonarQube for SAST, OWASP ZAP / Burp for DAST, Dependency-Check / Snyk for SCA, AFL / libFuzzer for fuzzing), the gating policy (which severities block a release), and aggregated statistics on findings closed pre-release.

### Mapping

| Framework                   | Reference / clause                                   |
|-----------------------------|------------------------------------------------------|
| ENISA Good Practices (2023) | Area 3.4 – Vulnerability handling                    |
| NIST SSDF (SP 800-218)      | Practice PW – Produce Well-Secured Software          |
| CISA SCRM Template          | Q. 3.14 – Formal vulnerability and weakness analysis |
| ISO/IEC 27034               | Application security                                 |
| EU Cyber Resilience Act     | Annex I – secure design and development              |

## V-03 Does the third party perform root-cause analysis of disclosed vulnerabilities and feed lessons back into its SDL, tools and training?

**Tier: Medium** · *Mandatory at Medium and High criticality procurements.*

### Rationale

Fixing a vulnerability is necessary but not sufficient. If the underlying cause – a missing pattern in the threat model, a class of bug not caught by static analysis, a process gap – is not addressed, the same defect will reappear in the next release.

CISA SCRM §3.17 asks suppliers explicitly whether root-cause analysis is conducted and whether it informs updates to the secure-development process, tools and training.

### Examples and further information

Evidence: a sample post-mortem from a recent disclosed vulnerability, showing the root cause, the corrective actions in the SDL, and the closure of those actions; a metric for repeat vulnerability classes year-on-year.

### Mapping

| Framework                   | Reference / clause                                          |
|-----------------------------|-------------------------------------------------------------|
| ENISA Good Practices (2023) | Area 3.4 – Continuous improvement of vulnerability handling |
| CISA SCRM Template          | Q. 3.17 – Root-cause analysis feeding the SDL               |
| NIST SSDF (SP 800-218)      | Practice RV – Respond to Vulnerabilities                    |

## V-04 Does the third party use a documented vulnerability-scoring system (e.g., CVSS) and a risk-based maintenance / patching policy?

**Tier: Low** · Mandatory at all criticality tiers (Low, Medium, High).

### Rationale

Treating every vulnerability the same is wasteful and slow. A documented scoring system (CVSS is the de-facto standard) and a maintenance policy that maps severity to time-to-fix and to communication obligations enables consistent, defensible decisions.

ENISA Good Practices §3.4 explicitly call for risk analysis of vulnerabilities using a vulnerability scoring system and maintenance policies for treatment of identified vulnerabilities depending on the risk.

### Examples and further information

Evidence: the policy itself (severity bands, time-to-fix targets per band, customer-notification triggers), and the CVSS environmental factors the supplier applies. The policy should also account for vulnerabilities in third-party components carried via the SBOM (S-06).

### Mapping

| Framework                   | Reference / clause                                                      |
|-----------------------------|-------------------------------------------------------------------------|
| ENISA Good Practices (2023) | Area 3.4 – Risk analysis with CVSS, maintenance policies                |
| FIRST.org CVSS              | Common Vulnerability Scoring System                                     |
| CISA SCRM Template          | Q. 3.16.1, 4.14 – Vulnerability assessment, prioritisation, remediation |
| ISO/IEC 30111               | Vulnerability handling processes                                        |

## V-05 Does the third party have a documented process and a cadence for notifying the entity of vulnerabilities affecting the procured product or service?

**Tier: Low** · Mandatory at all criticality tiers (Low, Medium, High).

### Rationale

A patch released without notification is invisible to most customers. The supplier must have a process for proactive notification, with a cadence and content sufficient for the entity's vulnerability-management programme.

ENISA Good Practices §3.4 list 'processes to inform customers' as a baseline. CISA SCRM §4.21 / §4.25 cover incident detection practices and the supplier's process to notify customers when a product or service is impacted.

### Examples and further information

Evidence: the supplier's advisory cadence (e.g., monthly or per-severity), the channel (signed email, RSS, customer portal), the content (CVE, CVSS, affected versions, exploit status, mitigation), and the SLA for proactive notification on critical advisories.

