Incident Response
FORENSIC & CYBER

Tertiary ICT – August 2023

Service Provider Management

How to respond to a cyber attack on your supply chain

New Zealand National Cyber Security Centre (NCSC)

SUPPLY CHAIN CYBER SECURITY.

IN SAFE HANDS.

NATIONAL CYBER SECURITY CENTRE
A PART OF THE GCSB

New Zealand Government

https://www.ncsc.govt.nz/resources/cyber-resilience-guidance/supply-chain/

What is Supply Chain Cyber Security

Supply Chain Risk Management (SCRM):

A set of activities and practices undertaken by organisations to identify, assess and manage risk in their supply chains.

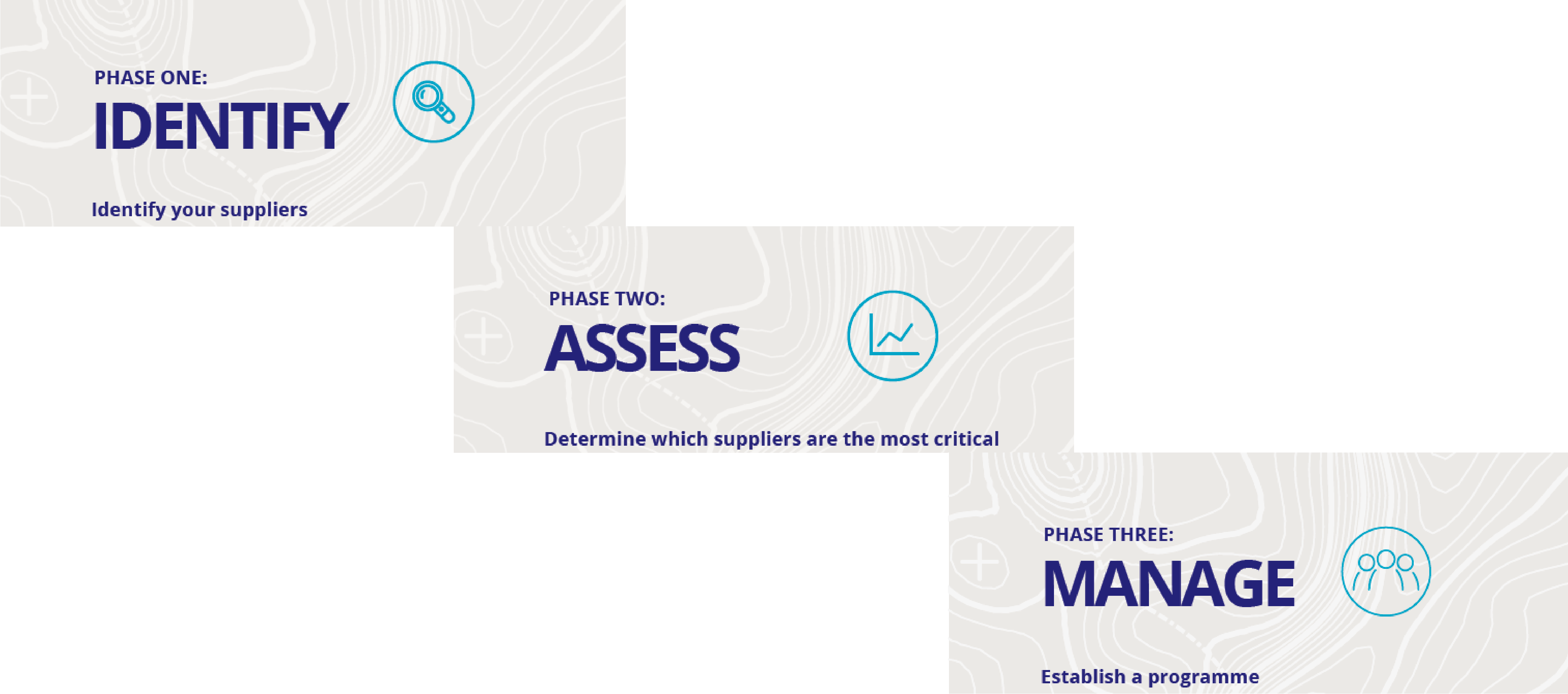
ICT Supply Chain Risk Management (ICT-SCRM)

Part of SCRM strategy that addresses risks presented by ICT assets and services, and their producers, distributors, service providers, and other associated entities in the supply chain.

Supply Chain Cyber Security

Identifying, assessing and managing cyber security risks in the supply chain, encompassing technological and human risk factors.

