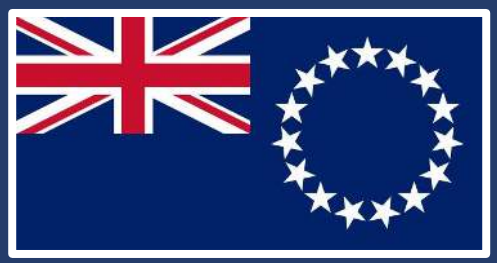

Protective Security Policy Framework

Guidance for Security Practitioners

Table of Contents

Directive on the security of the Cook Islands Government

Foreword

Kia Orana

The Cook Islands Government aspires to deliver its service in an efficient, safe and secure way while building trust and confidence in the ability of its employees to identify and manage risks that will interfere with the delivery of that service.

The Cook Islands Protective Security Policy Framework (CIPSPF) goals can only be achieved if Heads of Government Ministries and their employees actively implement the CIPSPF requirements and apply security measures to address risk environments that are unique to their respective Ministries.

The CIPSPF is tailored to take proper account of the very wide range of different jobs that we do, assets we handle and environments that we work in. Getting security right has never been more important as Government Ministries continue to modernise and improve ways of working, and deliver more and more services online. There are longstanding threats and risks to bear in mind but we must also continue to develop our growing appreciation of global and cyber challenges, critical infrastructure dependencies, together with wider resilience and sustainability issues.

The CIPSPF ensures we can keep and develop the public's trust that we will handle their information properly, advise Ministers in confidence and protect the many commercial and financial interests we are responsible for while maintaining national security.

It is critical therefore for all Cook Islands Government employees to understand and actively apply a security culture that is embedded in their Ministry as we continue to modernise and improve our ways of working and deliver more services online as well as appreciating the growing global and cyber security challenges.

The Cook Islands Government, through the Office of the Prime Minister with oversight of the Government Protective Security Committee, will continue to assess emerging security risks and develop and refine protective security policy that will contribute to the efficient, safe and secure delivery of government services.

Kia Manuia

Ben Ponia
Chief of Staff
Office of the Prime Minister

1.0 Protective security framework

What is protective security?

Protective security are the measures taken to protect people, information, and assets. Protective security encompasses and extends organisational practices such as health and safety, privacy, business continuity, incident management, and emergency and disaster management.

The protective security framework is a set of best practice guidelines and principles to help identify what your organisation must do to protect your people, information and assets.

The framework has been designed with enough flexibility to be used across all organisations with differing needs and capabilities.

Why security matters

In today's environment, threats to security come from many directions. It is important that organisations have systems in place to reduce their vulnerabilities. Threats may include natural disasters and weather events, violence, damage to organisational property, fraud, theft, breach of residents' privacy, loss or compromise of sensitive information, espionage and cyber-criminal attacks.

Good security protects an organisation's people, reputation, and effectiveness. It provides clients, partners and residents with confidence and trust in the Cook Islands public service.

Protective security is the responsibility of everyone working for an organisation, including suppliers.

Overview of the framework

Protective security framework

The protective security framework has four tiers and a hierarchical structure of 17 requirements.

Cook Islands Government organisations are expected to adopt the Protective Security Framework and build their capability over time to meet the 17 requirements as soon as practical. Private sector organisations should consider adopting the requirements as best practice. The framework provides you with guidance on how to meet the requirements.

Security governance requirements

Ensuring an organisation has security management structures, procedures and culture in place to respond appropriately to security events.

1. Establish and maintain the right governance and management
2. Understand what needs protection
3. Assess capability
4. Build security culture
5. Develop and maintain security policies, processes and procedures
6. Manage risks when working with others
7. Manage security incidents
8. Be able to respond

MORE INFORMATION

- Security Governance

Personnel security requirements

Ensuring your people are trusted to have access to official information and assets.

1. Recruit the right person
2. Ensure their ongoing suitability
3. Manage their departure

MORE INFORMATION

- Personnel Security

Information security requirements

Ensuring the confidentiality, integrity and availability of your information is protected.

1. Design information security
2. Check security measures
3. Keep security up to date

MORE INFORMATION

- Information Security

Physical security requirements

Providing and maintaining a safe and secure working environment.

1. Design physical security
2. Check security measures
3. Maintain security

MORE INFORMATION

- Physical Security

Classifications

The Cook Islands Government has four security classifications that must be applied to confidential information depending on the sensitivity of the information.

There are a number of further markings that can be applied to confidential information to further restrict access to information.

OFFICIAL	RESTRICTED	SECRET	TOP SECRET
Most of the information that is created or processed by the public service during routine business operations and services. This information is not subject to a heightened threat profile.	Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage law enforcement capabilities, international relations or the investigation of serious organised crime.	Government information that could have damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen, or published in the media, but is not subject to a heightened threat profile.	Cook Islands Government's most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could lead directly to widespread loss of life or threaten the security or economic wellbeing of the country or friendly nations.

MORE INFORMATION

- Cook Islands Information Classification System

Security Areas

The Cook Islands Government has three physical areas for handling information and people.

Public areas

These are unsecured areas including out-of-office working arrangements. They provide limited access controls to information and physical assets where any loss of information would be unlikely to damage the security or interests of the Cook Islands or the privacy of its residents. They also provide limited protection for people.

Work areas

These are low-security areas with some controls. They provide access controls to information and physical assets where any loss could result in prejudice to the maintenance of law and order, impede effective conduct of government or adversely affect the privacy of residents. They also provide some protection for people.

These areas allow unrestricted access for organisations, people and contractors. Public or visitor access is restricted.

Secure areas

These are security areas with higher levels of security measures in place. They provide access controls to information where any loss could result in serious (SECRET) or exceptionally grave (TOP SECRET) damage to national interests. They may also provide additional protection for people.

Access should be strictly controlled with ID verification, key/card access, and logging of access. People with ongoing access should hold an appropriate security clearance. Visitors and contractors must be closely controlled and have a business need to access the area.

MORE INFORMATION

- Physical Security

Alert Levels

The Cook Islands Government has three colour coded security alert levels. The different levels trigger specific actions to be taken by government organisations based upon their specific response plans.

Low risk – Green

A threat event is unlikely.

- No unusual activity exists beyond the normal concerns.

Moderate risk – Yellow

A threat event is possible.

- Increased threat risk including weather, natural, physical, social, or cyber threats
- Increased risk of harm to staff or the public
- Risk of significant damage to critical infrastructure or IT systems.

High risk – Red

A major threat event is imminent or has occurred and countermeasures are insufficient to prevent harm to people, information and/or assets.

- Severe weather event or natural disaster; i.e. cyclone
- Major internal incident such as fire, flooding, or cyber attack
- Potential for, or actual, loss of lives
- Widespread exploit, outage, or failure of critical infrastructure or IT systems.

> **MORE INFORMATION**
>
> - Being able to respond

Complying with the Protective Security Framework

The protective security requirements and security measures outlined in this framework are based on best practice relating to protective security and reflect the Government objectives for security.

When legislation requires organisations to manage protective security in a way that is different to the framework, that legislation takes precedence.

2.0 Security Governance

Effective protective security supports organisational goals and its' culture. It addresses the security threats and vulnerabilities that put people, information and assets at risk. Building the right security culture and plan for an organisation is essential.

This requires commitment and leadership from the top.

MORE INFORMATION

- Establish and maintain the right governance and management
- Understand what you need to protect
- Assess your capability
- Build security culture
- Develop and maintain security policies, processes and procedures
- Manage risks when working with others
- Manage security incidents
- Be able to respond

2.1 Governing and managing (GOVSEC-1)

GOVSEC-1
Establish and maintain the right governance and management

Establish and maintain a governance structure that ensures the successful leadership and oversight of protective security risk.

Appoint a member of the senior team as your Chief Security Officer, responsible for the organisation's overall protective security policy and oversight of protective security practices.

Create the security team

Identify who is responsible for the overall protective security policy and programme. Appoint a member of the senior team as the Chief Security Officer (CSO). Ideally this should be the Head of Department or equivalent. Give a mandate to the CSO for establishing and undertaking the organisation's protective security programme.

Build an effective security team with clear, well-defined, and rehearsed procedures. Ensure the CSO has clear reporting lines to all people with security responsibilities.

Establish governance

Ensure that protective security is on the agenda at your standing leadership meetings. Develop a governance structure that enables them to effectively:

- Identify and manage security risks
- Establish priorities and activities for improvement
- Govern the implementation of the protective security programme
- Monitor and assure the effectiveness of security management across the organisation
- Review security policy and programme to inform updates to the programme at regular intervals
- Obtain briefings on the emerging threats to the organisation.

Protective security roles and responsibilities

Heads of Ministry (HOM)

The Head of Ministry (HOM) or equivalent has overall accountability for protective security within an organisation. He or she is responsible for establishing and maintaining the right governance and management that ensures the successful leadership and oversight of protective security risk.

Chief Security Officer (CSO)

The CSO has overall responsibility for the protective security policy and programme. For most organisations, the CSO role will be a part time addition to an existing senior role rather than a full-time position.

The CSO's responsibilities include:

- oversight of organisation's protective security
- communicating and implementing protective security policy
- establishing a protective security programme based on the priorities and identified risks faced
- reporting on security performance and providing guidance to the Head of Ministry (HOM) on security matters
- managing and reporting security incidents
- implementing a security awareness programme
- liaison with security organisations in relation to protective security requirements.

It may be necessary to appoint specialist security personnel reporting to and/or supporting the CSO depending on an organisation's size, risk profile and the amount of protectively marked material held and equipment operated by the organisation.

In all cases, there must be a clear allocation of responsibilities for security.

Security Manager/Officer

Formalise management and operational roles and responsibilities for personnel security, information security, and physical security.

Consider appointing security roles other than the CSO designated as a 'security manager' or 'security officer' for the specialist domain role, for example, Information Security Manager. This role may only form part of their usual job.

Responsibilities include:

- Conducting security risks assessments
- Maintaining and managing the security risk management plan
- Monitoring emerging threats and assessing the effectiveness of existing capability and security measures to manage the risks
- Consulting with business teams to design the appropriate security measures to mitigate the risks
- Planning, developing and implementing the security programme
- Supporting the development, testing, and readiness assessment of response plans and business continuity plans
- Facilitating the implementation of the security policy into day-to-day operational processes, procedures and systems
- Overseeing the development and delivery of the security awareness campaigns and training programmes including training and communication materials
- Assessing compliance with security policies and standards, recording and investigating incidents, and root cause analysis to inform changes and new security measures
- Provide security advice to CSO, leaders, projects, and operational staff and contractors
- Liaising with suppliers and assuring their compliance with the organisation's security requirements
- Monitoring and reporting on security performance (compliance with policy, incidents, threats, vulnerabilities) and recommending actions to reduce risks.

2.2 Understanding what you need to protect (GOVSEC-2)

GOVSEC-2
Understand what you need to protect

Identify the people, information, and assets that your organisation manages. Assess the security risks (threats and vulnerabilities) and the impact of any security breach.

Deep understanding of the organisation's operating environment coupled with robust risk assessment will help to define the security capabilities needed and assess any shortfalls.

Identify the most valuable assets

Identify which assets are critical to organisational success and continuing operation. Include people, products, services, processes, facilities and information. Look outside the organisation to suppliers and contractors.

Some information is more valuable or sensitive, requiring a greater level of protection. Establish an accurate picture of the impact on the organisation if sensitive internal or customer information was lost or stolen.

Understand the risks

Identify and assess the security risks and threats to the most valuable assets. Threats are diverse, may exist in physical or cyberspace, and may change over time. Consider exchanging information with other organisations to help to identify emerging threats. Work on the premise is also likely to be a key target.

Use the protective security self-assessment to understand the organisation's current protective security capabilities and capability shortfalls as these can be key vulnerabilities for the organisation.

Accept that everything cannot be protected. Prioritise the risks to the organisation. Reduce the vulnerability to them and their impact by putting a range of personnel, information, and physical security measures in place.

Plan an improvement roadmap. Understand that one size does not fit all – each organisation faces different risks and therefore will need to focus their improvements in different areas.