### Mapping

| Framework                   | Reference / clause                              |
|-----------------------------|-------------------------------------------------|
| ENISA Good Practices (2023) | Area 3.4 – Processes to inform customers        |
| CISA SCRM Template          | Q. 4.21, 4.25 – Customer notification on impact |
| ISO/IEC 29147               | Coordinated vulnerability disclosure            |
| EU Cyber Resilience Act     | Art. 14 – Coordinated vulnerability disclosure  |

## V-06 Does the entity maintain its own vulnerability-management programme covering supplier-provided software, with continuous SBOM-based monitoring?

**Tier: Low** · Mandatory at all criticality tiers (Low, Medium, High).

### Rationale

Even with strong supplier practices, the entity is responsible for what runs in its own environment. CISA SCRM §4.14 and §4.22 ask the entity to maintain documented vulnerability identification and management, including scanning supplier-provided software before acceptance and continuously thereafter.

Pairing this programme with the SBOM (S-06) lets the entity determine, within hours of a new disclosure, whether any deployed product is affected – the absence of which was the principal pain point during Log4Shell.

### Examples and further information

Evidence: a vulnerability-management policy, a tool stack (CVE feed ingestion, SBOM monitoring such as Dependency-Track, scanner integration with the asset inventory), prioritisation criteria (asset criticality, exploitability, exposure), and a closed-loop metric of time-to-mitigate per severity.

### Mapping

| Framework                   | Reference / clause                                                                            |
|-----------------------------|-----------------------------------------------------------------------------------------------|
| ENISA Good Practices (2023) | Area 3.4 – Patch management; monitoring of vulnerabilities                                    |
| CISA SCRM Template          | Q. 4.14, 4.22 – Internal vulnerability management; vulnerability scanning prior to acceptance |
| CIS Controls v8             | Control 7 – Continuous Vulnerability Management                                               |
| NIST SP 800-40 Rev. 4       | Guide to Enterprise Patch Management                                                          |

## V-07 Does the entity test patches before deployment and maintain rollback / back-out procedures?

**Tier: Medium** · Mandatory at Medium and High criticality procurements.

### Rationale

Patches occasionally regress functionality, break integrations or – rarely – introduce new vulnerabilities. A test-then-deploy cadence and a tested rollback procedure are necessary for any service whose unavailability has material impact.

ENISA Good Practices §3.4 specifically include 'patch verification and testing' and 'rollback procedures and effective back-up & restore processes' in the patch-management baseline.

### Examples and further information

Test patches in a staging environment (or via canary deployment) before broad rollout; document the rollback procedure for each critical service; pair with O-06 (independent backups) and I-04 (restore tests) so that rollback is realistic when needed.

### Mapping

| Framework                   | Reference / clause                                                  |
|-----------------------------|---------------------------------------------------------------------|
| ENISA Good Practices (2023) | Area 3.4 – Patch verification, testing, rollback, back-up & restore |
| NIST SP 800-40 Rev. 4       | Guide to Enterprise Patch Management                                |
| ISO/IEC 27031               | ICT readiness for business continuity                               |

## V-08 Does the entity participate in coordinated vulnerability disclosure (CVD) and information-sharing arrangements (CSIRTs, MISP, sectoral ISACs)?

**Tier: High** · *Mandatory at High criticality procurements only.*

### Rationale

Vulnerability-handling maturity at the regional level requires coordinated disclosure rather than one-off bilateral exchanges. NIS2 introduces a coordinated-vulnerability-disclosure regime with national CSIRTs; ENISA's GP §3.3 calls for information sharing as part of supplier relationship management; the LAC4 community of practice provides the forum for the region.

### Examples and further information

Operational mechanisms: integrate with the national CSIRT's CVD scheme; subscribe to relevant ISAC feeds (e.g., financial, energy, health) and a MISP instance; ensure that suppliers' VDPs (S-09) reference the national CSIRT as one of the disclosure paths; share, on a confidential basis, indicators of compromise observed via supplier products.

### Mapping

| Framework                          | Reference / clause                                      |
|------------------------------------|---------------------------------------------------------|
| NIS2 Directive                     | Art. 12 – Coordinated vulnerability disclosure database |
| ENISA Good Practices (2023)        | Area 3.3 – Information sharing                          |
| ISO/IEC 29147                      | Coordinated vulnerability disclosure                    |
| FIRST.org CSIRT / PSIRT frameworks | Coordination patterns                                   |

## 10.5 Incident Handling

Incidents involving suppliers happen – sometimes from a vulnerability, sometimes from a different attack vector. The objective of this section is to ensure that the entity is not surprised when an incident occurs at or via a supplier – that the supplier notifies in time, that responsibilities are clear, that joint response is rehearsed, and that continuity is preserved.