NCSC’s Recommendations



PHASE ONE:

IDENTIFY

Identify your suppliers

PHASE TWO:

ASSESS

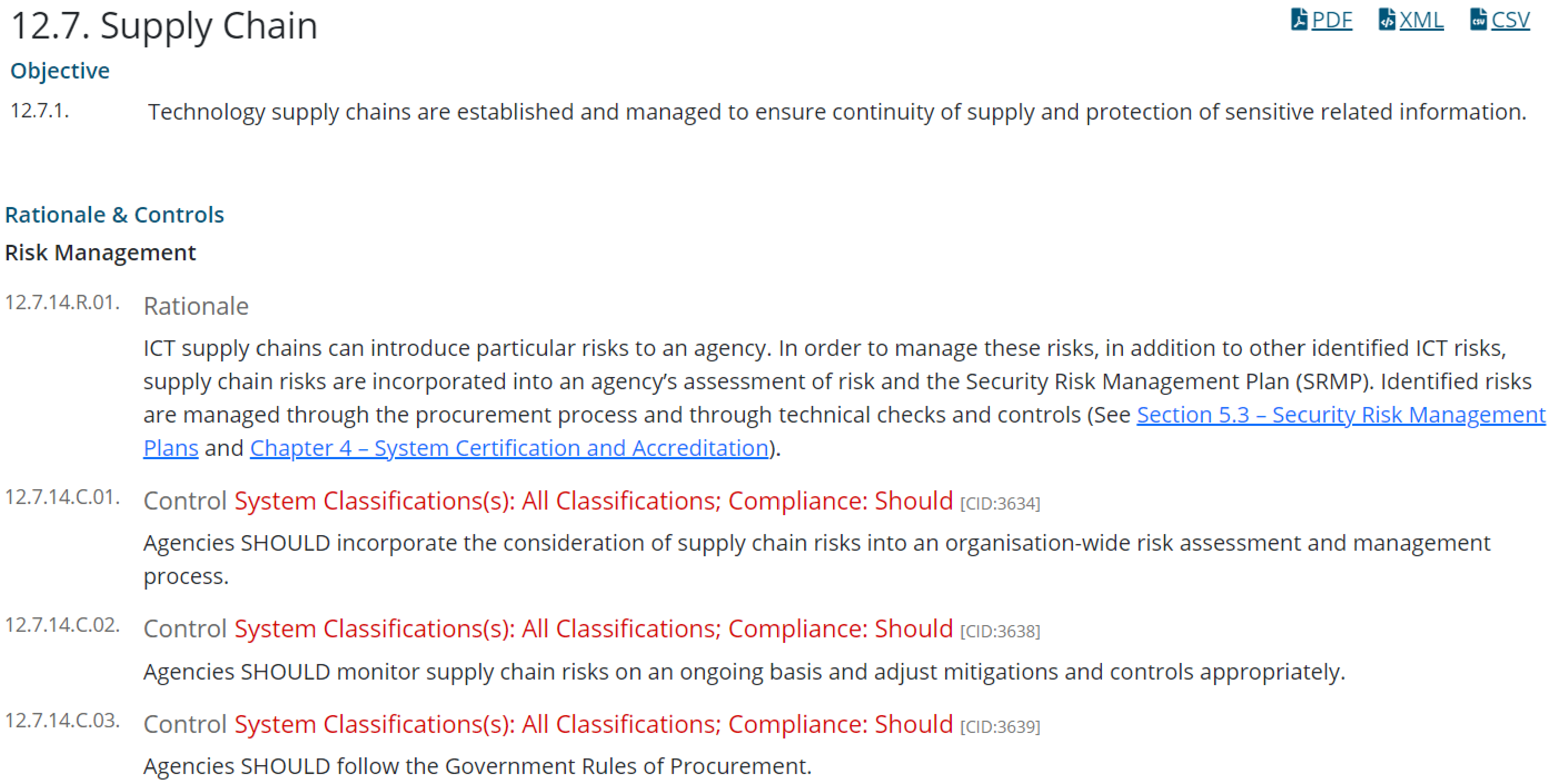
Determine which suppliers are the most critical

PHASE THREE:

MANAGE

Establish a programme

NZISM



12.7. Supply Chain

PDF XML CSV

Objective

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

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.

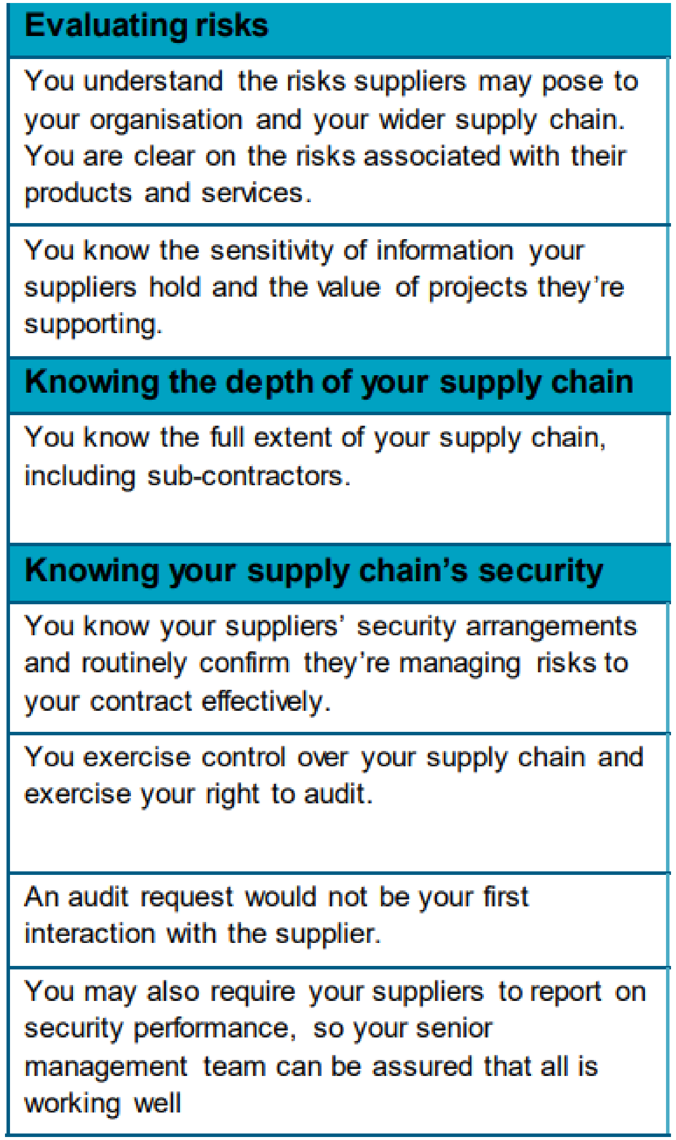
12.7.14.C.02. Control System Classifications(s): All Classifications; Compliance: Should [CID:3638]

