12.7. Supply Chain

Objective

12.7.1. Technology supply chains are established and managed to ensure continuity of supply and protection of sensitive related information.

Context

Scope

12.7.2. The NZISM provides additional guidance for managing supply chain security risks associated with the acquisition (lease or purchase) of ICT equipment or services for use in NZ Government systems.

Supply chain

12.7.3. A supply chain is the movement of materials as they move from their source (raw materials) through manufacture to the end customer. A supply chain can include materials acquisition, purchasing, design, manufacturing, warehousing, transportation, customer service, and supply chain management. It requires people, information and resources to move a product from manufacturer to supplier to customer. Every supply chain carries some risk which may include product protection; counterfeit products and goods and defective products. ICT supply chains are invariably global and complex.

12.7.4. Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (e.g. through supply contracts, interagency agreements, lines of business arrangements, service-level agreements), licensing agreements, and/or supply chain exchanges. The growing use of external service providers and new relationships being established with those providers present new and difficult challenges for organisations, especially in the area of information system security. These challenges include:

- Defining the types of external information system services provided to organisations;
- Describing how those external services are protected; and
- Obtaining the necessary assurances that the risks to organisational operations and assets, individuals, other organisations, and national security arising from the use of the external services are acceptable.

Supply chain risk

12.7.5. The degree of confidence that the risk from using external services is at an acceptable level depends on the assurance external organisations provide and trust that organisations place in external service providers. In some cases, the level of trust is based on the amount of direct control organisations are able to exert on external service providers in the use of security controls and assurance on the effectiveness of those controls.

12.7.6. The level of control is usually established by the terms and conditions of the contracts or service-level agreements with the external service providers and can range from extensive control (e.g., negotiating contracts or agreements that specify detailed security requirements for the providers) to very limited control (e.g., using contracts or service-level agreements to obtain commodity services such as commercial telecommunications services).

12.7.7. From an Information Assurance viewpoint, there are five key aspects to supply chain risk:

1. Protection of sensitive information and systems;
2. Continuity of supply;
3. Product assurance;
4. Security validation; and
5. National Procurement Policy

Protection of sensitive information and systems

12.7.8. This relates to the security of the supply chain, products and information relating to the intended use, purchaser, location and type of equipment.

Continuity of supply

12.7.9. This is the traditional set of risks associated with supply chain. As supply chains have globalised and components are sourced from a number of countries, a disruption to supply may have a global effect.

Product assurance

12.7.10. This relates to assurance that the product, technology or device performs as designed and specified and includes the provenance of the product, equipment, or device.

Security validation

12.7.11. Security validation checks the performance and security of the equipment. The security design elements and features of the equipment or product will need to be separately considered from any operational drivers.

National procurement policy

12.7.12. All agencies are required to follow the guidance of the Government Rules of Procurement. Some exemptions are permitted under Rule 13 including that of security, “essential security interests: Measures necessary for the protection of essential security interests, procurement indispensable for national security or for national defence…”. Care must be taken to follow these rules wherever possible.

References

12.7.13. While NOT an exhaustive list, further information on procurement and supply chain can be found at:

Reference	Title	Publisher	Source
	Government Use of Offshore Information and Communication Technologies (ICT) Service Providers - Advice on Risk Management April 2009	State Services Commission	1135964_1 (otago.ac.nz)
	The new Government Rules of Sourcing	Procurement.govt.NZ	Government Procurement Rules - Rules for sustainable and inclusive procurement Government Procurement Rules | New Zealand Government Procurement and Property
	Government Rules of Sourcing - Rules for planning your procurement, approaching the market and contracting	Ministry of Business Innovation and Employment	Procurement | New Zealand Government Procurement and Property
SP 800-161	**Special Publication, Supply Chain Risk Management**	Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology (NIST)	http://csrc.nist.gov/publications/drafts/800-161/sp800_161_draft.pdf [PDF, 3.1 MB]
SP 800-53 Revision 4	**Special Publication, Security and Privacy Controls for Federal Information Systems and Organizations**	NIST	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf [PDF, 5.1 MB]
NISTIR 7622	**Notional Supply Chain Risk Practices for Federal Information Systems**	NIST	http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf [PDF, 2.9 MB]
	Commercial Procurement & Relationships	UK Cabinet Office	https://www.gov.uk/government/organisations/cabinet-office
	CIO Council Government ICT Offshoring (International Sourcing) Guidance	UK Cabinet Office	https://www.gov.uk/government/publications/government-ict-offshoring-international-sourcing-guidance
	Commonwealth Procurement Rules	Department of Finance and deregulation (Financial Management Group)	Commonwealth Procurement Rules | Department of Finance https://www.finance.gov.au/sites/default/files/2022-06/CPRs 1 July 2022.pdf
ISO 31000:2018	**Risk management – Guidelines**	ISO	https://www.iso.org/standard/65694.html
HB 231:2004	**Information Security Risk Management Guidelines**	Standards NZ	https://standards.govt.nz/shop/hb-2312004/
ISO Guide 73:2009	**Risk management - Vocabulary**	ISO	https://www.iso.org/standard/44651.html
ISO/IEC 31010:2009	**Risk management - Risk assessment techniques**	ISO	https://www.iso.org/standard/51073.html
ISO/IEC 27002:2022	**Information security, cybersecurity and privacy protection — Information security controls**	ISO/IEC	https://www.iso.org/standard/75652.html
ISO/IEC 27005:2012	**Information technology - Security Techniques - Information Security Risk Management**	AS/NZS ISO/IEC	https://standards.govt.nz/shop/asnzs-isoiec-27005:2012/
ISO 28000:2007	**Specification for security management systems for the supply chain**	ISO	https://www.iso.org/standard/44641.html

Rationale & Controls

Risk Management

12.7.14.R.01. **Rationale**

ICT supply chains can introduce particular risks to an agency. In order to manage these risks, in addition to other identified ICT risks, supply chain risks are incorporated into an agency's assessment of risk and the Security Risk Management Plan (SRMP). Identified risks are managed through the procurement process and through technical checks and controls (See Section 5.3 – Security Risk Management Plans and Chapter 4 – System Certification and Accreditation).

