Digital Services

Cyber-Supply Chain Risk Management (SCRM) Framework

Contents

1. Document Control

Title	Cyber-Supply Chain Risk Management (C-SCRM) Framework
Version	1.0
Creation date	October 2025
Document live date	November 2025
Document owner	Head of Cyber & Information Security
Stakeholders consulted in development	Digital Services Data Privacy Finance Procurement Legal Team Information Assurance Committee (IAC)
For information & action	All staff and authorised affiliates of BUL systems
Supersedes	BUL-POL-15 Supply chain security Principles v1.0
Supporting policies	Supply Chain and Supplier Security Risk Management Policy Brunel University of London Procurement Policy Procurement Card (PCARD) Policy & Procedures

2. Purpose and Background

The purpose of this framework is to establish a structured, collaborative, and risk-informed approach to identifying, assessing, mitigating, and monitoring cyber and information security and resilience related risks arising from third-party suppliers, vendors, and service

providers engaged across Brunel University of London's (BUoL) operational, research, and academic environments.

Universities operate within complex ecosystems involving multiple external suppliers, from IT vendors and SaaS platforms, cloud service providers to research and outsourced partners. This framework ensures that security, privacy, compliance, and operational risks are managed holistically across the entire supply chain lifecycle, embedding controls from procurement to onboarding and through vendor offboarding.

2.1 Objectives

- To understand BUoL's vendor relationship tiering as much as possible (direct vendors (tier 1), direct vendors' sub-contractors (tier 2), etc.).
- To protect BUoL's data, systems, and reputation from supply chain risks.
- To embed cyber supply chain risk management practices into procurement and contract processes.
- To enable informed decision-making based on security, privacy, and operational risk ratings.
- To ensure compliance with relevant standards and regulations (GDPR, DPA 2018, NIST CSF, NIS2, etc.).
- To strengthen collaboration between Procurement, Finance, Legal, Digital Services, Cyber & Infosec, Privacy functions, and others.

The following BUoL policies should be referenced in conjunction with this Framework

- Supply Chain and Supplier Security Risk Management Policy
- Brunel University of London Procurement Policy
- Supply Chain Code of Conduct

2.2 Scope

This framework applies to:

- All BUoL staff, and authorised affiliates engaged in procurement or supplier management on behalf of the University.

- All types of system application and software, IT hardware, IT vendors, cloud providers, and all such vendors and third-party services that could impact BUoL's information systems and data's confidentiality, integrity and availability.
- All engagements involving software or hardware procurement, data sharing, SaaS/PaaS/IaaS services, research collaboration platforms, or outsourced operations.
- All business units, colleges, and departments within BUoL.

2.3 Risk Appetite

2.3.1 Mandate

All new and renewal suppliers, service providers, and vendors that would impact BUoL's data and systems must go through a risk review before onboarding. This review will help the University determine:

- The level of risk the third party may pose to its data, systems, or operations;
- The type and depth of assessment required (for example, basic screening or full security and privacy assessment); and
- The appropriate level of ongoing monitoring throughout the relationship.

No new or renewed engagement should proceed without completing this review and obtaining the necessary approvals.

2.3.2 Risk Tolerance

BUoL adopts a low tolerance for risks that directly impact personal data, sensitive organisational data and critical operational, academic and research systems.

3. Governance Structure

Stakeholder / Function	Core Responsibility in Supply Chain Risk Management
Procurement	Central coordination of supplier tendering, financial due diligence, conflict of interest declaration, and overall compliance with the Procurement policy.
CAB Finance / Finance Department	Reviewing and approving all significant financial expenditures related to new procurement activities. Evaluating proposed procurement spend, assessing financial justifications, authorising expenditure thresholds.
Legal Services / Contracts Office	Reviews and negotiates data protection, confidentiality, and liability clauses; ensures inclusion of standard security terms, breach notification clauses, data-processing agreements (DPAs), and right-to-audit provisions.
CAB-Digital Services	Reviews and approves changes related to the deployment, configuration, or integration of third-party systems and services within the University's IT environment, ensuring they are properly risk-assessed, tested, and scheduled to prevent disruption to business or academic operations.
Digital Services (Software Request Unit)	Validates technical integration, compatibility, and architecture implications. Ensures compliance with IT standards (e.g., SSO, MFA, patching, hosting location, and secure configuration) and other agreed risk mitigations arising from risk assessment.
Digital Services	Ensures secure deployment, enforcement of technical control, access permissions, and secure integration of vendor systems within the University's infrastructure.
Cyber & Information Security Team	Leads security due diligence, vendor risk assessment, and supply-chain threat analysis. Maintains Vendor Risk Register and issues vendor risk ratings.
Head of Privacy / Data Privacy	Reviews processing of personal or special category data, data transfer mechanisms, DPIAs, and UKGDPR/DPA 2018 compliance. Approves or rejects vendors from a data privacy and protection standpoint.

Stakeholder / Function	Core Responsibility in Supply Chain Risk Management
Research & Colleges	Identify academic/teaching or research-specific suppliers, ensure ethical and data-sharing compliance, and work with IT/Cyber teams to evaluate software/platform risks.
Business / Service Owner	Initiates software or service requests, provides business justification, and ensures ongoing compliance with contractual and risk requirements.