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

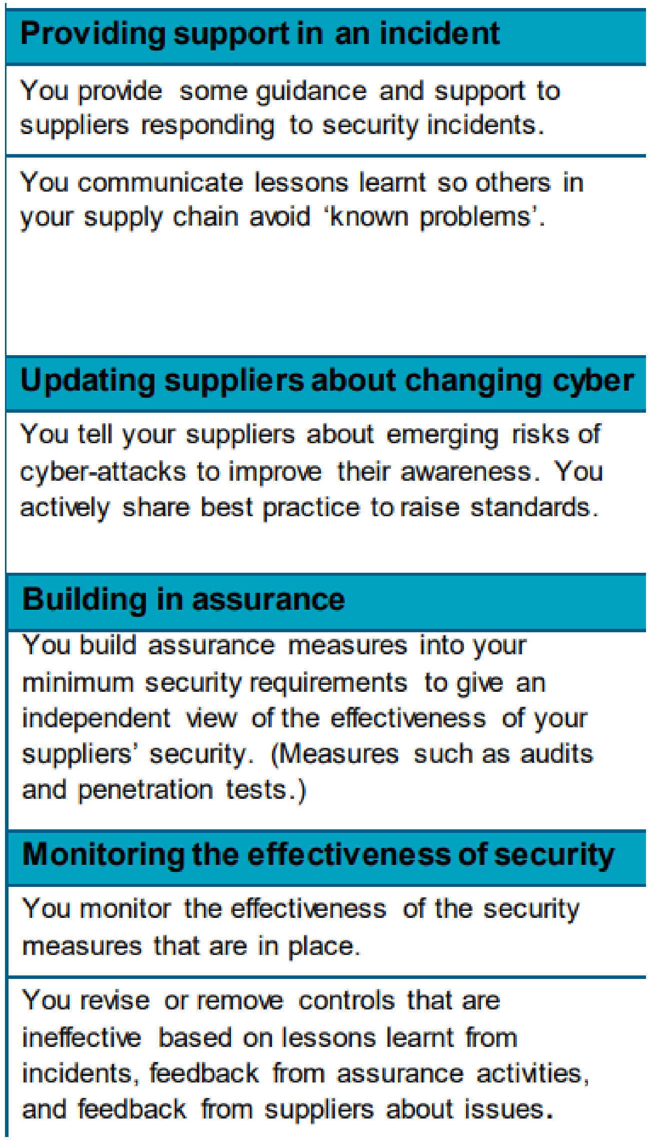
12.7.14.C.03. Control System Classifications(s): All Classifications; Compliance: Should [CID:3639]

Agencies SHOULD follow the Government Rules of Procurement.

NZ Protective Security Requirements

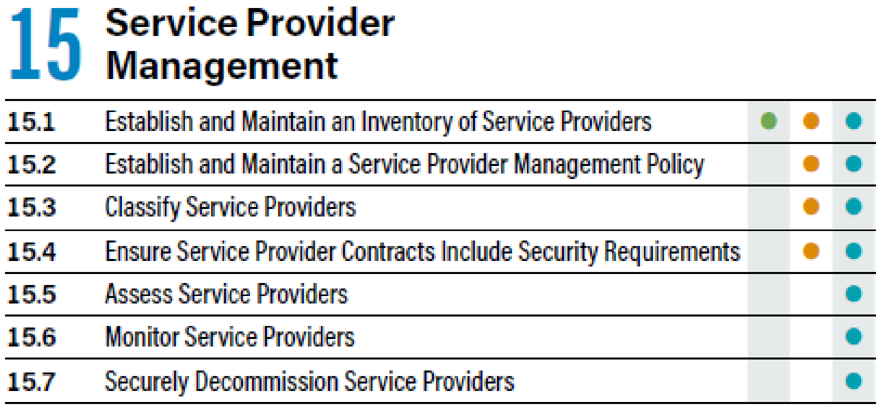


Evaluating risks
You understand the risks suppliers may pose to your organisation and your wider supply chain. You are clear on the risks associated with their products and services.
You know the sensitivity of information your suppliers hold and the value of projects they're supporting.
Knowing the depth of your supply chain
You know the full extent of your supply chain, including sub-contractors.
Knowing your supply chain's security
You know your suppliers' security arrangements and routinely confirm they're managing risks to your contract effectively.
You exercise control over your supply chain and exercise your right to audit.
An audit request would not be your first interaction with the supplier.
You may also require your suppliers to report on security performance, so your senior management team can be assured that all is working well