### I-01 Are incident communication channels with the third party predetermined, including out-of-band fallbacks?

**Tier: Medium** · *Mandatory at Medium and High criticality procurements.*

#### Rationale

In a security incident, fast and reliable communication between both parties is fundamental to resolve the incident. Channels and contacts must be pre-determined, since the general IT-infrastructure may not be available during an incident.

#### Examples and further information

Pre-agree primary and secondary channels (with at least one out-of-band – e.g., phone or signal-based – fallback in case email is impacted); named contacts on each side, with deputies; cadence of situational reports; legal hold and evidence preservation expectations. Document outside the usual IT systems (printed copy, plus Wiki entry).

#### Mapping

| Framework                          | Reference / clause                   |
|------------------------------------|--------------------------------------|
| ISO/IEC 27035                      | Incident response communication      |
| ENISA Good Practices (2023)        | Area 3.3 – Incident handling         |
| FIRST.org PSIRT services framework | Coordination with downstream parties |

### I-02 Is a maximum tolerable failure time (RTO) for the procured service or product determined?

**Tier: Medium** · *Mandatory at Medium and High criticality procurements.*

#### Rationale

Digital services may fail for various reasons. If business operations depend on the service, the entity needs to evaluate how long the service can be unavailable before the impact on operations becomes unbearable.

#### Examples and further information

The RTO depends on financial impact, loss of reputation, physical effects in OT environments, and SLA. Once defined, the RTO drives backup design, exit-plan timing, and continuity arrangements.

### Mapping

| Framework                   | Reference / clause                     |
|-----------------------------|----------------------------------------|
| ISO/IEC 22301               | Business continuity management systems |
| DORA – Reg. (EU) 2024/1774  | Major incident reporting / RTO         |
| ENISA Good Practices (2023) | Area 3.3 – Business continuity         |

### I-03 Is it determined how operations continue without the use of the procured service or product (business continuity plan)?

**Tier: Medium** · Mandatory at Medium and High criticality procurements.

#### Rationale

If a service or product fails for a prolonged period, business operations may not be possible, and the entity is at risk. A business continuity plan (BCP) prevents significant damages.

Insolvency, ransomware, geopolitical disruption – any of these can render the supplier unavailable for an extended period. CISA SCRM Q. 8.3 makes a formal BCP a standalone supplier obligation.

#### Examples and further information

The BCP should describe how the service can be at least temporarily replaced – alternative service with similar capabilities, manual handling of processes, secondary supplier, or in-house fallback. Include data extraction in the BCP.

*ENISA Threat Landscape – illustrative case: Kaseya (July 2021) – managed-service-provider customers were affected for days; entities with a manual fallback for the affected workflow were less impacted.*

### Mapping

| Framework                   | Reference / clause                          |
|-----------------------------|---------------------------------------------|
| NIS2 Directive              | Art. 21(2)(c) – business continuity         |
| DORA – Reg. (EU) 2022/2554  | Operational resilience and exit strategies  |
| ENISA Good Practices (2023) | Area 3.3 – Business continuity              |
| ISO/IEC 22301               | Business continuity management systems      |
| CISA SCRM Template          | Q. 8.3, 8.6, 8.7 – BCP / supplier diversity |

### I-04 Are backup-restore operations tested at regular intervals?

**Tier: Medium** · Mandatory at Medium and High criticality procurements.

#### Rationale

Creating backups regularly is fundamental, but many organisations fail to test whether a backup can actually be restored. The restore procedure should be tested at regular intervals, against a clean environment.

### Examples and further information

Test restoration at least annually for all critical services. Document the time-to-restore, the data integrity, and any deviations. CISA SCRM Q. 4.26 includes back-up media testing as part of the supplier's recovery process.

### Mapping

| Framework          | Reference / clause                           |
|--------------------|----------------------------------------------|
| ISO/IEC 27031      | ICT readiness for business continuity        |
| CIS Controls v8    | Control 11 – Data Recovery                   |
| CISA SCRM Template | Q. 4.26 – Frequency of back-up media testing |

## I-05 Are joint incident-handling playbooks prepared with each critical supplier?

**Tier: High** · *Mandatory at High criticality procurements only.*

### Rationale

Generic incident plans rarely survive contact with a supply-chain incident. A playbook tailored to each critical supplier – naming contacts, escalation paths and key decisions – saves precious hours during the response.