Personnel risks

Insider threats come from our past or present employees, contractors or business partners. They can misuse their inside knowledge or access to harm people, customers, assets or reputation. Personnel security focusses on reducing the risks associated with insider threats.

An 'insider threat', or 'insider', is any person who exploits, or intends to exploit, their legitimate access to an organisation's assets to harm the security of their organisation or the Cook Islands, either wittingly or unwittingly, through espionage, terrorism, unauthorised disclosure of information or loss or degradation of a resource (or capability). Common insider acts include:

- unauthorised disclosure of official, private, or proprietary information
- fraud or process corruption
- unauthorised access to ICT systems
- economic or industrial espionage
- theft
- violence or physical harm to others.

Many security breaches are unintentional and result from a lack of awareness or attention to security practices, being distracted or being fooled into unwittingly assisting a third party.

MORE INFORMATION

- Personnel Security
- Security Risk Management Handbook

Information risks

Threats to the security of information can come from inside and outside the organisation. Information in all forms (for example electronic, printed or spoken) needs to be appropriately protected. Information stored and processed on IT systems or mobile devices is vulnerable to cyber-specific threats.

We are far more exposed today than ever before:

- We have increasing quantities of electronic information, and organisations are often heavily dependent upon it to function.
- We have cloud, social media, mobile and other emerging technologies which have increased the means by which critical information can be accessed.
- The threats are increasing and continually evolving making detection challenging.

External actors and disgruntled insiders have been known to:

- expose or publish sensitive information in the public domain
- encrypt and then ransom critical information

- sell information to competitors and interested parties
- steal intellectual property (IP)
- compromise organisations by destroying or denying access to records.

Employees may also accidentally compromise your information because they:

- lack awareness of your security practices and why they're important
- get distracted or complacent while handling organisational information
- provide access to other parties seeking information for criminal or other inappropriate purposes. For instance: "social engineering" attacks attempt to manipulate people into breaking normal security controls and often disguise themselves as someone trusted through phishing, pretexting, baiting, quid pro quo, or other means.

MORE INFORMATION

- Information Security
- Security Risk Management Handbook

Physical risks

Physical security is multi-faceted and compliments security measures in other areas. Good physical security supports health and safety standards, and helps organisations operate more efficiently and effectively. Knowing where vulnerabilities are is the first step towards robust physical security.

Identify the people, information and assets that the organisation needs to protect and where they are. Assess the security risks (threats and vulnerabilities) and the business impact of loss or harm.

For facilities, consider how they are used, who will use them, and what will be stored in them. Other areas to think about are:

- Arrangements for people working away from the office
- Co-location arrangements with other parties
- Plans for new sites or buildings, and plans for alterations
- ICT equipment and information
- Other parties and your supply chain.
- Use this understanding to:
    - Protect employees from threats of violence, and support them if they experience a harmful event
    - Protect members of the public who interact with the organisation
    - Put physical security measures in place to minimise or remove risks to information assets.

MORE INFORMATION

- Physical security
- Security Risk Management Handbook

Where is the organisation vulnerable?

Identify areas where the organisation might be vulnerable to security breaches (deliberate or accidental). Determine which vulnerabilities might be exploited and how this might be limited.

A vulnerability is a weakness in security defences. To assess your vulnerabilities, it is important to understand where defences are weak. An annual security self-assessment is a great starting point for identifying security vulnerabilities.

Identify and document the potential threats to security and ensure that this information is kept current.

Here are some questions to help think about situations when the organisation might need to put extra protection in place.

- Who would benefit from having access to the organisation's people, information or assets and what would they want?
- How much do the public know about what employees do or what facilities are used for? Are there any contentious programmes being run out of facilities that might attract attention?
- Is there a high level of crime in the neighbourhood?
- Are employees at risk of violence from clients?
- Are facilities at risk from public violence arising from protests?
- Are there shared facilities or co-tenancies with other private or public high-risk tenants?
- How valuable are the information and assets? Would they be attractive to groups of security concern, including foreign intelligence services, issue-motivated groups, or trusted insiders?
- Are ICT systems that hold sensitive information connected to the internet and possibly vulnerable to cyber-attack?

Threats evolve continually. The CSO and security team should refer to international expert advice to stay ahead of emerging threats.

MORE INFORMATION

- UK National Protective Security Authority
- US CERT — US Computer Emergency Readiness Team Current Activity

- ASD CSC — Australian Signals Directorate Cyber Security Centre
- NZ NCSC – New Zealand National Cyber Security Centre
- Internet Storm Center – SANS Technology Institute
- Software Security – Carnegie Mellon University
- Security Risk Management Handbook

Manage security risks

An organisation's process for managing security risks should include:

STEP 1

Assess the likelihood of the risk being realised – including the vulnerabilities and threats you are exposed to

STEP 2

Assess the impact – the level of harm done if your security is breached

STEP 3

Assess the security risk against the adequacy of existing safeguards

STEP 4

Determine level of acceptable risk

STEP 5

Treat the risk – determining and implementing security measures to reduce risks to acceptable levels

STEP 6

Monitor and evaluate the risks.

MORE INFORMATION

- Security Risk Management Handbook

2.3 Assessing your capability (GOVSEC-3)

> **GOVSEC-3**
> **Assess your capability**
> Use an annual evidence-based assessment process to provide assurance that an organisation's security capability is fit for purpose. Provide an assurance report to Government if requested.

Ongoing improvement in protective security requires a cycle of assessing and managing risks in an ever-changing environment.

The self-assessment tool enables an organisation to:

- identify their needs for security measures
- evaluate the effectiveness of their protective security practices
- plan the focus areas and actions they will take to improve protective security
- report back to Government on current capability and improvement plans.

The protective security assessment spider diagram provides a quick snapshot of current security capability mapped against organisational across the dimensions of the protective security framework. The model has three capability levels:

- **Developing (1.0)** – you may meet protective security requirements in some areas but are developing your capability in other areas.
- **Managing (2.0)** – you meet all protective security requirements and are effectively managing protective security across all 4 domains.
- **Leading (3.0)** – you go beyond the requirements and are actively developing your organisation's skills, monitoring, and measures to rapidly address emerging threats.

Self-assessment

To conduct a self-assessment:

- Involve others in the self-assessment representing different parts of the organisation, from executives to specialists and take them on the journey. It is a learning process for everyone and provides a good forum for balancing needs and priorities.
- Do not assume that capability will be the same as it was during previous assessments. It still takes effort to retain capability at the same level.
- Gather the evidence that supports the assessment. This may include review of documentation of processes and procedures, security programme deliverables, security incidents, security performance measures and reports, and staff training, awareness and engagement surveys.

- Answer the questionnaire based on what best represents the organisation's current capability as demonstrated in the evidence gathered. Remember that the capability may have regressed if the organisation has lost key personnel or no longer has the resources assigned to maintain it.

Set capability goals

- The self-assessment tool will automatically calculate a current capability score and illustrate this in the spider diagram.
- Set a goal for improvement. Be realistic with what can be accomplished.

Organisations face different types and levels of security risk, so targets need to reflect specific goals and priorities. One size does *not* fit all.

- For organisations new to the framework, their year 1 goals will be very different to organisations who have been on the protective security journey for multiple years.

Year 1 priorities
Establish, understand and plan

When just starting out with the framework, organisations need to appoint a team, setup governance, establish a baseline to understand where they are, what they have, and what they need. You need to understand the risks faced and prioritise and plan the improvement effort. Core priorities in year 1 are likely to focus on:

- **GOVSEC-1: Establish and maintain the right governance and management**: Appoint the team, establish the governance, and commission the work. There must be a mandate to develop and undertake the first year's security programme.
- **GOVSEC-2: Understand what you need to protect:** Conduct a risk assessment to understand what the organisation has, what the risks and vulnerabilities are, and set the priorities for risk treatments such as mitigation.
- **GOVSEC-3: Assess your capability**: Conduct the first self-assessment to establish a baseline and identify specific development needs. Develop and plan a security programme.
- **GOVSEC-5: Develop and maintain security policies, processes, and procedures**: At a minimum, understand what security policies, processes and procedures you have in place and establish your security policy in line with the protective security framework.

Year 2 priorities
Consolidate and implement

In the second year, focus on implementing the core capability to build security awareness, address critical risks, and sustain momentum in improvement.

This is likely to include focus on:

- Maintain what was put in place in Year 1 and reassess the risks to ensure that emerging threats are identified and reassess priorities.
- **GOVSEC-5: Develop and maintain security policies, processes, and procedures:** Build core processes, procedures, and systems to implement security policies and mitigate the highest risks.
- **GOVSEC-4: Build your security culture:** Establish core training and security awareness campaigns to communicate security policies and ensure that people understand how to comply.
- **GOVSEC-7: Manage security incidents:** Build a security incident management capability to ensure that you record, report, respond, and investigate incidents and build the learnings into the security programme.
- Design and implement the security programme, establishing the most critical security measures for Personnel Security (**PERSEC**), Information Security
- (**INFOSEC**), and Physical Security (**PHYSEC**) to treat the highest risks.
- As part of the annual self-assessment in **GOVSEC-3** develop a stronger security programme and multi-year roadmap that will continue to build the capability over time.

Year 3+ priorities
Continually improve to mitigate your risks

By year 3, the priorities in the security programme will be driven by the organisation's specific risks and priorities. Where practical, aim to achieve at least '**Managing (2.0)**' capability across all 17 dimensions. However, this could take several additional years of effort and will be driven by the organisation's priorities and risk appetite.

Note: Even if it is not planned to increase capability in a dimension, it will take effort to maintain the capability at the current level.

> **MORE INFORMATION**
>
> - Self-assessment Tool Template

Reporting to Government

Certain organisations must report, externally and in writing, on their protective security capability and compliance with the protective security framework.

External reporting confirms organisations:

- have undertaken an assessment against the protective security requirements
- have gathered the evidence to support the assessment made
- understand where the organisation is at risk and have set appropriate protective security goals
- have an effective plan in place to reach goals and maintain the appropriate level of protective security capability based on the risk profile.

If required, conduct a self-assessment at least annually of the protective security capability and report back to Government on current capability, targets for improvement, and priorities and plans for the coming year.

The report should have enough detail to understand the progress that has been made since the last report (if applicable) and capture any issues and barriers that have been identified. You should add commentary to capture the changes in capability – whether positive or negative, and the reasons behind the change. Organisations should consider their progress over the previous 12 months in relation to each capability dimension, and then plan the 12 month and optimal maturity targets and the rationale behind them.

The report should be compiled and signed by both the HOM and CSO.

The Protective Security Reporting Template includes sections for:

- HOM's summary for the year
- CSO's reporting against the Protective Security Requirements and commenting on your capability levels, goals, and plans
- Providing feedback on the Protective Security Framework and requesting support for delivery of the Protective Security Programme.

> **MORE INFORMATION**
> Protective Security Reporting Template

Improving protective security

Establish and undertake a review of the protective security improvement programme at least annually that identifies prioritised improvements that will be implemented to address security capability gaps and manage risks.

The Protective Security Roadmap Template can be used to plan the Protective Security

Programme and show how compliance requirements overall will be met. The Roadmap is for internal use and does not need to be reported back to Government.

> **MORE INFORMATION**
>
> - Protective Security Roadmap Template

How information will be used by Government

The information provided in the organisation's report will be included in an assessment of the Cook Islands Government's progress towards meeting protective security objectives. The report should be submitted to the Chief of Staff, Office of the Prime Minister as Chair of the National Security Committee. It will form the basis of summary reporting to the National Security Committee. The Protective Security teams at the Office of the Prime Minister will use the information to:

- understand the current protective security capability of the Cook Islands Government and its overall progress against its protective security objectives
- plan required engagement and support for organisations
- inform verification activity.

The information provided will be treated according to the classification assign to it.

Any Official Information Act requests will be assessed on a case-by-case basis in consultation with organisations. The Protective Security team will transfer any requests for completed reports directly to the organisations concerned.