Providing support in an incident
You provide some guidance and support to suppliers responding to security incidents.
You communicate lessons learnt so others in your supply chain avoid 'known problems'.
Updating suppliers about changing cyber
You tell your suppliers about emerging risks of cyber-attacks to improve their awareness. You actively share best practice to raise standards.
Building in assurance
You build assurance measures into your minimum security requirements to give an independent view of the effectiveness of your suppliers' security. (Measures such as audits and penetration tests.)
Monitoring the effectiveness of security
You monitor the effectiveness of the security measures that are in place.
You revise or remove controls that are ineffective based on lessons learnt from incidents, feedback from assurance activities, and feedback from suppliers about issues.

CIS Controls



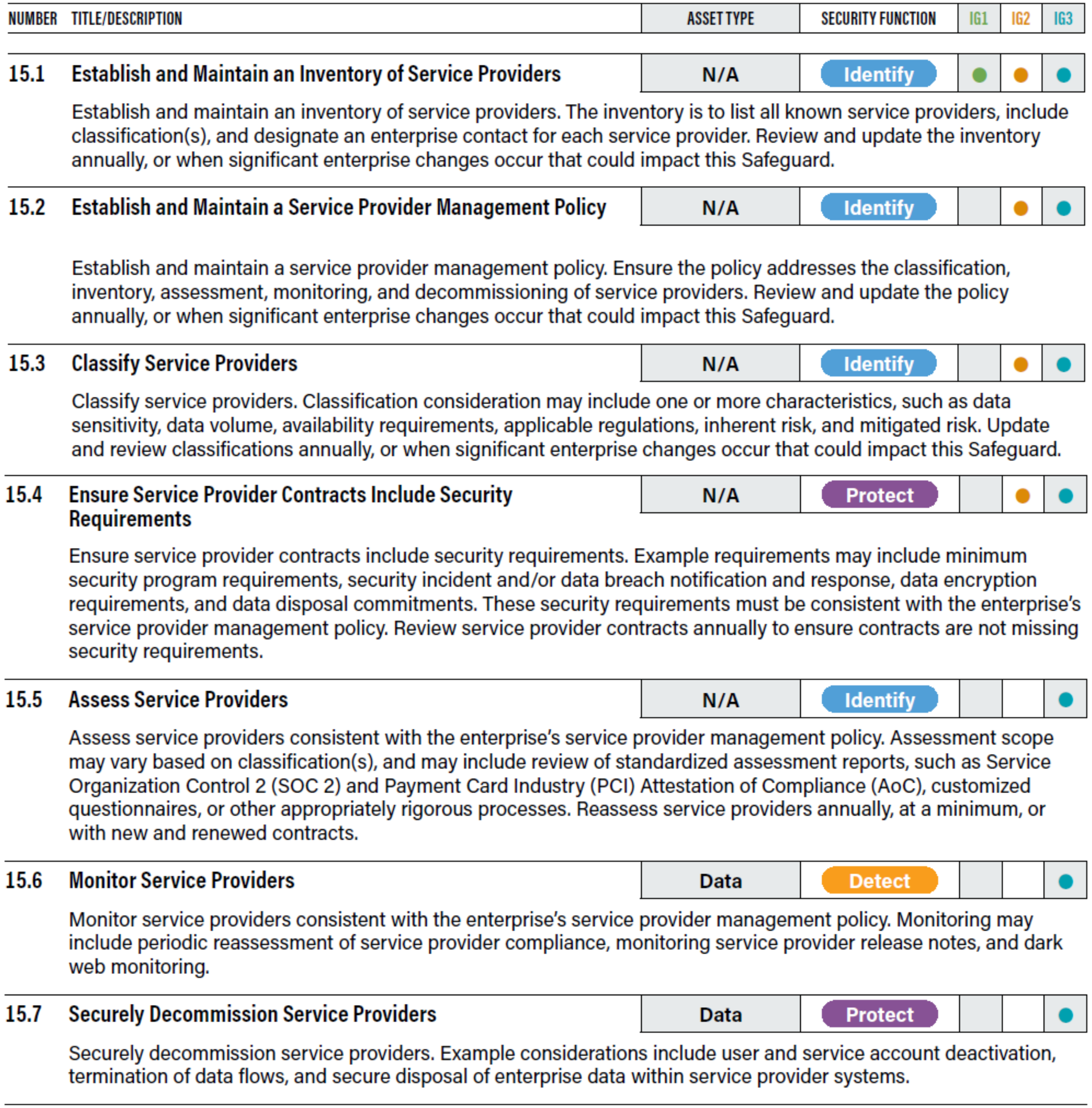
15 Service Provider Management

15.1	Establish and Maintain an Inventory of Service Providers	●	●	●
15.2	Establish and Maintain a Service Provider Management Policy		●	●
15.3	Classify Service Providers		●	●
15.4	Ensure Service Provider Contracts Include Security Requirements		●	●
15.5	Assess Service Providers			●
15.6	Monitor Service Providers			●
15.7	Securely Decommission Service Providers			●