### Examples and further information

Maintain a one-page incident playbook for each critical supplier covering: contacts at the supplier (operational and executive); the supplier's expected actions; the entity's actions (e.g., revoke connectivity, switch to backup); communication to internal stakeholders and regulators. Test the playbook at least annually with the supplier.

### Mapping

| Framework                   | Reference / clause                 |
|-----------------------------|------------------------------------|
| NIS2 Directive              | Art. 21(2)(b) – incident handling  |
| ENISA Good Practices (2023) | Area 3.3 – Joint incident response |
| ISO/IEC 27035               | Incident management                |
| DORA – Reg. (EU) 2024/1774  | Joint testing                      |

## I-06 Is contractual notification of incidents (with NIS2-compatible timelines) defined?

**Tier: Low** · *Mandatory at all criticality tiers (Low, Medium, High).*

### Rationale

When the entity is itself an essential or important entity under NIS2 – or under a national equivalent – it has tight notification timelines (24-hour early warning, 72-hour notification, 1-month final report). Suppliers must notify the entity in time for it to comply.

### Examples and further information

The contract should require the supplier to notify the entity without undue delay and in any case within a defined number of hours after detection, and to provide updates as the response progresses. The notification format should be agreed in advance.

### Mapping

| Framework                   | Reference / clause              |
|-----------------------------|---------------------------------|
| NIS2 Directive              | Art. 23 – reporting obligations |
| ENISA Good Practices (2023) | Area 3.3 – Notification         |
| DORA – Reg. (EU) 2024/1774  | Major incident reporting        |

## I-07 Are incident-reporting obligations and contractual penalties / service credits part of the contract?

**Tier: Medium** · *Mandatory at Medium and High criticality procurements.*

### Rationale

Incentives matter. A supplier that bears no contractual consequence for delayed notification or for incidents caused by its own negligence has weaker incentives to invest in prevention.

### Examples and further information

Service credits or contractual penalties should be calibrated to the criticality of the service. They are not a substitute for damages. The contract should also define when an incident is severe enough to trigger a contractual termination right.

### Mapping

| Framework                   | Reference / clause              |
|-----------------------------|---------------------------------|
| DORA – Reg. (EU) 2024/1773  | Termination rights and remedies |
| ISO/IEC 27036-2             | Contractual remedies            |
| ENISA Good Practices (2023) | Area 3.3 – Remedies             |

## I-08 Is there a joint or coordinated post-incident review with the third party, with named corrective actions and deadlines?

**Tier: Medium** · *Mandatory at Medium and High criticality procurements.*

### Rationale

Lessons-learned exercises that include the supplier are far more effective than internal-only reviews. The supplier is often the only party who can explain root cause and the trajectory of the response.

### Examples and further information

Within a defined period after closure of a major incident, hold a joint review covering timeline, root cause, what worked, what did not, and concrete corrective actions on each side, with owners and deadlines. Track corrective actions to closure.

### Mapping

| Framework                   | Reference / clause                 |
|-----------------------------|------------------------------------|
| ISO/IEC 27035-2             | Lessons learned                    |
| ENISA Good Practices (2023) | Area 3.3 – Continuous improvement  |
| NIS2 Directive              | Art. 23 – final report             |
| CISA SCRM Template          | Q. 3.17 – Vulnerability root cause |

## 10.6 Decommissioning / End of Use

End of contract is a high-risk moment. The entity must be able to take its data with it, leave behind no residual access, prevent the supplier from retaining or reusing entity data, and maintain confidentiality of information shared during the relationship.

### D-01 Is a decommission plan prepared in advance, including timing, transition period and named responsibilities?

**Tier: Medium** · Mandatory at Medium and High criticality procurements.

#### Rationale

When a product or service is taken out of use without considering all effects, business operations may be affected. A detailed plan for the transition prevents surprises.

#### Examples and further information

The decommission plan should at least include when the contract will be terminated; when the product or service will no longer be available for productive use; when users will be informed; how long the transition period will last; who is responsible for each step; and what data needs to be exported.