2.4 Building a security culture (GOVSEC-4)

GOVSEC-4
Build security culture

Provide regular information, security awareness training, and support for everyone in your organisation, so they can meet and uphold your organisation's security policies.

People are an organisation's biggest security strength and weakness. Ensure people are trusted to have access to official information and assets.

- Create a strong security culture
- Build security awareness
- Model good security behaviour
- Ensure compliance.

Create a strong security culture

In a strong security culture, personnel display an intuitive awareness of risk, security and trust in a way that attracts the respect of colleagues, the admiration of regulators and the ongoing trust of customers.

Evidence of a strong security culture can be observed if all personnel contribute to managing the problem. As well as complying with policy themselves personnel should be empowered to challenge colleagues who do not.

A simple example of the impact that senior leadership can have on security within an organisation is in the wearing of passes/identification cards. If leaders do not wear their passes/identification cards it sets a bad example and weakens the security culture of the organisation.

Lead by example. A good security culture relies on visible endorsement and engagement from the top.

Develop clear and fit-for-purpose security policies supported by training and regular communication.

Ensure people are clear on how to report a security incident, and on their responsibilities in managing and responding to security risks.

Establish transparent and accessible security policies, plans and procedures that address security risks including in the procurement and selection process for service providers and suppliers.

Consider including personal KPIs on continually developing individual security capability and the organisation's overall security performance.

Build security awareness

Design security awareness training and campaigns to:

- address the risks the organisation identifies during its risk assessment
- ensure the organisation's security policies and processes are followed
- promote personal responsibility for effective security by all staff and contractors, regardless of role or level of access.

Induction training

Start security awareness training as soon as new people join the organisation — make it a part of the organisation's induction programme. Induction training should cover protective security policies, procedures and security measures and include the information defined in the Protective Security Handbook:

- What is protective security
- Why security matters
- Protective security framework
- Good security behaviour
- How to protect information and assets
- How to report security incidents
- Specific security briefings to address your specific security policies and risks.

Provide refresher training regularly

Hold regular refresher sessions to remind people about security measures and let them know about any new measures.

Provide targeted training when the threat environment changes

When the organisation's threat environment changes or there's an increased risk of a security breach, provide targeted security awareness training on how to respond at different alert levels.

Provide training for people in emergency, safety, or security roles

Design extra training for people with emergency, safety, or security roles, so they can help to keep people, information and assets safe. These individuals play a key role in keeping everyone safe in times of emergency or heightened threat. Carry out exercises to help them practise their skills and confirm their ongoing competency.

Provide targeted training for people who face higher risks

Introduce targeted security awareness training and/or briefings for people who are regularly in elevated risk situations such as overseas postings, public facing or high-risk roles. If people and contractors work from home or travel around the Cook Islands and overseas, ensure they are always equipped to keep themselves and sensitive information secure.

Communicate effectively to enhance your security culture

To support security awareness training and culture, it is important to keep communicating about security measures. Some ways to keep security awareness high include:

- using security campaigns to address ongoing security needs or specific needs to do with sensitive areas, activities, or periods of time
- promoting security processes and tips through publications, electronic bulletins, and visual displays such as posters
- carrying out security drills and exercises
- including security questions in job interviews
- including security attitudes and performance in your performance management programme.

Keep a record of training participation and feedback

Keep a record of all participation in security training.

Request participants to complete a quality survey following the completion of training to assess the effectiveness of the training. Assess people's understanding of what they must and must not do before giving access to protected information and assets.

Review and use this information to ensure that everyone receives the appropriate training and briefings for their role.

Use security incidents as an opportunity to educate and learn from

Assess why non-compliance and poor behaviour occurs and use this to drive communication, education, and improve security measures that make is easier to detect, respond, and prevent security incidents.

To assess the effectiveness of the security training programme, ask the following questions:

- Did the individual(s) involved participate in the appropriate security trainings and/or briefings?
- Is the policy and/or procedure covered adequately in trainings and briefings?
- Are there patterns of non-compliance that signal needs for refresher training or improvements to existing training programmes?

MORE INFORMATION

- Managing security incidents (GOVSEC-7)

Model good security behaviour

Everyone plays a vital role in helping to protect organisational assets and keeping the organisation and its people safe and secure. By following good security behaviours, individuals will make a big difference to help reduce the organisation's vulnerability to threats.

- Understand and follow the organisations security policies and procedures
- Understand what information can and cannot be shared with whom
- Be aware of the surroundings when discussing or working with sensitive material
- Report any suspicious activity or security incidents.

This section describes the behaviours everyone should follow under different scenarios.

MORE INFORMATION

- Protective Security Handbook

Arriving and departing the workplace

Entrances and exits are the first and last point of protection for the organisation.

- Be alert to suspicious activity and report anything unusual
- Follow correct entry and exit procedures (e.g. swiping your pass, signing in) and ensure others do the same.

In and around the workplace

In the workplace, people need to be security conscious to minimise the chance of accidental breaches and to spot suspicious activity.

- Be observant for security incidents and report them no matter how minor they may appear – we only learn and improve through resolving incidents
- Don't discuss sensitive subjects or display sensitive information in areas where visitors are likely to be
- Clear desks of sensitive information at the end of the day – where necessary, lock it away
- Dispose of sensitive information appropriately
- Be aware of what to do when the organisation faces an increased alert level.

Receiving a visitor

Visitors can be a risk to security if not managed properly. Take responsibility for visitors when they are onsite.

- Verify the visitor's identity and confirm that their visit is expected
- Ensure visitors are signed in, out, and accompanied when appropriate
- Ensure visitors understand relevant security procedures
- Keep visitors away from areas they may not be authorised to go.

Handling queries

If regularly dealing with customers, partners or the public, be vigilant about security, even if the person is well known.

- Verify the person's identity before sharing information or working with them – don't make assumptions about their legitimacy or credentials
- Don't give away too much detail when requested – ask 'Do they really need to know this?'
- Be aware of how people may trick employees to get information.

Using computers and devices

Organisational ICT systems hold a wealth of information which can be a target of attack.

Using devices responsibly and securely can reduce the risk of cyber-attack.

- Use unique and complex passwords and change it immediately if it is suspected it has been compromised. Do not share passwords with others
- Lock the device or computer terminal when leaving it unattended. Protect mobile devices from loss or theft
- Be aware that electronic devices and media may contain viruses and malware that may affect the network
- Avoid using work devices and email for personal use
- Be cautious of free Wi-Fi networks.

Organisations online presence

In an increasingly digital world, organisations may conduct activities online. Increased digital presence can present an increased security risk if not managed well.

- Get official approval before posting anything online
- Be aware of becoming a target if linking with your organisation online.

Outside of work

Work lives inevitably spill over into personal lives such as in social situations or interacting online. These situations can put employees and organisations at risk.

- Keep personal and work lives as separate as possible
- Limit communication about any details of the sensitive work undertaken
- Report any suspicious activity or people trying to get sensitive information.

Travelling overseas

Employees are under greater risk when travelling overseas, whether personally or professionally.

- Consult with the organisation's security team to understand the risks and ensure staff and devices are secure
- Be aware of the environment, ensuring all conversations are conducted in a private and secure area and that devices and documents are always kept secure
- If it is suspected a device has been compromised, turn it off, and return it to the security team.

Hiring and managing others

Insiders are the biggest risk to the organisation. Ensure they are trustworthy to handle information securely.

- Undertake appropriate pre-engagement security checks when hiring
- Set the right behaviour expectations ensuring they attend induction, security awareness training and briefings and understand their responsibilities
- Model good security behaviour and watch for poor security behaviour from others
- When people change roles or leave the organisation, use robust procedures to manage their departure or change.

Procuring products and services

Often organisations rely on suppliers to deliver products and services. These suppliers become an extension of your organisation and broaden the risks you're exposed to.

- Understand the possible risks from suppliers – for example: insecure systems, malicious insiders, unknown supply chains, or sub-contractors with poor security practices
- Ensure suppliers understand their responsibilities to protect information and assets
- Assess the supplier and sub-contractor capability and personnel suitability before awarding contracts
- Build assurance and continuous improvement into contracts.

Monitor performance and compliance

Define security related performance measures for personnel, information, and physical security and establish mechanisms for measuring, monitoring and reporting against them. Consider conducting trend analysis to monitor effectiveness over time.

Treat all non-compliance with security policies, processes and procedures as a security incident. Ensure that all non-compliance is monitored, tracked, reviewed, and learned from as part of the security incident management process.

Establish robust procedures for dealing with poor security behaviour and incidents. Investigate non-compliance security incidents to confirm that security awareness training and campaigns are effective.

Enforce security policies visibly and quickly when employees, contractors, or suppliers do not comply.

2.5 Developing policies, processes and procedures (GOVSEC-5)

> **GOVSEC-5**
> **Develop and maintain security policies, processes and procedures**
> Develop and maintain security policies and plans that meet your organisation's specific business needs. Make sure you address security requirements in all areas: governance, information, personnel, and physical.
>
> Review your policies and plans every 2 years or sooner if there are changes in the threat or operating environment.

Communicate principles, policies and procedures clearly. Ensure policies are easy to understand and follow. If they are difficult or inaccessible, personnel will not comply and breaches or 'workarounds' will create security weaknesses.

Be prepared to enforce policies. To be effective, organisations must react to noncompliance, irrespective of the outcome. Non-compliance can easily become a habit, resulting in lack of respect for policies in general.

Policies and plans for protective security should:

- detail the objectives, scope and approach to managing security issues and risks
- be endorsed by the organisation's head
- identify security roles and responsibilities
- be reviewed when there are changes to the business or security risks or because of repeated security incidents

- be consistent with security risk assessment findings
- explain the consequences for breaching policies or circumventing protective security measures
- be communicated regularly.

Review policies and plans every 2 years, or sooner if changes in the threat or operating environment make it necessary.

To address priority security capability gaps, consider implementing systems, tools, and/or automation where needed to make it simpler for people to comply with policies and/or easier for security teams to monitor, detect, and respond quickly to security incidents and threats.

Consider implementing systems and processes for your employees and suppliers to regularly provide feedback and help optimising the security processes and procedures.

MORE INFORMATION

- National Protective Security Authority – Holistic Management of Employee Risk
- GCSB Information Security Manual
- SANS Information Security Policy Guidance
- CPNI Physical Security: Protecting my asset
- ASIO T4 Protective Security training

2.6 Working with others (GOVSEC-6)

GOVSEC-6
Manage risks when working with others

Identify and manage the risks to your people, information, and assets before you begin working with others.

Most organisations rely on others to manage their operations or deliver their products, systems, and services. Other organisations become an extension of a business and broaden the risks it is exposed to.

When undertaking a risk assessment, look beyond the organisation to others you work with or who provide products and services including suppliers and contractors.

Understand the security practices of others you work with. Ensure each organisation understands their respective security obligations. Assess how well others comply with security policies and practices.

What is a supply chain?

A 'supply chain' can be described as 'a network of organisations connected by a series of relationships involving the supply of goods or services.

Supply chains can be large and complex, involving many suppliers doing many different things. For example, some organisations may:

- outsource to a payroll provider whose systems are hosted in the cloud and maintained by another software provider
- partner with another organisation (for example, an NGO) to provide front-line services, and the partner in turn uses several providers to support their business.

Many organisations are not aware of all of the suppliers who make up their supply chain.

Securing a supply chain can be challenging because it can be difficult to identify vulnerabilities or recognise where they could be introduced and exploited.

The threats from an organisation's supply chain come in many forms. For example, a supplier may:

- fail to adequately secure their systems
- have a malicious insider working for them
- carry out malicious acts for their own gain
- use sub-contractors with poor security practices.

Or, the organisation may fail to clearly communicate its security requirements, so a supplier does the wrong things.

Once the risks faced by the supply chain are identified, organisations will assess them using the security risk management process.

Use a process to understand and manage risks

Organisations should:

STEP 1

Know who they do business with and understand the risks imposed

STEP 2

Define & communicate their protective security requirements to others they work with

STEP 3

Build security considerations into contracting processes and require suppliers to do the same

STEP 4

Meet their own security responsibilities as a supplier and consumer

STEP 5

Build assurance and support activities into supply chain management

STEP 6

Encourage continuous improvement of security within the supply chain.