Service Provider Management Policy Template

CIS Critical Security Controls

March 2023

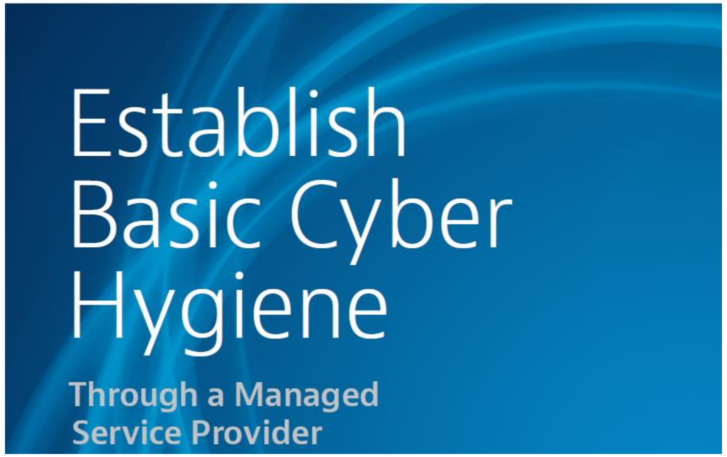


NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
15.1	**Establish and Maintain an Inventory of Service Providers** Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Identify	●	●	●
15.2	**Establish and Maintain a Service Provider Management Policy** Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Identify		●	●
15.3	**Classify Service Providers** Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Identify		●	●
15.4	**Ensure Service Provider Contracts Include Security Requirements** Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.	N/A	Protect		●	●
15.5	**Assess Service Providers** Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts.	N/A	Identify			●
15.6	**Monitor Service Providers** Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.	Data	Detect			●
15.7	**Securely Decommission Service Providers** Securely decommission service providers. Example considerations include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.	Data	Protect			●