### Mapping

| Framework                   | Reference / clause                                   |
|-----------------------------|------------------------------------------------------|
| ENISA Good Practices (2023) | Area 3.3 – Manage suppliers over the whole lifecycle |
| DORA – Reg. (EU) 2022/2554  | Exit strategies                                      |
| ISO/IEC 27036-2             | End of relationship                                  |

### D-02 Are all relevant stakeholders involved in the decommissioning?

**Tier: Medium** · Mandatory at Medium and High criticality procurements.

#### Rationale

Like the implementation of a new service, decommissioning may affect various parties. Insights may be missed if certain stakeholders are not consulted. All affected stakeholders should participate in the decommission phase.

#### Examples and further information

Stakeholders depend on the context – the same list as for procurement (P-05) generally applies.

- IT personnel and operations
- Cybersecurity officers / CISO
- Employees (or their representatives)
- Customers and citizens (where applicable)
- Existing suppliers or vendors that depend on the system
- Authorities
- Partner entities
- Legal counsel

### Mapping

| Framework                   | Reference / clause   |
|-----------------------------|----------------------|
| ISO/IEC 27036-2             | End of relationship  |
| ENISA Good Practices (2023) | Area 3.3 – Lifecycle |

### D-03 Are all data that need to be archived or used in the future exported before access is lost?

**Tier: Low** · Mandatory at all criticality tiers (Low, Medium, High).

#### Rationale

After a service is no longer used, the data processed and stored by it usually become inaccessible. Data must be exported before access is lost. The import to a new service may take time and that time must be planned in.

#### Examples and further information

Use the export format agreed under S-10 (data portability). Validate completeness and integrity of the export. Document the chain of custody from supplier to entity (or to the successor supplier).

### Mapping

| Framework                             | Reference / clause    |
|---------------------------------------|-----------------------|
| ENISA Cloud Computing Risk Assessment | Lock-in / exit        |
| EU Data Act – Reg. (EU) 2023/2854     | Switching obligations |
| DORA – Reg. (EU) 2022/2554            | Exit strategies       |
| ISO/IEC 27036-2                       | End of relationship   |

### D-04 Is all confidential data deleted from third-party servers, with verifiable attestation?

**Tier: Low** · Mandatory at all criticality tiers (Low, Medium, High).

#### Rationale

If a service processes and stores data on third-party servers, that information may still be on third-party systems after a contract is terminated. The decommission

process should include verifiable steps to delete all data on third-party systems, including in backups.

Data to be deleted may also be defined in external requirements, contracts and laws.

### *Examples and further information*

Require the supplier to provide a written attestation specifying the systems, the method (cryptographic erasure, secure deletion, physical destruction) and the date. The entity should retain a right to verify or to commission an independent verification. Address backups explicitly, including the timeline for data to leave the backup chain.

### *Mapping*

| Framework       | Reference / clause                              |
|-----------------|-------------------------------------------------|
| NIST SP 800-88  | Guidelines for media sanitisation               |
| ISO/IEC 27036-2 | End of relationship – data return / destruction |
| ISO/IEC 27040   | Storage security                                |

## **D-05 Are all installations of the product and all accounts to the service deactivated at end of contract?**

**Tier: Low** · *Mandatory at all criticality tiers (Low, Medium, High).*

### *Rationale*

After the contract for the product or service ends, installations usually stop receiving security updates and licensing agreements often prohibit continued use. All accounts and installations should be disabled by administrators.

### *Examples and further information*

Maintain a checklist that ties accounts and installations to the contract. Confirm deactivation, retain logs.

### *Mapping*

| Framework                   | Reference / clause   |
|-----------------------------|----------------------|
| ISO/IEC 27036-2             | End of relationship  |
| ENISA Good Practices (2023) | Area 3.3 – Lifecycle |
| CISA SCRM Template          | Q. 6.6 – Offboarding |

## **D-06 Are NDA / confidentiality obligations maintained beyond contract end?**

**Tier: Low** · *Mandatory at all criticality tiers (Low, Medium, High).*

### *Rationale*

Information shared during the contract – architecture, vulnerabilities, incident history, business processes – remains sensitive long after the contract ends. NDA obligations of standard duration (typically 3-5 years post-contract) should be agreed at signature.

### Examples and further information

The contract should specify the duration of confidentiality obligations after termination, list the categories of information covered, and define the consequences of breach.