> **MORE INFORMATION**
>
> - Supply Chain Management Handbook
> - Security Risk Management Handbook

2.7 Managing security incidents (GOVSEC-7)

> **GOVSEC-7**
> **Manage security incidents**
>
> Make sure every security incident is identified, reported, responded to, investigated, and recovered from as quickly as possible. Ensure any appropriate corrective action is taken.

What is a security incident?

A security incident is an event, breach, or attempted breach of protective security policies or procedures.

There are three different intents that can cause security incidents, accidental, negligent, or a deliberate act. Each of these can compromise the security of the public, your organisation, its people, information or assets.

ACCIDENTAL	NEGLIGENT	DELIBERATE
A failure to observe protective security requirements or policy.	A negligent or reckless action.	A deliberate malicious act.

Types of security incidents

The following examples highlight security incidents that might be seen to have a low impact, however, can quickly lead to incidents that have a high impact on the security of the Cook Islands Government, its people, information, or assets.

LOW IMPACT	MEDIUM IMPACT	HIGH IMPACT
• Key cards lost or left insecure • Classified material left in UNCLASSIFIED waste or • recycle bins • Classified material not properly secured or stored • Access doors wedged open for convenience without supervision that does not result in further harm • Unsuccessful attempt by someone seeking unauthorised access to information.	• Theft, attempted theft or loss of assets • Compromise or loss of classified information • Tampering with alarms, keys, windows, or doors • Suspicious contact from unknown individual • Suspicious email with attachments and links • Computer viruses • Information corruption • Disruption or damage to services or equipment.	• Physical event – e.g. perimeter, fire, water, • electrical • Social – e.g. public activity, event, protest • Espionage • Large scale cyber threat • Weather or natural events

Organisations need to provide their people with the guidance and resources to act in a timely, coordinated manner to prevent or respond to security incidents. They should develop and regularly test these procedures as part of their business continuity planning.

Reporting security incidents

It is everyone's responsibility to report incidents. When an incident happens, act quickly to reduce any impact and prevent further harm.

- Follow the organisation's incident reporting and response procedures.
- Report any incident no matter how minor it may seem
- Act quickly to reduce impact
- Learn from repeated infringements
- We all make mistakes, better to report incidents yourself than be reported on.

The security team maintains a register of all reported security incidents. Make sure they are kept aware and informed of all security incidents.

Include the following details when reporting a security incident:

- The date and time of the incident or when it was discovered
- The location of the incident
- Brief details of the incident
- What may have been compromised
- An initial assessment of damage or harm
- What actions have already been taken
- Who was involved in the incident, if known
- Your name and contact details for follow up.

If reporting an incident, ensure any updates or changes to the situation are reported.

For incidents requiring emergency service response (i.e Police, Ambulance, Fire) call 999.

> **Emergency services – 999**

For further support contact:

Chief of Staff, Office of the Prime Minister
nsd@cookislands.gov.ck

Investigating security incidents

A security investigation establishes what caused the incident and how far it compromised or threatened the security of people, information, or assets.

The purpose of a security investigation is to establish what has happened and how. It is not to establish whether a criminal offence has been committed, to aid prosecution, or to resolve employment or code of conduct disputes.

A security investigation focuses on establishing:

- the nature of the incident
- how the incident occurred
- what circumstances led to the incident
- who was involved
- the degree of damage to national security interests
- procedures needed to prevent a similar event or reduce its likelihood.

If a security investigation gives way to a criminal investigation, from then on procedures for a criminal investigation and for gathering evidence that is admissible in court need to be used.

Understand the likely outcomes of an investigation

Outcomes of an investigation may include:

- training/education
- changes to administrative or security policies, procedures, or practices
- security outcome, including potential loss of security clearance
- disciplinary action
- referral to an outside organisation for further investigation or prosecution
- dismissal of the disciplinary charge(s).

It is required to comply with the organisations policies and procedures while undertaking investigations and implementing measures.

The principles of procedural fairness apply to all investigations. People whose rights, interests or expectations are affected should be told the case against them and given an opportunity to be heard by an unbiased decision-maker.

The actions that result from an investigation must be fair.

Investigate and respond to incidents

When an incident happens, act quickly to reduce any impact and help the organisation recover as quickly as possible. Undertake a proper process for investigating the incident.

1. Set interim measures while an investigation is underway
2. Identify who needs to be involved and select an investigator
3. Set procedures for investigating security incidents
4. Plan the investigation
5. Undertake the investigation.

MORE INFORMATION

- Security Incident Investigation Handbook

Communicating with affected parties

Make sure that security incidents are communicated to affected parties for their action. If necessary, alert any relevant authorities.

Keep stakeholders informed as to the progress of the incident investigation and response and any residual risks they may be exposed to. It may also be necessary to actively warn people how to avoid harm.

Recovering and learning from incidents

Following the incident, it will be important to recover any lost information and assets if possible and reinstate normal business functions. Make sure the organisation learns from the incident so that it can improve security measures to prevent future incidents or reduce harm caused by incidents.

2.8 Being able to respond (GOVSEC-8)

> **GOVSEC-8**
> **Be able to respond**
>
> Be prepared to implement heightened security levels in emergencies or situations where there is an increased threat to your people, information, or assets.
>
> Maintain a business continuity management programme, so that your organisation's critical functions can continue to the fullest extent possible during a disruption. Ensure you plan for continuity of the resources that support your critical functions.

Planning how to respond

Be prepared to implement heightened security levels in emergencies or situations where there is an increased threat to people, information, or assets.

Sources of security risks fall into three main categories:

- **Event** – an important happening or incident that affects the organisation's ability to function. Examples include a weather event such as a storm or an emergency event, such as flooding, cyclones, fires.
- **Threat** – a declared intent and capability to inflict harm on people, information or property. Examples include cyber-threats or terrorism threats.
- **Activity** – an action by one or more people likely to have a negative impact on physical security. For example, protest activity, occupation or attempted occupation, or filming near your facilities.

If protective security measures are damaged or breached by an event or activity, or there is reliable evidence to support the possibility of a threat, then the alert level may need to be escalated.

Changing alert levels

Establish a plan, criteria and process for increasing organisational security alert levels as well as the criteria and process for returning to normal alert levels after a heightened event has concluded.

The table below defines the alert levels and identifies example responses that may be taken for each level. Consider these when developing response plans.

Alert level	Description	Response
GREEN	**Low Risk** A threat event is unlikely. No unusual activity exists beyond the normal concerns.	Normal – Continue normal operation and awareness. Localised incidents are managed through standard response procedures.

YELLOW	**Moderate Risk** A threat event is possible. Increased threat risk including weather, natural, physical, social, or cyber threats Increased risk of harm to staff or the public Risk of significant damage to critical infrastructure or IT systems.	Heightened – Prepare for event and establish countermeasures. Implement heightened responses for the specific threat as defined in your response plans. Example response actions are: • Doors in night mode / only allow authorised entry and exit • Plan, prepare and communicate with affected people • Issue event watch or advisory warnings to affected people • Increase monitoring of non-essential visitors or contractors • Heighten screening of mail and delivery • Increase monitoring of vulnerable infrastructure or IT systems • Address infrastructure and IT system vulnerabilities • Prepare for critical functions to transfer to alternative sites • Advise police, ambulance, or other emergency services that services may be required.

RED	**High Risk** A major threat event is imminent or has occurred and countermeasures are insufficient to prevent harm to people, information and/or assets Severe weather event or natural disaster Major internal incident such as fire, flooding, or cyber attack Potential for, or actual, loss of lives Widespread exploit, outage, or failure of critical infrastructure or IT systems.	Exceptional – Respond to event Implement your exceptional responses for the specific event as defined in your response plans. Example response actions are: • Strict access control measures in place • Lock down, evacuate or close facilities • Isolate, shutdown or enact disaster recovery of affected infrastructure or IT systems • Conduct essential operations at alternative sites • Make staff aware not to come to work • Communicate and coordinate responses; people understand how to respond • Request police, ambulance or other emergency services to respond • Prepare for recovery.

Draw on internal and external sources to plan responses

Seek information on risks from internal and external sources.

Internal sources

The organisation's overall risk assessment is an excellent source of information. Check the assessment and consult with business areas to learn more.

Business areas should be able to tell you about the business impact of disruptions to their operations, harm to their people, or the compromise or loss of information or assets.

Other important internal sources of information about risks are:

- protective security risk reviews

- security incident and staff reports
- security and operational risk registers.

External sources

External sources include any organisations that your organisation may work, partner, or co locate with. Do the other organisations have unique risk factors and how might they affect the combined business continuity plans?

Other examples of external sources of information that can be used are:

- Police, Emergency Management Cook Islands (EMCI) and Ministry Ministry of Infrastructure
- International cyber security threat centres
- Media reports.

Debrief after changing alert levels

A debrief can be helpful for improving response. Consider debriefing after every alert level change. A debrief should consider:

- why the alert level change was initiated
- how the alert level change was initiated
- what activity and actions were undertaken
- what and where, if any, improvements could be made to alert level procedures and communications.

Managing business continuity

Identify the organisations' priorities for business continuity. Identify what is needed to keep critical functions running or to restore them promptly if disrupted.

A disruption is anything that interrupts business-as-usual operations. Disruptions can occur at any time, for any reason, and their impact varies.

Causes of disruptions include natural events such as cyclones or flooding, loss of a key resource such as a power failure or supply chain disruption, and security threats such as cyber-attacks.

Why managing business continuity is important

A programme for managing business continuity helps to manage the impact of disruptions, regardless of cause. A successful programme includes:

- continual planning and improvement
- carrying out activities to ensure being prepared for disruptive incidents
- embedding business continuity into the organisation's culture and practice.

Process to develop a business continuity programme

Business continuity management follows an ongoing cycle to:

- set the scope and approach of the programme
- identify and prioritise critical functions
- develop plans to maintain critical functions
- setup teams to manage business continuity in a disruption
- run exercises to test plans and prepare for disruptions
- maintain the business continuity programme.

Set the scope of the programme

The scope defines at a high level the priority areas the programme will cover — not everything an organisation does as 'business as usual' can or should be maintained during a disruption. The scope of the programme should take into account the organisation's:

- legislative responsibilities
- overall strategy
- objectives
- structure.

When setting the scope, make sure it includes anything the priority areas depend on, such as supporting functions and resources.

Once a business continuity programme is established, review its scope regularly so it continues to reflect the organisation's responsibilities, objectives, and functions.

Identify and prioritise critical functions

CONSIDER RESOURCES AND REQUIREMENTS

Which resources and requirements are essential for maintaining critical functions?
Think about:

- people and their capabilities
- facilities
- supplies and equipment
- information
- technology (systems, applications)
- suppliers of goods and services.

CONDUCT A BUSINESS IMPACT ANALYSIS

Business continuity professionals use a technique called business impact analysis to identify business continuity requirements.

A business impact analysis can capture varying levels of detail. Consider the organisation's needs, and the stage it is at in implementing the programme. In the business impact analysis:

- Identify the requirements necessary to deliver the function
- Assess the impact of a disruption to the function and related timeframes
- At what point would the impact be unacceptable (the maximum tolerable period of disruption)?
- When is it targeted to recover this function by (the recovery time objective)?
- At what point are the identified requirements needed, so the recovery time objective can be achieved?
- Identify any other internal or external people, services, or suppliers that the function depends on
- Determine how critical the function is over time.

CARRY OUT A RISK ASSESSMENT

A business impact analysis should include a risk assessment to identify and quantify the risk of disruption to the function, including risks to the requirements the function needs. Collaborate with the people in the organisation who are responsible for risk management to carry out the risk assessment. Remember to consider risks that the organisation has already identified, and any measures for reducing them that are already in place.

Take a wide view

Collate and review the information from the business impact analysis, taking an organisation-wide perspective. Then consider:

- interdependencies between functions
- shared requirements across the organisation.

Develop plans to maintain your critical functions

DESIGN AND IMPLEMENT SOLUTIONS

Once the requirements for each critical function are identified, plan how to maintain or resume these functions if they are disrupted.