CIS Controls

CIS. Center for Internet Security®

CIS Controls

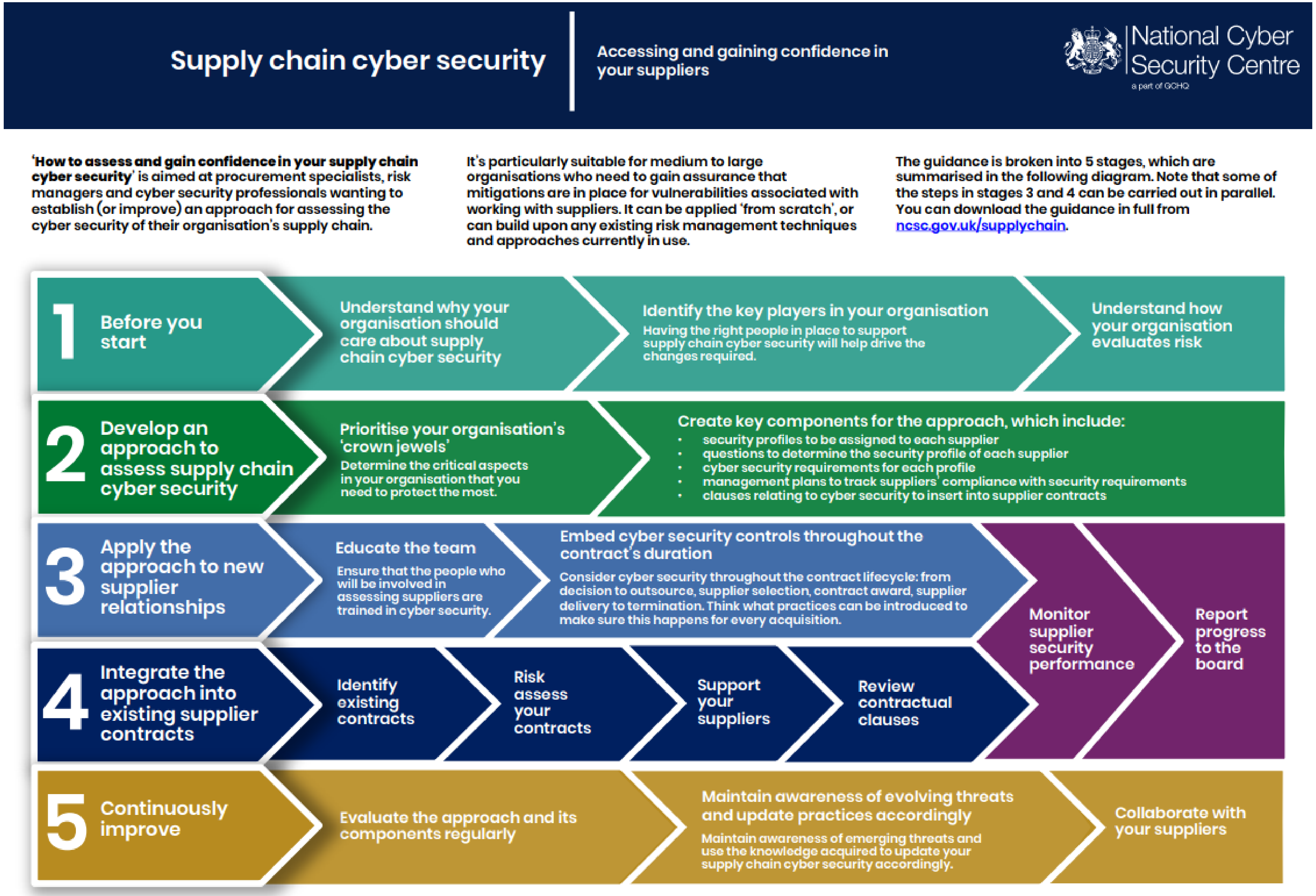


Establish Basic Cyber Hygiene

Through a Managed Service Provider

1. **Does the MSP maintain documentation describing the environment used to administer customer environments? (Sub-Controls: 1.4, 1.6, 12.1, 12.4)**
   - a How often is the documentation updated?
   - b Does the MSP assess against a framework to protect their own and customers' environments?
2. **Is my (customer) network isolated from other networks within the MSP's environment? (Sub-Controls: 2.2, 7.1, 7.7, 8.2, 8.4, 8.5, 9.4, 11.4, 19.6)**
   - a Does the MSP have a defense-in-depth approach to protect the MSP and customer environments?
   - b Is there a process in place to ensure all devices are up-to-date?
   - c Does the MSP use a framework to guide these efforts?
3. **Does the MSP have a backup and system recovery strategy for itself and customers? (Sub-Controls: 19.1, 19.3, 19.5, 19.6)**
   - a Can the strategy be customized?
   - b Are my (customer) high-value assets and data backed up more frequently?
4. **Does the MSP manage and restrict access to management systems within the environment and into customer environments? (Sub-Controls: 4.3, 6.2, 14.6)**
   - a Does the MSP have a list of processes that require recurring access to the customers' systems?
   - b Is the access restricted to only those individuals responsible for those specific processes?
   - c Does the MSP monitor the use of these accounts?

UK NCSC



Supply chain cyber security

Accessing and gaining confidence in your suppliers

National Cyber Security Centre
a part of GCHQ

'**How to assess and gain confidence in your supply chain cyber security**' is aimed at procurement specialists, risk managers and cyber security professionals wanting to establish (or improve) an approach for assessing the cyber security of their organisation's supply chain.

It's particularly suitable for medium to large organisations who need to gain assurance that mitigations are in place for vulnerabilities associated with working with suppliers. It can be applied 'from scratch', or can build upon any existing risk management techniques and approaches currently in use.

The guidance is broken into 5 stages, which are summarised in the following diagram. Note that some of the steps in stages 3 and 4 can be carried out in parallel. You can download the guidance in full from ncsc.gov.uk/supplychain.

1 Before you start

- Understand why your organisation should care about supply chain cyber security
- Identify the key players in your organisation
  Having the right people in place to support supply chain cyber security will help drive the changes required.
- Understand how your organisation evaluates risk

2 Develop an approach to assess supply chain cyber security

- Prioritise your organisation's 'crown jewels'
  Determine the critical aspects in your organisation that you need to protect the most.
- Create key components for the approach, which include:
  - security profiles to be assigned to each supplier
  - questions to determine the security profile of each supplier
  - cyber security requirements for each profile
  - management plans to track suppliers' compliance with security requirements
  - clauses relating to cyber security to insert into supplier contracts

3 Apply the approach to new supplier relationships

- Educate the team
  Ensure that the people who will be involved in assessing suppliers are trained in cyber security.
- Embed cyber security controls throughout the contract's duration
  Consider cyber security throughout the contract lifecycle: from decision to outsource, supplier selection, contract award, supplier delivery to termination. Think what practices can be introduced to make sure this happens for every acquisition.

4 Integrate the approach into existing supplier contracts

- Identify existing contracts
- Risk assess your contracts
- Support your suppliers
- Review contractual clauses