### Mapping

| Framework          | Reference / clause                                         |
|--------------------|------------------------------------------------------------|
| ISO/IEC 27036-2    | Confidentiality and information protection                 |
| ISO/IEC 27001:2022 | Annex A.6.6 – Confidentiality or non-disclosure agreements |

## D-07 Is hardware sanitisation / disposal at end of life addressed (where hardware is procured)?

**Tier: High** · *Mandatory at High criticality procurements only.*

### Rationale

Hardware that leaves the entity's control may carry residual data. The supplier of the hardware (or a disposal supplier) should sanitise media to recognised standards before disposal, and the chain of custody should be documented.

### Examples and further information

Require evidence of sanitisation per NIST SP 800-88 or equivalent. For end-of-life hardware sent to a disposal supplier, require a chain-of-custody document and a destruction certificate. Where the hardware was leased, ensure the lessor cannot return it to the market without sanitisation.

### Mapping

| Framework                   | Reference / clause                |
|-----------------------------|-----------------------------------|
| NIST SP 800-88              | Guidelines for media sanitisation |
| ISO/IEC 27040               | Storage security                  |
| ENISA Good Practices (2023) | Area 3.5 – Hardware lifecycle     |
| CISA SCRM Template          | Q. 7.11 – Reuse / recycle         |

## 11. Definitions

Throughout this document the following terms are used.

**Entity:** User of this guideline. The organisation that procures services or products from third parties and is responsible for managing the supply-chain risk.

**Supplier / third party:** Any organisation that provides a service or product used by the entity, including software vendors, hardware manufacturers, cloud providers, managed service providers (MSPs), managed security service providers (MSSPs) and consultancies.

**Sub-processor / fourth party:** An organisation engaged by a supplier of the entity to deliver part of the contracted service or product. From the entity's perspective these are indirect suppliers.

**Procurement lifecycle:** The full sequence from needs identification, market analysis, vendor pre-qualification, tendering, contracting, delivery, operation, monitoring and decommissioning.

**Procurement criticality tier:** Low / Medium / High classification assigned to a procurement based on the sensitivity of the data processed, the impact of unavailability, and the regulatory regime. Drives which questions in the Vendor Questionnaire are mandatory.

**Critical service or product:** A service or product whose failure or compromise would have a significant impact on the entity's mission or on the public.

**SBOM:** Software Bill of Materials: a formal, machine-readable inventory of the components that make up a software product (CycloneDX or SPDX).

**VDP:** Vulnerability Disclosure Policy: a public policy describing how researchers may responsibly report vulnerabilities to the supplier and how the supplier handles them.

**PSIRT:** Product Security Incident Response Team: the supplier function responsible for receiving, triaging, remediating and communicating product vulnerabilities.

**CVD:** Coordinated Vulnerability Disclosure: a process by which a vulnerability is disclosed to multiple parties in a coordinated manner – typically the supplier, a national CSIRT and ultimately the public.

**SDL / SSDF:** Secure Development Lifecycle / Secure Software Development Framework: a structured process by which security activities are integrated into each stage of software development. NIST SP 800-218 (SSDF) is a leading reference.

**ISMS:** Information Security Management System: a systematic framework for managing information security risks (e.g., ISO/IEC 27001).

**Supply-chain attack:** Per ENISA: a combination of at least two attacks – one on a supplier and one used to attack the customer through that supplier.

**NIS2:** Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union.

**CRA:** Regulation (EU) 2024/2847, the EU Cyber Resilience Act, on horizontal cybersecurity requirements for products with digital elements.

**DORA:** Regulation (EU) 2022/2554 on digital operational resilience for the financial sector.

**ENISA:** European Union Agency for Cybersecurity.

## 12. Annex A – Cybersecure Supply Chain Standards

This annex consolidates the standards that suppliers should meet across the lifecycle. Each standard is summarised, and entities can reference them directly in tender documents or contract clauses.

### A.1 Software Bill of Materials (SBOM)

- Required: every software / digital-service procurement.
- Format: machine-readable; CycloneDX or SPDX accepted; depth: at least one level beyond first-party code.
- Cadence: at acceptance and on every major release.
- Reference: EU CRA Annex I Part II, NTIA / CISA SBOM Minimum Elements.

### A.2 Vulnerability Disclosure Policies (VDP)

- Required: every supplier of products / digital services.
- Content: public point of contact, acknowledgement timeline, triage and disclosure process.
- Reference: ISO/IEC 29147, ISO/IEC 30111, EU CRA Art. 13-14.