4. Supply Chain Risk Management Lifecycle

BUoL's SCRM process follows a seven-stage lifecycle integrating procurement, security, and governance checkpoints.

Stage 1: Supplier Identification

- The business or academic unit identifies a need for a new supplier, vendor, software, hardware, or service.

Stage 2: Pre-Assessment & Risk Rating (Cyber & Infosec/Data Privacy)

- Procurement and Digital Services - Software Request conducts initial triage to determine if supplier is new or existing and if there are suitable alternatives or not.
- Cyber & Infosec and Data Privacy performs a pre-assessment using a quick-screening checklist covering among others:
    - Data sensitivity and hosting model (cloud/on-prem)
    - System integration or API access
    - Regulatory exposure (e.g., GDPR, PCI, research data obligations)
    - Supplier geography and data transfer risk
- Vendors are rated Low-risk/Non-critical, Moderate-risk/Important, or High-risk/Critical.
- Low-risk vendors may proceed directly to approval with baseline security clauses.
- Moderate and High-risk vendors proceed to full risk assessment.

- High-risk vendors undergo a cyber kill chain threat assessment as part of full risk assessment.
- See Appendix A for risk rating criteria

Stage 3: Full Risk Assessment (Cyber & Infosec, Data Privacy)

For Moderate and High-Risk Suppliers:

- **Cyber & Infosec** conducts a comprehensive security risk assessment including:
    - Security questionnaire (aligned with NIST CSF, ISO 27001).
    - Review of responses to questionnaire, supplier's sub-processors, controls, certifications, security policies, third-party audit reports
    - Conducts a risk assessment including a threat analysis based on Cyber Kill Chain for high-risk suppliers.
- **Data Privacy** reviews personal data handling, data flows, retention, and cross-border transfer mechanisms; initiates Data Protection Impact Assessment (DPIA) if needed.

Stage 4: Risk Mitigation and Approval

- Identified gaps are communicated to the vendor for remediation or compensating controls.
- **Cyber & Infosec** and Data Privacy confirms closure or acceptance of residual risks.
- **Head of Information Security and Head of Privacy** (or delegates) formally approves risk acceptance for unresolved medium/high risks.
- **Digital Services - Software Request** validate technical and architectural controls (SSO, MFA, encryption, API security, etc.). Coordinates all feedback and ensures approvals before purchase order issuance.
- Engagement can only proceed once **all sign-offs** (Cyber, Privacy, Legal, Finance, Procurement, Digital Services) are documented.

Stage 5: Finance Expensing, Contracting and Onboarding

- **Finance (CAB Finance)** provides financial approval based on final vendor risk and cost implications.

- **Legal Services** finalises and ensures inclusion of key clauses: Information Security Addendum, Data Protection Agreement (DPA) when necessary, breach notification clauses, Service Level Agreements (SLAs) with incident response expectations, audit rights, and termination and exit provisions
- **CAB-Digital Services r**eviews and approves/decline changes related to the deployment, configuration, or integration of third-party systems and services within the University's IT environment, providing assurance that technical and architectural controls are in place prior to go-live.
- **Procurement** in addition to agreeing and establishing SLAs, commercial terms, ensures performance metrics are in place, enables vendor registration, PO issuance, and entry into the Preferred Supplier List (PSL).
- **Cyber & Infosec** updates the Vendor Risk Register and establishes review frequency based on criticality.
- **Data Privacy** updates Information Asset Register.
- **Sponsor** initiates the Supplier Set-Up (SSU) and raises a requisition.

Stage 6: Continuous Monitoring & Performance Review

- **Cyber & Infosec** monitors vendor security posture through:
    - Periodic reviews (see Appendix B)
    - Threat intelligence feeds and supply-chain alerts
    - Public breach or compromise notifications
    - Vulnerability scanning and patch status (for integrated systems)
- **Data Privacy** ensures continued GDPR compliance, especially for cross-border transfers or data processing changes.
- **Procurement** and **Finance** track contractual and financial compliance.
- **Business owners** provide ongoing performance feedback.

Stage 7: Offboarding and Exit Management

- When a vendor relationship ends:
    - **IT and Cyber teams** ensure all accounts, credentials, and integrations are decommissioned.

    - **Data Privacy** confirms data return or secure deletion.
    - **Contract Manager (often Stakeholder) contacts Procurement** who updates the ERP System and flags vendor status as “inactive.”
    - **Business owner** verifies transition to new supplier, if applicable.
- Lessons learned are captured to inform future supplier evaluations.

5. Exemptions

Where it is not possible to apply or enforce any part of this framework, then a request detailing the reason(s) why it is not possible must be raised with the Head of Information Security, who will review the business justification and advise on the associated risks. Exceptions will only be issued when the relevant Business Service Owner has signed off on the identified risks or provided compensating controls are documented and approved.

