

Supply Chain Management Process

Management of Information Security within Supply Chain relationships at BITS Technology Group

Table of Contents

| | |
|--|----------|
| <i>Supply Chain Management Process</i> | 1 |
| <i>Purpose</i> | 3 |
| <i>Scope</i> | 3 |
| <i>Initial Supplier Assessment</i> | 4 |
| Criticality Assessment | 4 |
| Risk Assessment | 5 |
| <i>Data Governance</i> | 6 |
| Data Types & Classification | 6 |
| Data Storage Locations | 6 |
| <i>Supply Chain agreements and terms management</i> | 7 |
| <i>Supplier Review & Monitoring</i> | 8 |
| Periodic reviews | 8 |
| Automatic Monitoring | 8 |
| <i>Policy Compliance</i> | 9 |
| <i>Review and Maintenance</i> | 9 |
| Document Control..... | 9 |
| Revision History..... | 10 |

Purpose

This policy establishes the criteria and process for vetting, onboarding, and ongoing management of suppliers to ensure compliance with information security requirements. It aims to mitigate risks related to information security, confidentiality, privacy, and notifiable data breaches while aligning with ISO/IEC 27001:2022 and other applicable global standards.

Scope

This policy applies to all suppliers, vendors, contractors, SaaS, Software providers and third-party service providers who interact with, manage, or access the organisation's information systems, data, and supply chain resources.

It covers all aspects of the supplier lifecycle, from onboarding, ongoing management, offboarding and review.

Initial Supplier Assessment

Criticality Assessment

A structured approach will be applied to evaluate suppliers based on their criticality to business operations and potential associated risks.

To determine the supplier's impact on business continuity, operations, and regulatory obligations, the following factors will be used to determining the criticality:

- **Business Continuity Impact:** The degree to which supplier failure would disrupt essential business operations and/or disrupt incoming revenue generating activities.
- **Regulatory and Compliance Dependency:** The extent to which a supplier helps the organisation meet compliance obligations (e.g., ISO 27001:2022, Privacy Act and any other legal obligations).
- **Supply Chain Dependency:** The level of reliance on the supplier for operational stability and service delivery.
- **Alternative Availability:** The ability to quickly replace or mitigate disruptions caused by supplier failure.
- **Financial and Reputational Impact:** The potential business cost or reputational damage resulting from supplier failure.
- **Data Sensitivity & System Access:** The level of confidential, personal, or business-critical data the supplier will process or access and whether they have access to critical IT infrastructure and network systems.

Suppliers will be categorised into 3 levels of criticality as follows:

- **High - Critical Suppliers**
Essential for core business operations, regulatory compliance, or security posture. These suppliers provide services or products that, if unavailable, would cause significant disruption to operations, financial loss, or regulatory non-compliance. They often have direct access to sensitive company data, infrastructure, or key systems.
- **Medium – Medium Impact Suppliers**
Significant but non-essential contributors to business operations, data handling, or security. These suppliers support key business functions but do not have a direct impact on overall business continuity. If a high-impact supplier experiences failure, there may be disruptions, but alternative solutions may exist.
- **Low - Support Suppliers**
Indirect impact on operations with minimal interaction with critical systems or data. These suppliers provide ancillary services that support business processes

but do not pose a major risk to business continuity or regulatory compliance.

Risk Assessment

Each supplier is evaluated against the following criteria to determine their risk level:

Type of Information handled or accessed:

- Does the supplier store or process BITS Technology Group personal, financial, PII or sensitive business information?
- Is the data regulated (e.g., privacy laws, financial regulations, or industry-specific compliance requirements)?

Data Access & Storage

- Does the supplier have direct or indirect access to the organisation's critical systems?
- Does the supplier have direct or indirect access to the organisation's customers critical systems or data?
- Is the data stored on-premises, in a cloud environment, or processed in offshore locations?
- Are subcontractors or third-party providers involved in data handling?

Compliance & Security Measures

- Does the supplier comply with industry security standards (e.g., ISO 27001, SOC 2, NIST, Australian Privacy Act)?
- Do they implement encryption, access controls, and secure data transfer mechanisms?
- Have they been subject to security breaches or compliance violations in the past?

Business Continuity & Incident Management

- Does the supplier have a robust business continuity and disaster recovery plan?
- Does the supplier have an incident response plan for security incidents or data breaches?
- What contractual obligations exist for reporting security incidents?