Consider the range of solutions that can be applied to each resource requirement, implement the preferred strategy, and address any gaps identified.

Solutions include:

- diversifying (for example, having separate facilities where the same activity occurs in parallel)
- replicating (for example, having people in another location who are trained and able to carry out a critical process, but don't do it as 'business as usual')

- using standby options (for example, maintaining an alternate facility that can be made operational within the recovery timeframe)
- acquiring a resource or service after an incident
- outsourcing the function to a third party
- having insurance
- using manual workarounds
- doing nothing.

To implement solutions, this may need supporting expertise or resources, such as information technology. Consider the organisation's context. It may require a cost-benefit analysis to help decide which solutions to pursue.

DOCUMENT YOUR PLANS AND PROCESSES

Create a business continuity plan to document the organisations' procedures for responding to a disruption of any kind.

The structure of business continuity plans depends on the organisation.

Small organisations may have all the information in one plan.

Larger organisations may have separate plans that cover different requirements or business functions. For example, a large organisation may have an overall plan which describes the business continuity scope and response procedures, and separate plans for business units, service locations, or specific functions.

An organisation's plans should cover:

- processes for notification, activation, and escalation
- roles, responsibilities, and authority for invoking the plan and responding to disruptions
- leadership continuity
- structures and processes for responding to disruptions
- details of critical functions:
    - requirements and timeframes
    - processes for maintaining the function, including where detailed operational procedures or plans can be found
- communication procedures (internal, external)
- any links to other plans and processes within the organisation.

Plans should be simple, fit for purpose, and easy to use under the pressure of a response situation. Use templates and checklists to make plans easy to use.

Remember to apply the chosen solutions to all the resources that support business continuity — people, facilities, supplies and equipment, information, technology, and suppliers.

Setup teams to manage business continuity and response in a disruption

PUT PROCESSES IN PLACE

Ensure response processes include:

- who will fulfil key roles in a response (strategic oversight, tactical, and operational roles)
- response priorities
- who is authorised to activate and manage a response, and who that responsibility may be delegated to
- notification, activation, and escalation.

CREATE TEAMS TO MANAGE STRATEGY, TACTICS, AND OPERATIONS

The organisation will need to consider its response structure at the strategic, tactical, and operational level.

For some organisations, one response team may manage all levels. In large organisations it may need to create separate teams to manage these responsibilities.

Hold regular exercises to ensure people know what to do, arrangements are fit for purpose, and to identify any gaps.

Strategic response team – crisis management team

- The strategic response team focuses on the issues from an organisation-wide perspective. The team is usually led by top management and is often called a crisis management team. This type of team needs to be flexible and involve experienced managers with the authority to apply the organisation's full resources to the response.

Tactical response team – the coordinators

- The tactical response team manages and coordinates the processes required to deliver critical functions and to ensure resources are appropriately allocated.

Operational response team – enabling continuity or recovery

- The operational response team keeps critical functions running or does the work to recover them.

Run exercises to test plans and prepare for disruptions

Systematically train for handling disruptions by running exercises. Test, assess, practice, and improve the organisation's plans for ensuring business continuity.

Exercises allow the validation of assumptions made during the planning process and identify issues or gaps in planning. Exercises also build the capability of response teams.

Run regular exercises as part of a continuous improvement process, so that capacity and capability can be gradually built over time.

The type of exercises chosen will depend on the exercise objectives. Each type of exercise requires a different amount of time to prepare and carries a different level of risk and cost.

Review and maintain response and continuity plans

Incorporate learnings from response and business continuity exercises into plans to continually improve response effectiveness.

Update plans to reflect any changes in the organisation including its goals, structures, plans, products, or services.

As part of the business planning cycle, consider reviewing and updating security response and business continuity plans to address the highest organisational priorities. Incorporate security improvements into the protective security programme.

3.0 Personnel security

This section has information and tools to help your organisation set up effective personnel security measures to protect your people, information, and assets.

Insider threats come from our past or present employees, contractors or business partners. They can misuse their inside knowledge or access to harm our people, our customers, our assets or our reputation. Personnel security focusses on reducing the risks associated with insider threats.

An 'insider threat', or 'insider', is any person who exploits, or intends to exploit, their legitimate access to an organisation's assets to harm the security of their organisation or the Cook Islands, either wittingly or unwittingly.

Common insider acts include:

- unauthorised disclosure of official, private, or proprietary information
- fraud or process corruption
- unauthorised access to ICT systems
- economic or industrial espionage
- theft
- bullying, violence or physical harm to others.

Many security breaches are unintentional and result from a lack of awareness or attention to security practices, being distracted or being fooled into unwittingly assisting a third party.

3.1 Managing insider risk

Reduce the risks from people within organisations by applying good personnel security practices.

Recruit the right person (PERSEC-1)

PERSEC-1
Recruit the right person

Ensure that all people working for your organisation (employees, contractors, and temporary staff) who access Cook Islands Government information and assets:

- have had their identity established
- have the right to work in the Cook Islands
- are suitable for having access
- agree to comply with government policies, standards, protocols, and requirements that safeguard people, information, and assets from harm.

Pre-employment checks are the foundation of good personnel security. They reduce the risk of a trusted person harming an organisation or business.

Pre-employment checks allow organisations to:

- confirm the identity, eligibility, and capability of the person they are recruiting
- find out if an applicant has concealed important information or misrepresented themselves.

Carry out pre-employment checks on everyone being considered for employment, including existing staff changing roles, contractors, and short-term staff. Do not skip pre-employment checks because of a person's background, work experience, or seniority.

Baseline pre-employment checks

Government organisations must carry out all of the following baseline checks at the pre-employment stage. The base pre-employment checks include:

- confirming their identity – sight source documents such as their passport
- confirming their right to work in the Cook Islands – confirm their nationality and their visa status and conditions
- checking their references with former employers – validate information that the applicant has provided and confirm their skills and character
- conducting a criminal record check – identify any history that could make them unsuitable for the role. For non-residents, consider whether you need to do an offshore criminal history check.

Additional checks for people requiring SECRET or TOP SECRET level access

When you identify that an individual will have access to SECRET or TOP SECRET information or has an increased security risk related to a specific role or the nature of your organisation's work, additional checks are necessary.

For example, for an IT administrator who has broad access to the organisation's information, take greater steps to ensure they are trustworthy and don't have factors in their life that would increase the risk that they could become an insider threat.

The additional checks that applied will depend on a range of factors including the organisation's operating environment, security context and culture. Undertake additional checks that give confidence in the applicant's trustworthiness and integrity for keeping sensitive information and assets safe.

Types of additional checks

- **Psychometric testing** – used to test skill levels in a variety of areas to give an analysis of the applicant's personality traits.
- **Financial check** – used to understand a person's financial history including their assets, liabilities, ability to service their debts, and uncover associations with businesses or associations.
- **Qualification check** – used to confirm a person's educational qualifications, professional memberships, or practicing certificates are legitimate and still valid.
- **Drug and alcohol check** – used to assess if a person may have an undisclosed addiction that could impair their judgement or ability to fulfil the role.
- **Personal references** – used to further assess the person's character and to test information that has been supplied by the applicant and by other referees. Note that you should not accept family members as personal references.

Mitigate any concerns

If there are any concerns arising from the pre-employment checks, assess the risks in relation to the role the person is being employed for and determine whether the risks can be mitigated.

It is good practice to record any concerns, risk assessments and decisions to mitigate risks.

If a person is being employed with any identified risks, work with them to create an individual risk management plan.

Set the right expectations

Set clear expectations about security. New employees, employees changing roles, and contractors, must understand security policies and practices as soon as possible after joining an organisation.

As part of your induction process, brief people on their responsibilities before disclosing information or granting access to classified information, assets, or facilities.

Agree to confidentiality

Have all people who will be given access to SECRET or TOP SECRET information or assets sign a confidentiality agreement or take an oath that clearly states their responsibilities and obligations which continue in perpetuity.

Formally grant and register security clearances

Formally grant security clearances and maintain an up-to-date register of all people who have been granted access to SECRET and TOP SECRET information and assets.

Ensure their ongoing suitability (PERSEC-2)

Effective pre-employment checks reduce the risk of threats to people, information and assets. However, people and their circumstances can change. Changes can happen over time or suddenly as a reaction to a particular event. Ensure that people remain suitable for having access to organisational information and assets.

> **PERSEC-2**
> **Ensure their ongoing suitability**
> Ensure the ongoing suitability of all people working for your organisation. This responsibility includes addressing any concerns that may affect the person's suitability for continued access to classified or unclassified information, assets and locations.

Because people and their circumstances can change over time, it is important to monitor changes and events that can affect people.

Ongoing security education helps to keep people, information, and assets safe from harm.

Baseline checks to ensure ongoing suitability

Monitor and assess security behaviour

Include security obligations and expectations as a component in personnel performance reviews. Assess the individual's security performance and behaviour in line with these obligations.

Ensure that security incidents are communicated to the appropriate people in the organisation and investigated. The investigation provides information to assess a person's ongoing suitability for using classified information and assets. It may identify needs for communication, additional training, or disciplinary action for repeated breaches and noncompliance.

Make all people aware of their responsibilities and the procedure for reporting security incidents.

Good communication between managers and employees, along with clear security expectations and procedures makes it easy for people to raise concerns, and report changes and incidents.

A manager must monitor a security clearance holder's behaviour for any concerns to do with security, poor performance, or unacceptable conduct. Monitoring also means watching for any signs that could suggest the person is unreliable or susceptible to pressure.

Develop and undertake processes for reviewing and possibly revoking security clearances and accesses as a result of disciplinary action.

MORE INFORMATION

- Managing security incidents (GOVSEC-7)
- Model good security behaviour

Monitor for insider threats

Whether malicious or negligent, insider threats pose serious security problems. Monitoring for common early indicators of insider threats is very important. Consider implementation of a formal insider risk management process to monitor and manage insider risks.

Managers and co-workers are in the best position to notice changes in a person's behaviour or attitude. Encourage your people to report what they notice and make it easy for them to do so confidentially.

Any form of monitoring involves collecting personal data. It must be collected lawfully and processed in a fair and proper way.

Negligent insider risks are managed through security awareness education, malicious threats are trickier to detect. However, there are some warning indicators that could lead to malicious insider attacks if not managed sensitively and appropriately:

- Decline in performance or attitude
- Missed promotions or poor performance appraisals
- Voicing disagreement with policies without engaging in the organisations processes to provide feedback for improvement
- Showing hostile or aggressive behaviour
- Experiencing financial distress
- Showing signs of drug or alcohol abuse, gambling, or illegal activity
- Unexplained wealth
- Using organisational assets and systems for personal use without authorisation
- Working outside the usual hours without a true need to do so
- Unnecessarily copies materials and/or removes material from the premises
- Shows interest in organisational matters outside their job scope and authority
- Unusual and unexplained foreign travel
- Resigning from the organisation (See PERSEC-3 for more information).

Provide ongoing security awareness

Organisations must provide ongoing security education to ensure the ongoing safety and security of everyone and to enhance their security culture.

Make security everyone's responsibility by increasing peoples understanding of security practices and processes. Communicate clear policies that explain each person's responsibility. Outline their compliance requirements and ensure that they understand their obligations.

MORE INFORMATION

- Build security awareness

Additional checks for security clearance holders

For people who hold a security clearance for access to SECRET or TOP SECRET information or has an increased security risk related to their specific role, additional ongoing checks could be necessary. The checks that are applied will depend on a range of factors including the organisation's operating environment, security context and culture.

Additional checks that can be considered for security clearance holders to ensure ongoing suitability include:

- requiring people to report any significant change in personal circumstances (e.g. a divorce, new partner, bankruptcy, foreign citizenship)
- requiring people to report any suspicious contacts
- encouraging people to report any suspicion of 'insider threat'
- carrying out an engagement survey to understand people's satisfaction and level of engagement
- briefing people on the risks related to international travel
- carrying out periodic criminal record checks with the Cook Islands Police Service or the Ministry of Justice
- carrying out periodic financial checks
- carrying out drug and alcohol testing.