6. Integration with the Cyber Kill Chain

The BUoL’s SCRM process incorporates threat-informed defence principles.
During vendor assessment and continuous monitoring, potential adversarial behaviours are mapped across:

- **Reconnaissance:** OSINT exposure via supplier websites or repositories.
- **Weaponization & Delivery:** Compromise of software dependencies or update mechanisms.
- **Exploitation & Installation:** Unpatched vulnerabilities or misconfigured integrations.
- **Command & Control:** Unauthorized remote management or API misuse.
- **Actions on Objectives:** Data exfiltration or research data theft.

This mapping informs control priorities, red-team exercises, and early-warning indicators.

7. Reporting and Metrics

Quarterly reports shall be presented to the **Audit and Risk Committee** including:

- Number of vendors onboarded and assessed.
- Distribution by risk rating (Low/Non-Critical, Medium/Important, High/Critical).

- Open and closed risk mitigation actions for High-risk vendors.
- Incidents or breaches involving third party suppliers.

8. Continuous Improvement

- The framework shall be reviewed annually by the Head of Information Security in collaboration with Procurement and Digital Services-Software Request.
- Lessons from incidents, audits, or sector guidance (UCISA, Jisc, NCSC) will inform updates.
- Staff awareness sessions shall be conducted to reinforce the importance of supply chain risk management.

Appendix A – Vendor Pre-Assessment Screening and Risk Rating Criteria

The Pre-Assessment Screening Checklist used during Stage 2: Pre-Assessment (Cyber & Infosec/Privacy) evaluates each prospective or renewing vendor across several key dimensions. The outcome of the screening determines the initial vendor risk rating (Low/Non-critical, Moderate/Important, or High/Critical), which defines the level of due diligence and ongoing monitoring required.

A.1 Screening Dimensions

Each vendor is screened using a short questionnaire or checklist covering, at minimum, the following areas:

1. Data Sensitivity – Does the vendor process, store, or transmit University or personal data?
2. System Connectivity – Will the vendor's system integrate with, or have network access to, University systems?
3. Service Criticality – Would an outage or compromise materially affect teaching, research, or operations?
4. Regulatory / Compliance Impact – Is the service subject to GDPR, PCI DSS, export controls, or other statutory obligations?
5. Geographic & Hosting Factors – Where is data hosted or processed, and are there cross-border transfers?
6. Security & Privacy Maturity – Does the vendor hold relevant certifications (e.g., ISO 27001, SOC 2, Cyber Essentials Plus)?

7. AI / Open-Source or Emerging Tech Components – Does the product involve AI models, open-source libraries, or third-party code dependencies?

A.2 Scoring Method

Each checklist item is scored as follows:

Flag Status	Description	Indicative Score
No Flag (0)	No concern identified; control or requirement fully met.	0 points
Minor Flag (1)	Low-impact gap or uncertainty; easily mitigated.	1 point
Moderate Flag (2)	Medium-impact gap requiring validation or compensating control.	2 points
Significant Flag (3)	High-impact issue requiring full risk assessment and mitigation plan.	3 points

The total score determines the vendor's Pre-Assessment Risk Rating.

A.3 Risk Rating Matrix

Total Score / Flags Identified	Risk Rating	Interpretation & Next Action
0 – 1 flag	Low Risk	No material issues. Proceed with baseline security clauses and record in the Approved Vendor Register.
2 – 4 flags	Moderate Risk	Potential exposure identified. Conduct a Full Risk Assessment (security + privacy review) before approval.
5 – 7 flags	High Risk	Significant data, system, or compliance risk. Require detailed assessment, remediation plan, and Head of Infosec/DPO sign-off prior to engagement.
8 or more flags / Critical issue detected	Unacceptable Risk	Engagement paused pending executive review. Vendor may be rejected or required to demonstrate substantial control improvements.

Appendix B – Periodic Review Frequency Based on Vendor Risk Rating

This appendix formalises the periodic review schedule outlined under Stage 6: Continuous Monitoring & Performance Review.

The frequency and depth of reviews are determined by the vendor's risk rating, ensuring that monitoring efforts are proportionate to the potential impact of vendor failure, compromise, or non-compliance.

B.1 Review Frequency and Scope

Vendor Risk Rating	Description	Review Frequency
Low / Non-critical	Vendors with minimal operational impact or processing of public/non-sensitive data.	**Ad-hoc reassessments upon material change** (e.g., service update, new data/system access), incident, audit finding, or threat intelligence, etc.
Moderate / Important	Vendors supporting important but not mission-critical functions or processing moderate-sensitivity data.	**Every 24 months or more frequently if triggered by a material change** (e.g., service update, new data/system access), incident, audit finding, or threat intelligence, etc.
High / Critical	Vendors providing mission-critical services or handling highly sensitive/confidential/regulated data.	**Every 12 months, or more frequently if triggered by a material change** (e.g., service update, new data/system access), incident, audit finding, or threat intelligence, etc.

B.2 Trigger-Based (Ad-hoc) Reviews

In addition to scheduled reviews, ad-hoc reassessments must be initiated when any of the following occur:

- A security incident, breach, or data-protection violation involving the vendor.
- Material changes to the vendor's ownership, infrastructure, or service delivery model.
- Introduction of new data categories, system integrations, or APIs.
- Significant change in regulatory or compliance requirements.