Suppliers will be categorised based on the potential impact they may have on BITS Technology Group's security and compliance obligations. The categories are as follows:

- **High Risk**
Suppliers with access to or stores sensitive, confidential, or regulated data, including PII, financial records, or intellectual property.
- **Medium Risk**
Suppliers handling internal or non-critical business data but not personally identifiable information (PII) or regulated data.
- **Low Risk**
Suppliers with no or minimal access to sensitive data and systems.

Data Governance

Data Types & Classification

When evaluating a supplier, it is essential to define what types of data will be shared, accessed, processed, or stored by the supplier. This assessment will consider:

- The Data Types being shared or accessed will also be identified.
- The **classification level** of the data being shared, stored or accessed.

The type of data shared or accessed should align with the Principle of Least Privilege, ensuring that suppliers only receive the minimum data necessary for their service delivery.

Data Storage Locations

The physical and legal location where the supplier systems store data is a key factor in risk assessment. The following will be considered:

- **Data Residency Requirements:**
Is there a requirement or legal obligation through either client contracts or regulatory requirement to store Acme Inc Data within Australia or a set location.
- **Jurisdictional Risks:** If data is stored in a foreign jurisdiction, the supplier must disclose the applicable legal framework, including any government access risks.

Supply Chain agreements and terms management

A foundational element of secure supplier relationships is the formalisation of clearly defined enforceable agreements that address information security, privacy, compliance, and continuity obligations. This section outlines the minimum requirements for contract terms and conditions that must be integrated into all supplier agreements, especially those classified as medium or high risk.

The follow elements will be covered in all agreements

- Confidentiality and Non-Disclosure:
 - Clearly defined confidentiality clauses ensuring the protection of BITS Technology Group's information.
 - Obligate suppliers to protect data during and after contract term.
- Incident or Breach notification:
 - Mandatory notification of security incident and breach notifications.
 - Clearly defined timelines will also be stated.
- Locations of Data Storage:
 - Either the privacy policy or the agreement will state what jurisdictions/locations BITS Technology Group's Data is stored.

The following Elements may be considered for medium and high-risk suppliers:

- Compliance to ISO 27001:2022 Standards and/or SOC2.
Preferably the organisation should retain a current certification.
- Right to Audit
If required, have the ability to audit and inspect the supplier operations. Such areas may include:
 - Business Continuity and Disaster recovery processes.
 - Vulnerability Management processes.
 - Incident Management processes.
 - ISO 27001 audit responses.
 - Use of sub-contractors and the flow-down obligations.
 - Relevant penetration test results.
- Data Encryption standards.
This will include data in transit and data at rest.

Supplier Review & Monitoring

Periodic reviews

To ensure continued compliance and risk mitigation, all suppliers must undergo a regular review assessment.

Review will be conducted annually or can be triggered if there are material changes in services, data handling or regulatory requirements.

A reassessment will also be triggered by:

- Security incidents involving the supplier.
- A data disclosure event.
- Changes in data access or storage locations.
- New regulatory requirements affecting the supplier relationship.

Automatic Monitoring

Where possible the de.iterate platform will automatically display an online security score. This is done by monitoring the attack surface of the vendor using the Upguard platform.

- Vendor Score 650 and above are considered to be in the standard operating range.
- Vendor Scores that drop below 650 but above 400 will be in the watch and observe status.
- Vendor Scores that are below 400 will trigger a re-assessment of the Vendor to ensure the Confidentiality, Integrity and Availability of the supplier is sufficient.

Policy Compliance

Failure to comply with this policy may result in disciplinary action, up to and including termination.

Any security incidents resulting from improper onboarding or offboarding must be reported to the Information Security Officer immediately.

Review and Maintenance

This policy will be reviewed annually or after significant organisational changes. Updates will be approved by the ISMS Committee and communicated to all relevant stakeholders.

Document Control

| DESIGNATED POLICY OWNER | Classification | Publication Date | Next Review Date |
|-------------------------|-----------------------|------------------|------------------|
| CEO | Business Confidential | 25/06/2025 | 25/06/2026 |

Revision History

| Version | Date | By | Summary of Changes |
|---------|-----------|--------------------|--------------------|
| 0.1 | 23/6/2025 | Esther Mangelsdorf | Initial draft |
| 1.0 | 26/6/2025 | Esther Mangelsdorf | Published Copy |