### A.3 Security Certification and Assurance Levels

- Risk-tier mapping: low risk → ISO/IEC 27001 or equivalent; medium → ISO/IEC 27001 + product-level conformity (CRA Annex I); high → EUCC / EUCS / sector-specific schemes.
- Validation: certificate, scope, expiry, accrediting body, recent audit report.
- Reference: EU Cybersecurity Act (Reg. (EU) 2019/881); EUCC (Reg. (EU) 2024/482); EUCS (in adoption).

### A.4 Secure Development Lifecycle (SDL) and Build-pipeline Integrity

- Documented secure coding standards.
- Threat modelling for every release containing material change.
- Mandatory peer review and security testing (SAST, DAST, dependency scanning, fuzzing).
- Code-signing of releases; reproducible builds; restricted access to build infrastructure; build-pipeline auditing.
- Optional alignment with Google SLSA (Supply chain Levels for Software Artifacts).
- Security training of developers; periodic re-training.
- Reference: NIST SSDF (SP 800-218), ISO/IEC 27034, EU CRA Annex I, CISA SCRM Template Q. 3.6, 3.7, 3.10, 3.13.

## A.5 Vulnerability Handling – Supplier and Entity

- Supplier-side: PSIRT-equivalent function; formal vulnerability and weakness analysis on every release; root-cause analysis fed back into the SDL; CVSS-based risk-tiered maintenance policy; proactive customer notification cadence.
- Entity-side: internal vulnerability-management programme; continuous SBOM monitoring against new disclosures; patch testing and rollback procedures; participation in national CSIRT and CVD arrangements.
- Reference: ENISA Good Practices Area 3.4, CISA SCRM §3.14-3.17 and §4.14-4.23, ISO/IEC 29147 / 30111, NIST SP 800-40 Rev. 4, NIS2 Art. 12.

## A.6 Hardware Integrity (where hardware is procured)

- OEM-or-authorised-reseller-only sourcing for key components.
- Tamper-evident packaging and chain-of-custody documentation in transit.
- Counterfeit-prevention processes at the supplier.
- Sanitisation per NIST SP 800-88 at end of life.
- Reference: CISA SCRM Template Q. 2.6, 2.7, 5.8-5.10, 7.11.

## A.7 Incident Reporting and Contractual Penalties

- Notification timeline aligned with NIS2 obligations of the entity.
- Pre-agreed communication channels (primary and out-of-band).
- Service credits / penalties calibrated to criticality.
- Right to terminate for serial or severe non-compliance.
- Reference: NIS2 Art. 23, DORA Reg. (EU) 2024/1774.

## 13. Annex B – How-to: Minimal Supplier Risk Assessment

This annex provides a minimal, six-step methodology that procurement and security teams can use without prior expertise in formal risk-management frameworks. It is not a replacement for ISO/IEC 27005 or NIST SP 800-30 for entities that already operate one of these – it is a starting point.

### B.1 Step 1 – Characterise the Procurement

What service or product is being procured? What data does it process? What is the highest classification? What is the maximum tolerable downtime? Maximum tolerable data loss? Which other systems does it depend on? Which entity processes / services depend on it? Use the answers to assign a procurement criticality tier (Low / Medium / High) that will drive which questions are mandatory.

### B.2 Step 2 – Identify the Supplier and the Supply-chain Depth

Who is the contracting party? Who is the operating party? Where is the supplier headquartered? Where does it operate the service? Which sub-processors are involved? Are any of them critical for the service?

### B.3 Step 3 – Identify the Threat Scenarios (use the ENISA taxonomy)

ENISA's Threat Landscape (2021) classifies attacks by: attack technique on supplier, supplier asset targeted, attack technique on customer, customer asset targeted. Use this taxonomy to characterise scenarios specific to the procurement.

### B.4 Step 4 – Estimate Likelihood and impact

A 3x3 matrix (Low / Medium / High on each axis) is sufficient at this level. For each scenario, document the assumed likelihood and the assumed impact in a one-line note that explains the reasoning.

### B.5 Step 5 – Identify and Tier the Controls

Map the in-scope recommendations from this document to the scenarios. For each scenario, note which recommendations mitigate it and at what level (prevent / detect / respond / recover).