Report significant change in personal circumstances

Significant changes in personal circumstances can arise from many different areas: relationships, finances, health, work issues, substance abuse, or new interests and contacts.

These changes can put people under pressure to act irrationally or inappropriately or make them more vulnerable to exploitation by others.

Reporting significant changes in circumstances will help you to manage any risk that an individual could intentionally or unintentional breach security or be coerced by an external party.

Employees should know which changes of circumstances they need to report and who they should report them to.

Report suspicious contacts or behaviour

Commercial, political or issue-motivated groups, foreign officials, and foreign intelligence services can devote considerable energy into accessing political, economic, scientific, technological, military, and other information.

Small pieces of information can all contribute to a valuable picture. Make sure your people understand that a seemingly innocent conversation or contact (e.g. email) may be part of an intelligence gathering exercise. Contacts can be official, as part of a person's role, social or incidental and could take place in a wide variety of contexts.

Employees should complete a contact report when a contact has occurred that appears suspicious, persistent or unusual in any respect, or becomes on going (whether in an official or social capacity) with:

- embassy or foreign government officials within the Cook Islands
- foreign officials or nationals outside the Cook Islands, including trade or business representatives
- any individual or group, regardless of nationality, that seeks to obtain official or commercially sensitive information they do not have a valid 'need-to-know'. This may include various types of social engineering such as phishing or tailgating.

Brief people on the risks related to international travel

When people travel overseas, for work or personal reasons, there is a risk they could be targeted by foreign intelligence services aiming to get access to confidential information.

To protect the organisation and the Cook Islands interests, brief travellers on the risks and the security measures they need to take.

They should:

- consult the CSO, or their delegate, before travelling to check if a security briefing is necessary
- know what methods foreign agents may use to gather information
- understand how to protect the organisation's information
- know what information they must protect
- know what information they can share and trade
- be aware of how to manage electronic equipment.

Manage role changes

Reassess the personnel security implications whenever a change occurs to a person's role, location or responsibilities.

It is common for people to enter an organisation in one role then move to another role with greater responsibilities and a higher risk profile. Not completing the appropriate checks for the new role because the person is 'known' to the organisation increases the risk of problems.

Make sure that all required pre-employment checks and/or on-going suitability checks have been completed to the level required for the new role before they are confirmed in the role.

Support staff with high-risk positions

In line with organisational Health and Safety process, establish mechanisms to support people in higher-risk positions or vulnerable situations to help them understand and manage their security risks.

Managing their departure (PERSEC-3)

PERSEC-3
Manage their departure

Manage people's departure to limit any risk to people, information and assets arising from people leaving your organisation. This may include:

- remove access rights to systems and buildings
- ensure property is returned
- ensure people understand their ongoing obligations.

When a person leaves the organisation, they retain their knowledge of the business operations, intellectual property, information, and security vulnerabilities. Managing their departure well will reduce the risk of this knowledge being misused.

Whether a person is leaving by choice or not, a positive exit experience reduces the risk they will misuse their knowledge of operations, intellectual property, official information, or any security weaknesses.

Baseline departure activities

Remove access rights

Before a person leaves the organisation, remove their access to electronic resources, physical resources, and physical sites.

Collect security passes and keys

Make sure the departing person returns all identification cards, keys, and access passes, including any tools that allow them remote access to information management systems.

Make sure assets are returned

A departing person must return all property that belongs to the organisation. Take particular care with your intellectual property, physical assets, and official information.

Additional departure activities for security clearance holders

For security clearance holders or anyone with a higher risk role or personal circumstance, consider asking them to:

- complete an exit debrief or interview
- transfer or revoke security clearance
- sign a deed of confidentiality.

Conduct exit interviews

In addition to their broader function exit interviews provide the opportunity to remind the departing person of their obligations to protect the organisation's information.

Exit interviews are also a good opportunity to allow the affected individual to:

- discuss their reasons for leaving, and their attitude to the organisation and people
- surrender any passes or access cards they hold.

Use a deed of confidentiality if the risk is high

A deed of confidentiality may be necessary to protect the organisation's proprietary information or intellectual property.

3.2 Managing contractors

Giving a contractor access to organisational information and assets comes with the same security risks as for permanent employees, and some extra risks.

To protect information and assets:

- use the same personnel security measures with contractors as you would with permanent employees
- consider extra measures to counter the security challenges that contractors can present.

Extra security challenges with contractors

Before employing contractors, assess the risks and create a plan to address them. Be mindful of the following security challenges.

Level of loyalty

A contractor's main loyalty may not be to the organisation, so their commitment to security measures may not be as strong.

Sense of inclusion

A contractor may not feel fully part of the team they are working in, which can lessen their sense of responsibility for applying security measures.

Competing interests

A contractor may work for a competitor before, during, and after their contract with the organisation.

Extended contracts

Contracts can be renewed or extended to the point where a contractor can work in the organisation for many years, often with little or no re-screening.

Moving around your organisation

A contractor might move from one area of the organisation to another. Without a security handover, the contractor might not be aware of the security controls in the new area. The manager of the area they move to also needs to know what security measures are in place for the contractor.

Less support

An organisation might not see the same responsibility to provide assistance, welfare support, or monitoring to a contractor as to permanent staff. A contractor may have less commitment to the organisation if they feel unsupported.

MORE INFORMATION

- Working with others (GOVSEC-6)

3.3 Managing security clearances

Maintain a register

Once someone has been formally granted a security clearance to SECRET or TOP SECRET information, maintain an up-to-date register of all security clearance holders. Include information about who has been cleared, their access level, any restrictions or caveats applied to the clearance, date cleared, their position, and manager.

Review and maintain this register when there are changes to the individual's role, their clearance level, or when the clearance is transferred or revoked. Ensure that their system and facilities access rights are maintained in parallel.

Review every five years

Consider reviewing security clearances after five years or sooner if clearance restrictions were applied when granted.

The clearance holder's manager is responsible for managing the process to ensure that the holder maintains their security clearance. The manager should undertake additional security checks to confirm their continuing suitability to hold a security clearance.

MORE INFORMATION

- Additional checks for security clearance holders

Suspend, revoke or transfer security clearances

Establish processes for suspending access, revoking clearances and access, or transferring clearances to another Government organisation.

Suspend access

If the clearance holder is being investigated for a security violation, their manager should suspend their access to protectively marked information or resources until the investigation is complete.

Revoke a clearance

A HOM may recommend the revocation of a national security clearance to the National Security Directorate (NSD) if the HOM considers a clearance holders breaches, or violations, of security are too frequent or of a sufficiently serious nature.

When a clearance holder leaves the organisation, you must either revoke the clearance or transfer it to another Government organisation if appropriate.

Transfer a clearance

Consider establishing a process for transferring clearances across Government organisations. These processes should be reported and recorded by the NSD.

If a clearance holder is transferring to another Government organisation and their new role requires access to SECRET or TOP SECRET information within the new organisation, it is possible to transfer their clearance if the clearance was granted or renewed within the last 5 years.

The HOM, or their delegate of the new Government organisation must request and obtain from the clearance holder's previous employer:

- Results of the latest security checks undertaken
- CSO's written assurance of the person's continuing suitability to hold a national security clearance.

Granting emergency access without a security clearance

Consider establishing a formal process to allow a HOM or their delegate to assess and grant emergency access to SECRET or TOP SECRET information or assets without having undertaken the appropriate security checks. The NSD must be notified if this access is granted.

What does "emergency access" mean?

- Access where an urgent and critical operational need for access to particular material is established and there is insufficient time to complete the security checks and grant a security clearance
- Access only to specified material required for the particular emergency
- Access for no longer than the duration of the emergency
- Access governed by a very strict application of the need-to-know principle.

Example process

1. A risk assessment is conducted to define the access requirements and risks and agree the mitigations to manage the risks.
2. A permanent record is kept of the names of the individuals given emergency access, the reason for the emergency, the materials and assets required, the date and duration of the emergency, the names of the security cleared supervisor and other personnel involved in the emergency.

3. The approval is given and signed by the HOM or their delegate. The signatory is accountable for ensuring the safety and security as a result of the emergency access.
4. Access is continually supervised by an appropriate security clearance holder.
5. Access is removed at the expiration of the granted period or earlier when the job is completed.

4.0 Information security

Ensure the confidentiality, integrity, and availability of information is protected within your organisation.

Implement the Cook Islands Information Classification System within the organisation and ensure proper handling of information in line with its classification.

Protect organisational information with robust security practices. When information security controls are well designed and implemented, they reduce the risks of information being compromised.

Encourage a strong security culture, so that information security practices are known and followed.

Design and maintain robust information security

Establish an information and cyber security framework and policy that identifies the information risks across the organisation and applies appropriate security measures.

Monitor for security events and establish procedures for responding to them. Conduct regular reviews to incorporate changes in technology.

Share information securely

Ensure everyone including contractors, suppliers, and other organisations that handle (create, send, receive, store, or dispose) organisational information are clear on their obligations to protect it.

4.1 Cook Islands Information Classification System

Protective markings help to keep official information secure. They're a visual reminder of the security measures that apply to information or equipment.

Who should mark information and when

The person who creates the information is the 'originator'.

The originator is responsible for assigning a protective marking when the information is created.

If the level of protection changes during the drafting process, the originator should adjust the protective marking.

When the draft is final, the originator must confirm that the protective marking is at the right level to keep the information secure.

Classifying information

The classification and additional markings should be added as following to all documents:

- Centred top and bottom of each page
- All Caps
- Bold
- In the following colours:

OFFICIAL	RESTRICTED	SECRET	TOP SECRET
Marking is optional	Black	Blue	Red

When printed documents are filed, their protective markings should be clearly visible on the front and rear covers of files or containers. The same rule applies to removable electronic and optical media, such as USBs, CD-ROMs, microfilms, photographs, and removable hard drives.

Marking paragraphs

Sometimes paragraphs may need to be marked because they have different or higher security needs. For example, a paragraph in a document might contain SECRET information. Paragraph markings are called 'paragraph grading indicators'.

Organisations should consider developing a policy on protectively marking paragraphs within documents that require security classifications.

Applying paragraph grading indicators

Put paragraph grading indicators in brackets at the beginning of each paragraph. Write them in full or abbreviate them using the first letters of the security classification. For example, (S) for SECRET or (R) for Restricted. Table 1 shows the standard abbreviations you can use.

Paragraph grading indicators should be the same colour as the text in the document.

If you use paragraph grading indicators, you must also mark all the paragraphs in the document, so that no one is confused about which markings apply to what text.

Use UNCLASSIFIED for paragraphs that don't carry a protective marking.

Table 1: Abbreviated security classifications

UNCLASSIFIED	(U)
OFFICIAL	(O)
RESTRICTED	(R)
SECRET	(S)
TOP SECRET	(TS)

Additional protective markings

Additional protective markings can be applied to warn people that the information has specific handling requirements in addition to its overall classification.

You must not use additional markings without a security classification.

When a document needs an additional marking:

- put the security classification at the top and bottom of the page, e.g. RESTRICTED
- put the additional marking below the top security classification at the top of the document and above the bottom security classification at the bottom of the document, e.g. CABINET

An additional marking should always be in the same size, format, and colour as the security classification.

Following are a small set of standard additional markings. Organisations need to define the additional set of protective marking relevant to your requirements.

COOK ISLANDS EYES ONLY

- Used for material where access to information is restricted to Cook Islands residents with an appropriate security clearance and on a need-to-know basis.

CABINET

- Used for material that will be presented to, and/or require decisions by Cabinet.

[DEPARTMENT] USE ONLY

- Used for material intended only for use within the specified department(s).

PERSONAL

- Used for material relating to an identifiable individual, where inappropriate access could have damaging consequences.

COMMERCIAL

- Used for commercially sensitive processes, negotiations, or affairs.

LEGAL PRIVILEGE

- Used for material that is subject to legal privilege.

Don't mark titles

Whenever possible, don't put protective markings on titles of things like files, documents, books, and reports. They could be seen in management systems that aren't protectively marked, and this could put the information at risk.