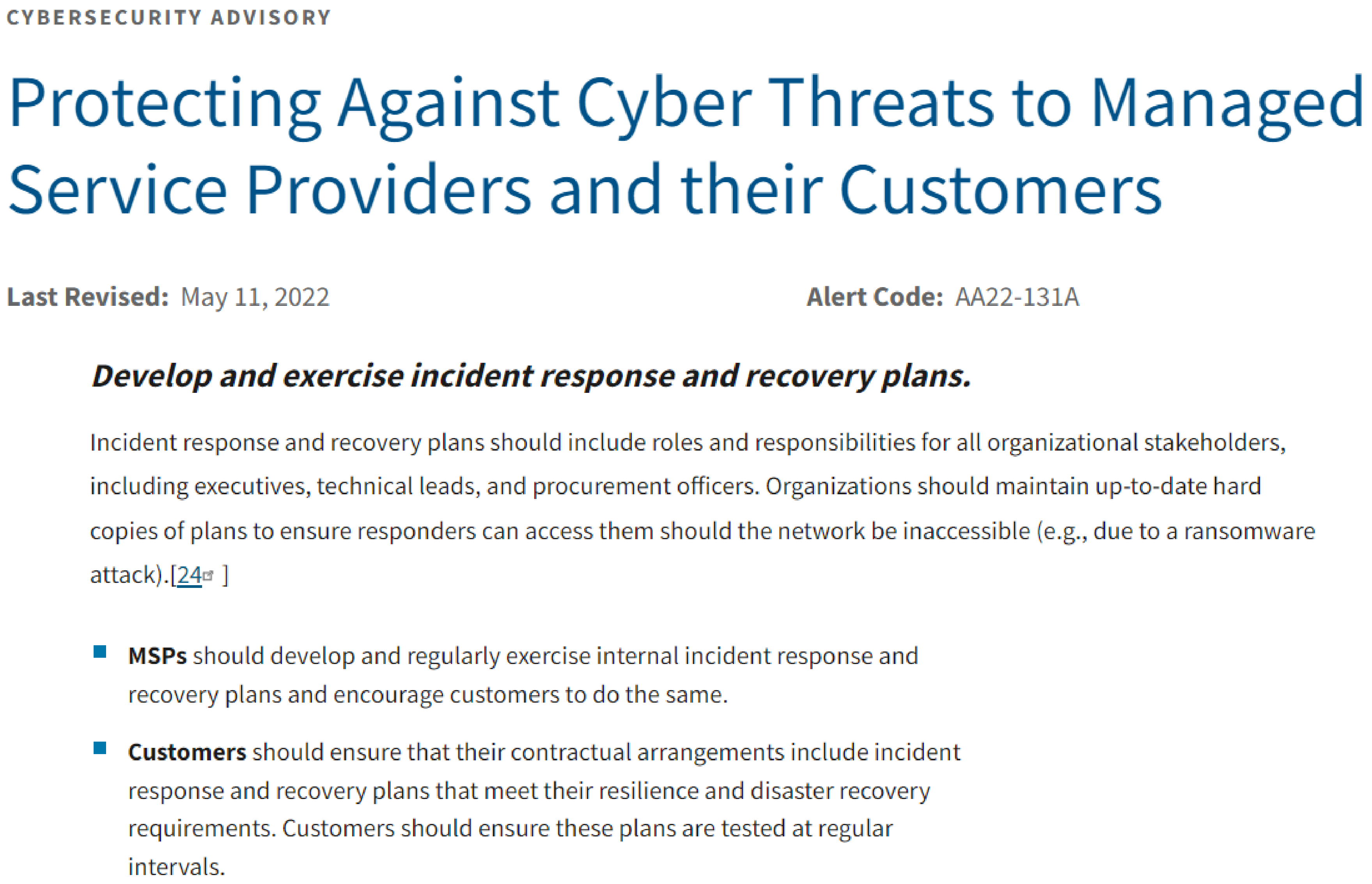
(Stages 3 and 4:)

- Monitor supplier security performance
- Report progress to the board

5 Continuously improve

- Evaluate the approach and its components regularly
- Maintain awareness of evolving threats and update practices accordingly
  Maintain awareness of emerging threats and use the knowledge acquired to update your supply chain cyber security accordingly.
- Collaborate with your suppliers

US CISA



CYBERSECURITY ADVISORY

Protecting Against Cyber Threats to Managed Service Providers and their Customers

Last Revised: May 11, 2022

Alert Code: AA22-131A

Develop and exercise incident response and recovery plans.

Incident response and recovery plans should include roles and responsibilities for all organizational stakeholders, including executives, technical leads, and procurement officers. Organizations should maintain up-to-date hard copies of plans to ensure responders can access them should the network be inaccessible (e.g., due to a ransomware attack).[24]