### B.6 Step 6 – Decide and Document

For each residual risk, document one of: accept (with named risk owner), transfer (e.g., contractual remedies, insurance), mitigate (with named actions and deadlines), or avoid (do not procure the service from this supplier). The decision and the underlying reasoning should be visible to the procurement governance group.

## B.7 Example Threats from the ENISA Threat Landscape

- SolarWinds Orion (Dec 2020) – supplier code modified during build process; ~18,000 customers received the malicious update.
- Mimecast (Jan 2021) – compromised supplier certificate used to authenticate to customers' Microsoft 365 tenants.
- Codecov (Apr 2021) – credentials stolen from a Docker image used to modify the customer-facing bash script.
- Verkada (Mar 2021) – credentials found online (OSINT) gave attackers access to 150,000 customer cameras.
- Kaseya VSA (Jul 2021) – zero-day used to push ransomware via the supplier's update channel.

## B.8 Example Mitigations from These Guidelines

- S-08 (SDL) and S-18 (build-pipeline integrity) mitigate the SolarWinds / Codecov pattern.
- S-13 (personnel screening) and O-09 (named accounts, MFA, JIT for supplier staff) mitigate the Verkada pattern.
- V-04 (CVSS-based maintenance policy) + V-06 (entity-side VM with SBOM monitoring) + O-11 (patching SLA) mitigate the Log4Shell-style cascading vulnerability.
- S-14 (sub-processor control) and S-15 (change of control / location) mitigate the sub-processor change pattern.
- S-10 (data portability) and D-01-D-04 (decommissioning) mitigate vendor-lock-in and data-loss patterns.

## 14. References

- Directive (EU) 2022/2555 (NIS2)
- Regulation (EU) 2024/2847 (Cyber Resilience Act)
- Regulation (EU) 2019/881 (Cybersecurity Act)
- Regulation (EU) 2022/2554 (DORA)
- Commission Delegated Regulation (EU) 2024/1773 (RTS on ICT third-party policy)
- Commission Delegated Regulation (EU) 2024/1774 (RTS on ICT risk management)
- Commission Delegated Regulation (EU) 2025/532 (RTS on subcontracting)
- Commission Implementing Regulation (EU) 2024/482 (EUCC scheme)
- Commission Implementing Regulation (EU) 2024/2690 – and ENISA Technical Implementation Guidance
- Regulation (EU) 2023/2854 (Data Act)
- ENISA – Good Practices for Supply Chain Cybersecurity (June 2023)
- ENISA – Threat Landscape for Supply Chain Attacks (July 2021)
- ENISA – Cloud Computing Risk Assessment
- EU ICT Supply Chain Security Toolbox
- ISO/IEC 27001:2022 – Information security management systems
- ISO/IEC 27036 – Information security for supplier relationships (multi-part)
- ISO/IEC 27005 – Information security risk management
- ISO/IEC 27035 – Incident management (multi-part)
- ISO/IEC 27040 – Storage security
- ISO/IEC 27034 – Application security
- ISO/IEC 22301 – Business continuity management systems
- ISO/IEC 19086 – Cloud SLA framework
- ISO/IEC 19941 / 22123 – Cloud interoperability and portability
- ISO/IEC 29147 – Vulnerability disclosure
- ISO/IEC 30111 – Vulnerability handling processes
- NIST SP 800-161 Rev. 1 – Cybersecurity Supply Chain Risk Management Practices
- NIST SP 800-218 – Secure Software Development Framework (SSDF)
- NIST SP 800-30 – Guide for Conducting Risk Assessments
- NIST SP 800-40 Rev. 4 – Guide to Enterprise Patch Management
- NIST SP 800-88 – Guidelines for Media Sanitisation
- NIST SP 800-207 – Zero Trust Architecture

- CIS Controls v8 and CIS Benchmarks
- CISA / ICT SCRM Task Force – Vendor SCRM Template (April 2021)
- CISA / NTIA – SBOM Minimum Elements
- FIRST.org – PSIRT Services Framework
- FIRST.org – CVSS (Common Vulnerability Scoring System)
- Google – SLSA (Supply chain Levels for Software Artifacts)
- MITRE – ATT&CK® and D3FEND
- Inter-American Development Bank / OAS – 2025 Cybersecurity Report (LAC)
- National Cyber Security Index (NCSI) – e-Governance Academy