If marking the title is essential, the originator should use a separate UNCLASSIFIED reference. This mark can appear behind the title in brackets.

Marking printed graphics

For graphics such as maps and drawings:

- print or stamp the protective markings near the map scale or drawing numbers
- print the protective markings at the top and bottom centre of the graphic.
- If the graphic will be folded, make sure the marking remains visible after folding.

Marking annexes, appendices, attachments, and covering documents

In some cases, the annexes or appendices to a document need protective markings even if the rest of the document is UNCLASSIFIED.

Occasionally, an annex or appendix may also need a different protective marking from the principal document it is attached to.

If the annex, appendix, or attachment has a higher protective marking than the principal document, the document's front cover should indicate that the document as a whole has a higher security classification.

If the annex, appendix, or attachment is at the same protective marking level as the principal document or lower, you don't need to show that on the cover.

Marking imagery

Photographs and film, and their storage envelopes or containers must all carry clear protective markings when applicable.

Protective markings must be:

- on both sides of containers and spools
- projected for at least five seconds in the title and end sequences of roll imagery, cinefilm, and video tape.

You must also mark photographic negatives, so that the protective marking is reproduced on all copies made from that negative.

Marking presentations

Official presentations with security classifications need appropriate protective markings.

Treat each slide or screen as an individual page, as you would for a paper-based document. The protective marking should be verbally stated to the audience.

Marking audio

For audio recordings, the level of protective marking must be clearly stated at the beginning and end of each recording. The tape or other media and its container must be conspicuously labelled with the appropriate protective marking.

Marking emails

Emails should be marked with an appropriate protective marking in line with the classification system. Marking emails ensures that:

- appropriate security measures are applied to the information
- helps to prevent information being accidentally released into the public domain.

Ensure that emails containing COOK ISLANDS EYES ONLY or other nationality marked information are sent only to named recipients and must not be sent to distribution lists or groups unless the nationality of all members of the distribution lists can be confirmed.

When an unmarked email has been received, the organisation must assess the information and determine how it is to be handled in accordance with the classification system.

Personal emails should not be classified as they are not official government information.

Consider configuring systems so that protective markings appear at the top and bottom of every page when an email is printed.

MORE INFORMATION

- NIST Guidelines on Electronic Mail Security

Marking equipment and storage media

Organisations must develop specific procedures for marking equipment and electronic storage media. Applying protective markings to assets assist in determining the appropriate usage, disposal and destruction requirements of the asset. Organisations should clearly label all IT equipment and media capable of storing protectively marked information. Protective markings should be clearly visible and not easily removed.

Develop procedures for reclassifying and declassifying media in the event that the media is not classified correctly or where the information classification stored has been changed.

MORE INFORMATION

- New Zealand Information Security Manual
- ISO/IEC 27001:2013

Classified document register

A Classified Document Register (CDR) records the creation, ownership, location, and destruction details for all TOP SECRET information produced, copied, or received by the organisation.

Organisations may also choose to use the CDR for SECRET information and for risk mitigation of lower classified information.

Handling information

Following are the requirements for storing, filing, using, transporting, and disposing of classified material.

Dealing with oral information

If information that carries a protective marking is delivered orally (for example, through classified discussions), the recipient(s) must be told that the information needs protection before the information is conveyed.

Receipting process

Consider having a receipt process for when protectively marked information or equipment is delivered to an organisation. The benefits include being able to:

- provide confirmation that information has been delivered
- trace the movement of protected information
- ensure the recipient takes responsibility for protecting the information.

Any type of receipt mechanism is suitable, as long as it identifies the document either by reference number or title.

A reference number is often easier than a title, as the title of a document may describe the content of a protectively marked document or, in limited cases, contain a word such as 'secret' or 'confidential'.

Specify a period on the receipt (for example, 7 days) in which the recipient must sign and return the receipt.

Confirm all expected receipt returns are received within a month of their due date.

Store and file

Below are the requirements for storing and filing sensitive information in an organisation based upon its classification.

OFFICIAL

- Stored in any area commensurate with the sensitivity of the information
- Physical folder is uncoloured.

RESTRICTED

- Stored in Work Area under single barrier and/or lock and key
- While in use, material / equipment is not left unattended – secured and/or locked away
- Physical folder should be marked

SECRET

- Stored in locked cabinet in Work Area or Security Area using approved security furniture
- Physical material is immediately placed in a folder
- Physical folder should be marked

TOP SECRET

- Stored in a strictly controlled, locked, and monitored Security Area (e.g. strong room or safe)
- Physical material is immediately placed in a folder
- Physical folder should be marked

Adding information to a file

Organisations should use a file reference and folio number for protectively marked files to maintain a record of the information held on the file. It is also considered good practice to follow normal filing procedures, such as recording the date and name of the person holding the file.

When new information is added to a file, the file user must ensure that the protective marking is still appropriate. If information is added that is at a higher security classification than the file itself, the file user must reclassify the file before attaching the new document.

The protective markings on files must be clear and easy to distinguish from other markings. If possible, use the standard colours for file covers on your protectively marked files.

Use, copy or share

Below are the requirements for using, printing, copying and sharing sensitive information in your organisation based upon its classification.

OFFICIAL

- Clear desk and screen policy to protect against accidental or opportunistic compromise
- Obtain owner approval prior to printing, copying or sharing
- Sensitive materials should be kept to a minimum
- Social media and online sharing are not permitted except through approved communication and media authority.

RESTRICTED

Including OFFICIAL requirements:

- Printing, copying or sharing may be prohibited by the originator

- Confidential conversations and meetings held only in approved and secured areas
- Copies should not be left unattended on printers and devices.

SECRET

Including RESTRICTED requirements:

- Consider recording copies in CDR
- Shared only with people with appropriate security clearance and valid need to know
- Secure telephones, video, conference equipment
- Material assessed for redaction before disclosure • Printers and devices are secured before use.

TOP SECRET

Including SECRET requirements:

- Accessed only within an approved security area
- All copies in any form (e.g. physical, electronic, media) are numbered, recorded and tracked in CDR
- Disclosure assessment undertaken before approval given
- Approval authorising copying, printing, or sharing recorded in original file
- Printer and device access and use is strictly controlled and supervised.

Copying guidance

To help control protectively marked information, keep the number of copies to a minimum. Only reproduce protectively marked information when necessary.

To make copies of protectively marked information with a copy number, it is required to get permission from the originator or originating organisation (the person or organisation that created the information). However, it is better to ask the originator to supply any additional copies that the organisation needs.

If the originator gives permission to make copies, let them know how many copies are intended to be distributed. The originator will then advise which copy numbers need to be marked on the copies.

USING PHOTOCOPIERS, FAX MACHINES, AND SIMILAR DEVICES

Organisations should develop a policy for use of photocopiers, fax machines and similar devices. Devices used to copy and transmit protectively marked documents come with risks that must be understood and managed.

Photocopiers, fax machines and similar devices, known as multi-function devices (MFDs) may:

- retain images of copied documents that can then be transmitted

- be connected to ICT systems that do not have the necessary level of protection.
- To reduce risks when coping and transmitting protected information take the following steps:
- Put approved devices in an area where you can observe all copying and transmitting activity.
- Make sure a designated person stays near the device until all activity is finished.
- Make sure documents are removed from the device as soon as activity is over.

Remove or Transport

Below are the requirements for removing or transporting information from an organisation.

OFFICIAL	RESTRICTED	SECRET	TOP SECRET
Authorised by owner of the information. In accordance with organisation policies and procedures.	Including OFFICIAL requirements: Authorised by the originator (may be the same person as the owner).	Including RESTRICTED requirements: Authorised by the CSO.	Including SECRET requirements: Authorised by the Chief of Staff, Office of the Prime Minister as Chair of the National Security Committee.
REMOTE WORKING			
		Including RESTRICTED requirements: Risk assessment to determine need and identify appropriate security controls Approved security storage.	Including SECRET requirements: Exception is granted and risks have been accepted by senior management.

REMOVABLE MEDIA			
Can be used based on your organisation's policies.	Appropriately encrypted.	Appropriately encrypted.	Appropriately encrypted.
MOVING BY HAND			
Does not require special enveloping or folders within physical location Single envelope between locations for sensitive material.	Single envelope Must always be in personal custody of an authorised person.	Double enveloped and sealed in a tamper-evident manner Evidence of receipt.	Movement recorded in CDR.
TRANSPORTING BY POST/COURIER			
Single envelope Include specific addressee and return address Never mark classification on envelope.	Consider reputable mail or courier with 'track and trace' service.	Double enveloped and sealed in a tamper-evident manner Approved government or commercial courier Track and trace or evidence of receipt.	Do not send by post or courier. Transport by hand only.
TRANSPORTING OVERSEAS			
Single envelope Include return address	Consider reputable mail or courier with 'track and trace' service.	Double enveloped and sealed in a tamper-evident manner	Security cleared diplomatically accredited courier only

Never mark classification on envelope.		By authorised person only (with appropriate security clearance) or diplomatically accredited courier Track and trace or evidence of receipt.	Movement recorded in CDR.
ELECTRONIC TRANSFER (e.g. email, internet, online app)			
Communication of recipient's legal and destruction obligations if the incorrect party receives it.	Risk assessed Password protection and encryption may be required.	Appropriately encrypted. Evidence of receipt.	Appropriately encrypted. Movement recorded in CDR.

Transporting guidance

If an organisation wants to take (remove) protectively marked information from its premises, it must have policies and processes in place to ensure it is protected. Protected information might need to be taken to another organisation or workplace for a meeting or to work from home.

Protected information should only be removed from premises when:

- there is a definite need
- the right level of protection can be maintained on route and at the destination.

Removing protected information

Before anyone in an organisation takes protectively marked information from secure or authorised work areas, they must have approval.

Take special care when organisation employees plan to take protectively marked information overseas. It can be exposed to far greater risks, so more security measures are necessary.

Authorising removals

The organisation decides who can authorise removals. However, it should be the manager or equivalent person responsible for the information who gives approval.

The approver must:

- be satisfied that a genuine need exists
- brief the person removing the information on the risks involved
- be satisfied that there are adequate arrangements for the safe custody of the information
- be prepared to accept responsibility for the safe custody of the information.

Make sure to keep a record of all removals at TOP SECRET and SECRET levels.

Carrying protectively-marked information securely – briefcases and satchels

When protectively marked information is transported outside of an organisation in an approved briefcase or satchel, you must place it in an opaque envelope within the briefcase.

The briefcase or satchel must be:

- locked at all times
- kept under the personal protection of the custodian.

To prevent keys being copied or locks being manipulated:

- do not leave the keys in the lock
- lock the briefcase or satchel, even when it is empty.

Protecting electronic media

It is a requirement to protect electronic media, such as laptops, CDs, and USBs, used to process protectively marked information to the same degree as paper-based materials.

The level of protection must be equivalent to the highest level of protectively marked information ever placed on the media until it is sanitised.

Working away from the office or off-site

For regular and long-term arrangements for people working away from the office, refer to information on Working away from the office.

Sometimes arrangements might be needed for information to be transferred to a secured site such as a regional or branch office rather than allowing it to be taken to a place where you cannot guarantee its security. For example, keeping protected information in a hotel room overnight might not be secure enough in some cases.

Transporting guidance

You must use security measures to protect protectively marked information when it is in transit.

Measures can include:

- using approved briefcases, satchels, seals, pouches, or transit bags
- using special enveloping procedures
- transferring information by hand between people with the appropriate security clearance or by authorised messengers.
- Security methods can be used together to create tighter security. For instance:
- using an inner and outer envelope — double enveloping
- combining an inner barrier with an outer barrier — the 'double barrier' method.

Whichever combination you use, the inner barrier must be tamper evident and the outer barrier must obscure the nature of the information being transferred.

Addressing information correctly

Address protectively marked information to a specific position, appointment, or named individual.

Make sure the addressee and alternative have the required level of security clearance.

Specify the intended recipient's name, designation, and full street address.

Do not send protectively marked information to a post office box.

For TOP SECRET information, provide an alternative individual or appointment.

It is recommended that this approach is used for protectively marked information classified below TOP SECRET.