12.7.14.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3634]

Agencies SHOULD incorporate the consideration of supply chain risks into an organisation-wide risk assessment and management process.

12.7.14.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3638]

Agencies SHOULD monitor supply chain risks on an ongoing basis and adjust mitigations and controls appropriately.

12.7.14.C.03.

Control System Classifications(s): All Classifications; Compliance: Should [CID:3639]

Agencies SHOULD follow the Government Rules of Procurement.

Contractor or Supplier Capability

12.7.15.R.01. **Rationale**

Agencies can assess the capability of a contractor and any subcontractors to meet their security of information, supply and product requirements.

12.7.15.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3644]

Agencies SHOULD require tenderers and contractors to provide information:

- identifying any restrictions on the disclosure, transfer or use of technology arising out of export controls or security arrangements; and
- demonstrating that their supply chains comply with the security of supply requirements set out in the contract documents.

12.7.15.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3646]

Agencies SHOULD request information from contractors and subcontractors to assess their ability to protect information.

Security of Information

12.7.16.R.01. **Rationale**

After conducting a risk assessment, agencies and suppliers have the means and capability to protect classified information throughout the tendering and contracting process.

12.7.16.C.01. **Control System Classifications(s): Confidential, Top Secret, Secret; Compliance: Must** [CID:3651]

Agencies MUST include contractual obligations on all contractors and subcontractors to safeguard information throughout the tendering and contracting procedure.

12.7.16.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3653]

Agencies SHOULD include contractual obligations to safeguard information throughout the tendering and contracting procedure.

12.7.16.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3654]

Agencies SHOULD reject contractors and subcontractors where they do not possess the necessary reliability to exclude risks to national security; or have breached obligations relating to security of information during a previous contract in circumstances amounting to grave misconduct.

Continuity of Supply

12.7.17.R.01. **Rationale**

You can also require suppliers to provide commitments on the continuity of supply. These can include commitments from the supplier to ensure:

- delivery time;
- stock levels;
- visibility of the supply chain; and
- supply chain resilience.

12.7.17.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3658]

Agencies SHOULD ensure that changes in their supply chain during the performance of the contract will not adversely affect the continuity of supply requirements.

Product Assurance

12.7.18.R.01. **Rationale**

In addition to the product selection and acquisition guidance in this section, agencies are able to identify and mitigate risks through supply chain visibility, provenance, security validation and pre-installation tests and checks.

12.7.18.R.02. **Rationale**

Agencies, with the cooperation of their suppliers, should establish the provenance of any products and equipment. Provenance is defined as a record of the origin, history, specification changes and supply path of the products or equipment.

12.7.18.C.01. **Control System Classifications(s): Secret, Top Secret, Confidential; Compliance: Must** [CID:3669]

Agencies MUST require suppliers and contractors to provide the provenance of any products or equipment.

12.7.18.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3674]

Agencies SHOULD require suppliers and contractors to provide the provenance of any products or equipment.

Security validation

12.7.19.R.01. **Rationale**

Validation of the performance and security of the equipment is a vital part of the ongoing integrity and security of agency systems. The security design elements and features of the equipment or product will need to be separately considered from any operational drivers. Where compromises in security performance, capability or functionality are apparent, additional risk mitigation, controls and countermeasures may be necessary.

12.7.19.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3691]

Agencies SHOULD validate the security of the equipment against security performance, capability and functionality requirements.

12.7.19.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3693]

Where deficiencies in security performance, capability and functionality are identified, agencies SHOULD implement additional risk mitigation measures.

Pre-Installation Tests and Checks

12.7.20.R.01. **Rationale**

An essential part of quality and security assurance is the delivery inspection, pre-installation and functional testing of any equipment. In particular, large systems that integrate equipment from different suppliers or that have specialised configuration and operational characteristics may require additional testing to provide assurance that large scale disruptions and security compromises are avoided.

12.7.20.C.01. **Control System Classifications(s): Confidential, Top Secret, Secret; Compliance: Must** [CID:3698]

Agencies MUST consult with the GCSB on pre-installation, security verification and related tests before the equipment is used in an operational system.

12.7.20.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3700]

Agencies SHOULD inspect equipment on receipt for any obvious signs of tampering, relabelling or damage.

12.7.20.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3701]

Agencies SHOULD inspect equipment on receipt and test the operation before installation.

12.7.20.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3703]

Agencies SHOULD conduct installation verification and related tests before the equipment is used in an operational system.

12.7.20.C.05. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3704]

Where any software, firmware or other forms of programme code are required for the initialisation, operation, servicing or maintenance of the equipment, malware checks SHOULD be conducted before the equipment is installed in an operational system.

Equipment Servicing

12.7.21.R.01. **Rationale**

Some larger or complex systems can have dependencies on particular infrastructures, equipment, software or configurations. Although these types of systems can be less flexible in responding to the rapid changes in technologies, the risks are outweighed by the functionality of the system. In such cases, the continuing support and maintenance of essential components is vital.

12.7.21.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3709]

For equipment that is expected to have an extended operational life in a critical system, and in the event that the supplier is no longer able to supply these, agencies SHOULD provide for the acquisition of:

- necessary licences;
- information to produce spare parts, components, assemblies;

- testing equipment; and
- technical assistance agreements.