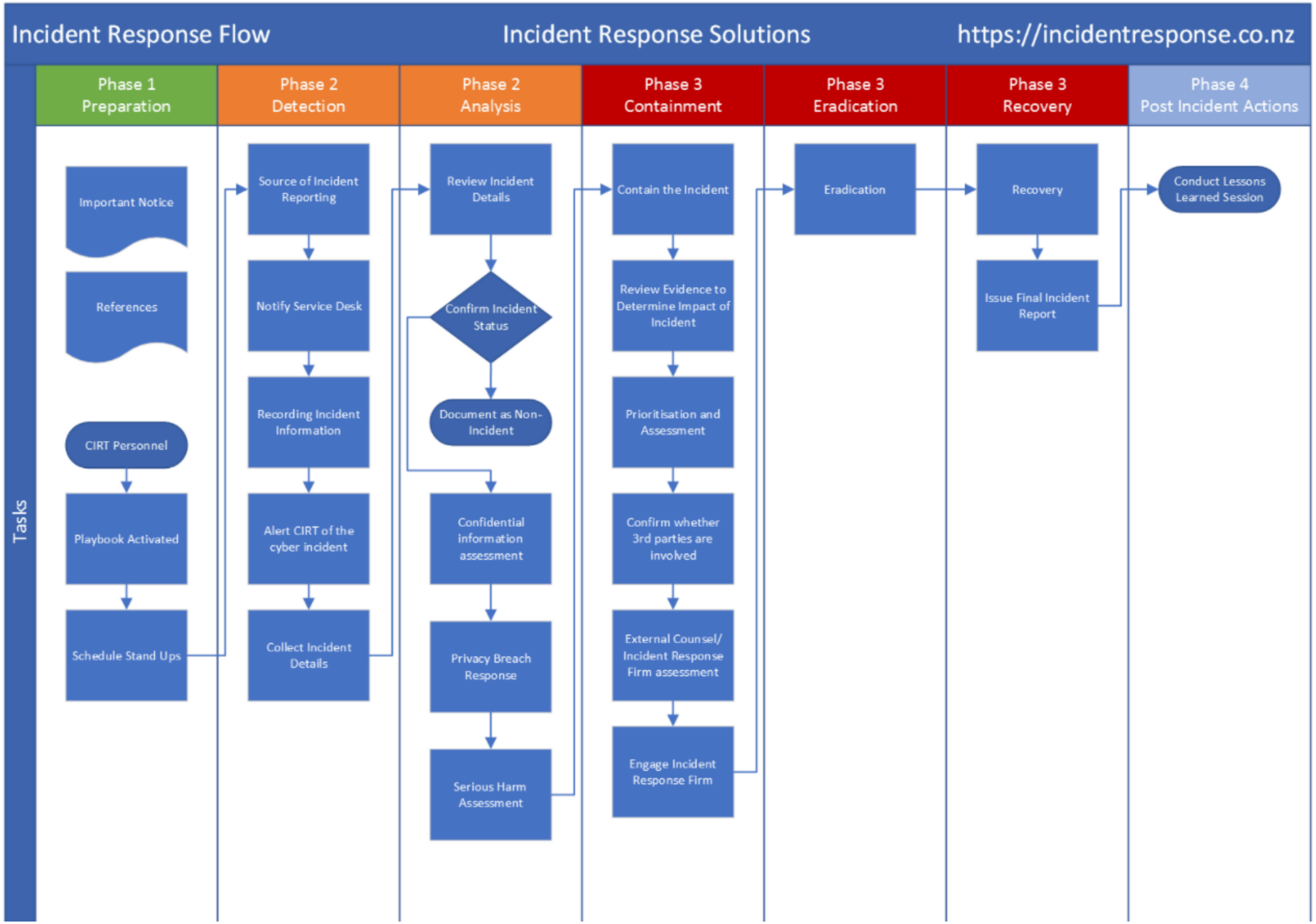
- **MSPs** should develop and regularly exercise internal incident response and recovery plans and encourage customers to do the same.
- **Customers** should ensure that their contractual arrangements include incident response and recovery plans that meet their resilience and disaster recovery requirements. Customers should ensure these plans are tested at regular intervals.

Incident Response - Next Steps

To support the improvement steps outlined above, we recommend considering actioning the following initiatives to improve your level of cyber incident preparedness:

1. *Develop an incident response plan and set of relevant playbooks (e.g. Third Party Attack etc).*
2. *Conduct a forensic readiness assessment, including of the service providers systems.*
3. *Have a pre-populated out-of-band incident response control room tool that you can interact with external parties on.*
4. *Conduct a series of cyber simulations to test improvements in the above initiatives, include your key service providers.*
5. *Ensure that changes to technology, procedures and people at your key service providers are updated within the above documentation.*

Incident Response Plan and Playbooks



Incident Response Flow

Incident Response Solutions

https://incidentresponse.co.nz

Tasks

Phase 1
Preparation

Important Notice

References

CIRT Personnel

Playbook Activated

Schedule Stand Ups

Phase 2
Detection

Source of Incident Reporting

Notify Service Desk

Recording Incident Information

Alert CIRT of the cyber incident

Collect Incident Details

Phase 2
Analysis

Review Incident Details

Confirm Incident Status

Document as Non-Incident

Confidential information assessment

Privacy Breach Response

Serious Harm Assessment

Phase 3
Containment

Contain the Incident

Review Evidence to Determine Impact of Incident

Prioritisation and Assessment

Confirm whether 3rd parties are involved

External Counsel/ Incident Response Firm assessment

Engage Incident Response Firm

Phase 3
Eradication

Eradication

Phase 3
Recovery

Recovery

Issue Final Incident Report

Phase 4
Post Incident Actions

Conduct Lessons Learned Session

What services are clients engaging in?

- Cyber Framework
- Cyber Controls
- Incident response plans and playbooks
- Incident response control room
- Tabletop simulations
- Responding to incidents including forensics
- Incident Response Retainer

Thank you

Campbell McKenzie

0800 WITNESS or 021 779 310

campbell@incidentresponse.co.nz

incidentresponse.co.nz

whistleblowers.co.nz

Incident Response
FORENSIC & CYBER