Transferring information within your office

Protectively marked information can be transferred within a discrete office environment without any coverings, such as envelopes, when:

- the information is transferred directly between staff who have the appropriate level of clearance to access it and the need-to-know
- there is no opportunity for unauthorised people to view the information.

If there is a risk that an unauthorised person could view the information, it must be covered.

Double enveloping

A double barrier must be used to transfer protectively marked documents securely outside an organisation.

Double enveloping is used to help protect the need-to-know principle when transferring protectively marked information.

Double enveloping provides evidence of tampering. As the name suggests, double enveloping consists of placing protectively marked information in two sealed envelopes.

Organisations must use double enveloping for all information classified as SECRET and TOP SECRET when delivering by hand or using an approved courier.

Use double enveloping at your discretion for information classified as RESTRICTED. Use your security risk management plan to inform decisions.

RESTRICTED information or material should be double enveloped when it is sent by post or commercial courier.

INCLUDING RECEIPTS

Double enveloping must be used along with receipts that:

- are enclosed with the protectively marked documents
- identify the date and time of dispatch, and the dispatching officer's name
- have a unique identifying number.

GETTING THE OUTER ENVELOPE RIGHT

Use the outer envelope in a similar way to normal mail envelopes. It gives protection to the inner envelope.

The outer envelope must not:

- display the protective markings of the document
- use tamper-evident seals.

The outer envelope must display:

- the physical address of the recipient
- a distinct reference number (this may be the receipt number if the envelopes are not individually numbered)
- the name and signature of the dispatching officer
- the date of dispatch.

GETTING THE INNER ENVELOPE RIGHT

The inner envelope is used to give evidence of tampering.

The inner envelope should:

- display the protective markings at the top and bottom, and front and back of the envelope
- be sealed with an approved tamper-evident seal in such a way that covert entry to the envelope is countered.

Methods for transferring protected information

Your organisation should choose the transfer method that best achieves the safe transfer of protected information.

Using the 'Safe hand' method

The 'safe hand' method is when information with protective markings is despatched to the addressee in the care of an authorised officer, or succession of authorised officers, who are responsible for its carriage and safekeeping.

At each handover, a receipt is obtained showing at least:

- the identification number of the package
- the time and date of the handover
- the name and signature of the recipient.

The purpose of sending an article using safe hand is to establish an audit trail that allows the sender to receive confirmation that the addressee received the information.

To send information using the safe hand method:

- enclose it in a double barrier (double envelope it)
- give it a unique identification number (usually the receipt number)
- place a two-part receipt in the inner envelope with the information — the addressee keeps one portion and signs it and then returns the other portion to the sender
- ensure some form of record or receipt system accompanies the package, so that every handover is documented
- transport the information in an approved briefcase or mailbag
- ensure the information is not left unattended, except when placed in the cargo compartment of an aircraft.

USING COMMERCIAL COURIERS OR POSTAL SERVICES

When no authorised messenger or safe-hand courier service exists, an organisation may allow material classified RESTRICTED to be carried by signature-required commercial courier.

Only commercial couriers that have been approved by the organisation must be used to carry SECRET material.

GENERAL GUIDELINES

- **Receipts:** information sent via commercial courier or postal organisation must be accompanied by a receipt. The receipt must be signed by the receiving organisation and returned to the sending organisation.
- **Packaging:** For carriage by commercial courier, the courier satchel itself when opaque can stand as the outer envelope. Envelopes and wrappings need to be robust to stand up to the wear and tear of transit.
- **Dispatch and delivery:** Do not leave protectively marked information unattended while awaiting pick-up by courier.

Do not dispatch protectively marked information before weekends or public holidays unless the addressee is able to receive it the following day and secure it appropriately.

Check delivery documentation to ensure items arrive within expected timeframes.

If there has been an undue delay or there is any sign of tampering, both the sending and receiving CSOs should be notified.

WHEN YOU CAN'T USE A COURIER

TOP SECRET material must not be carried by a commercial courier or postal organisation. Special handling requirements that apply to information carrying endorsement markings may also preclude the use of a commercial courier.

Information marked with the COOK ISLANDS EYES ONLY additional marking must be transferred according to its level of security classification.

The requirements for other additional markings are established by the organisation.

DEALING WITH BULKY MATERIAL

Generally, when the size and weight of material means it can't be moved using the safe hand method or commercial couriers, you need to take special precautions to ensure the material is not compromised, lost, or damaged in transit.

Seek advice from your CSO.

DEALING WITH HIGH-RISK UNCLASSIFIED MATERIAL

If required to transfer valuable material, such as artwork or money, to another organisation, commercial courier services can be used.

However, take care to assess the courier service first. Make sure it is legitimate, reliable, and can offer the right level of protection for the risks identified.

Ensure any legislative requirements that apply to the material are met.

Whenever possible, avoid drawing attention to the specific nature of the material being moved.

Extra security steps might be necessary in some circumstances. Steps such as:

- sealing the material
- security clearing the employees of the courier service
- arranging a security or police escort.

RECEIVING HARD COPIES

Before allowing anyone in the organisation to receive hard copies of protectively marked information, make sure they are aware of their responsibilities and, when necessary, hold the appropriate security clearance.

Protectively marked documents should only be opened by the addressee or the alternative addressee. However, the organisation HOM may authorise a specified person or area to open all mail and perform the related information or security management functions.

When someone other than the intended addressee is charged with its opening, adopt the normal practice of opening the outer envelope only. The inner envelope should only be opened in the presence of the addressee.

The recipient of a package containing protectively marked documents must verify that the:

- information was transferred by the appropriate means
- seals and packaging are still intact.

Report any breakages, signs of tampering, or inappropriate transfer methods to the CSO and the CSO of the sending organisation.

The recipient must check that the contents and their integrity are preserved. For example, check the pages and table of contents, and sign and return any receipt accompanying the information.

If the organisation keeps a register for protectively marked documents, make sure the information is registered.

TRANSFERRING ELECTRONIC DATA

• Communication of • recipient's legal and destruction obligations if the incorrect party receives it.	• Risk assessed • Password protection and encryption may be required.	• Appropriately encrypted. • Evidence of receipt.	• Appropriately encrypted. • Movement recorded in CDR.

Organisations must establish a policy and procedure for transferring protectively marked information to prevent information and privacy breaches.

Data can be transferred electronically using various means including email, system-to-system gateways, and removable media. Conduct a risk assessment of ICT systems and methods used for data transfer to understand the risks and needs for security controls.

Establish security controls to protect the information during transfer. Consider how to control information transferred:

- between higher classified systems to lower classified systems and assets
- over the internet, email, or cloud-based applications
- via removable media such as USBs, removable hard drives, etc.

Consider requirements for encryption of information both at rest and in transit. Encryption of data in transit can be used to provide protection for information being communicated over insecure mediums and reduce the security requirements of the communication process. Review best practices in cryptography for more information.

MORE INFORMATION

- GCSB NZISM Cryptography
- OWASP Guide to Cryptography

Archive or disposal

Below are the requirements for archiving and disposing of information in your organisation based upon its classification.

OFFICIAL	RESTRICTED	SECRET	TOP SECRET
• Archival of public records is subject to the Public Records Act • Dispose with care using approved commercial disposal products and services.	Including OFFICIAL requirements: • Physical waste should be kept separate from unclassified waste and secured under same precautions as Filing / Storing • Must not be disposed by standard rubbish or recycling	Including RESTRICTED requirements: • Use only approved service providers, products, and destruction processes • Media that has held SECRET information must be declassified by approved declassification	Including SECRET requirements: • Verify material is complete (all pages) • Media that has held TOP SECRET • information cannot be declassified and must be sanitised and destroyed by approved disposal process

	collection unless it has already been through an approved • destruction process (e.g. shredding, pulping, burning, disintegration) • Disposal of electronic media should make reconstruction highly unlikely.	and disposal processes.	• Supervise and witness destruction by an authorised • officer • Disposal is recorded in CDR.

Disposal guidance

Use approved procedures for destroying ICT media and documents with protective markings. These requirements apply to all information (with or without security classifications.)

Organisations should have a policy for destroying information that is in line with their security risk management plan.

Do not use rubbish or recycling services or systems to dispose of protected information unless it has already been through a destruction process such as shredding.

Waste, whether it is placed in a rubbish skip or other area for collection, or delivered directly to a waste disposal service, is extremely vulnerable.

Disposing of official records

Dispose of official records in line with the Public Records Act. This usually means under the provisions of a disposal authority issued by National Archives of Cook Islands.

Destruction methods

The following are the usual methods of destruction of protectively marked information.

- **Pulping**— transforming mass to a given size determined by a removable screen
- **Burning** — burning in line with relevant environment protection restrictions
- **Pulverisation** — using hammermills with rotating steel hammers to pulverise the material

- **Disintegration** — using blades to cut and gradually reduce the waste particle to a given size determined by a removable screen
- **Shredding** — using strip-shredders and crosscut shredders. Only crosscut shredders are recommended for protectively marked information.

USING THE SHREDDING METHOD

Commercial strip shredders are not suitable for destroying of protectively marked material or sensitive waste. Anybody wishing to access the information will have little difficulty reconstructing the pages from the resultant strips.

Cross-cut shredders produce smaller pieces that are harder to reconstruct. The smaller the particle size the more secure the results.

Manufacturers often grade their shredders based on various international standards that often have differing specifications for each security level.

Take care when purchasing a shredder to ensure the maximum particle size is suitable for requirements.

Use the following shredder requirements to destroy paper-based protectively marked information.

- **Grade 3 shredder**, maximum particle size 4 mm x 15 mm, suitable for information classified up to and including RESTRICTED.
- **Grade 4 shredder**, maximum particle size 1 mm x 15 mm, suitable for information classified at SECRET.
- **Grade 5 shredder**, maximum particle size 1 mm x 5 mm, suitable for information classified at TOP SECRET and information with COOK ISLANDS EYES ONLY marking.

When possible, use a commercial cross-cut shredder for paper waste for official information.

When the destruction method is shredding, use the correct grade of shredder for the security classification on the information.

Destroying microfiche and other photographic material

Protectively marked microfiche and other photographic material must be destroyed using an approved equipment or processes.

CONTRACTING OUT THE DESTRUCTION OF HARD-COPY MATERIAL

Base any decision on contracting out the destruction of protected material on sound risk management.

Here are some factors to consider.

- How does the company transport information?
- What are their procedures?
- How secure are their containers including vehicles and storage areas?
- How secure is their facility?
- What equipment do they use?
- What is the result of their destruction process? (For example, the resultant particle size of the destroyed material).

Remember that classified waste bags and bins are not security containers. Therefore, they must receive appropriate protection before they are collected. Classified waste bags and bins need to be stored according to the highest level of protectively marked information they contain.

Before entering into a contract for the destruction of paper-based information that is protectively marked, be satisfied that the contractor can safeguard the information throughout the destruction process.

PROCESSES FOR DESTRUCTION

Organisations should determine the processes they and the contractor will use to maintain an appropriate level of security throughout the pickup, transportation, and destruction of the waste.

Appropriate processes include:

- the waste must not be left unattended at any time
- the vehicle and storage areas must be appropriately secured
- the destruction must be performed immediately after the material has arrived at the premises
- organisation representatives with the right level of security clearance must escort the waste and witness its destruction
- the destruction company staff must have a security clearance to the highest level of the protectively marked information being transported and destroyed.

Information marked TOP SECRET must be destroyed within organisation premises and only once the originating organisation has been notified. The originators may also apply special conditions to the destruction of some protectively marked information that might prevent contracting out destruction. Destruction must be recorded in the CDR.

SANITISING AND DESTROYING ICT MEDIA AND EQUIPMENT

ICT media and equipment should be sanitised or disposed of securely to prevent the disclosure of classified information into the public domain.

Sanitisation is defined as the process of removal of data and information from the device such that data recovery using any known technique or analysis is prevented or made unfeasible.

- **Sanitise copier drums and printer cartridges** - print at least three pages of random text with no blank areas on each colour printer cartridge with an integrated drum or separate copier drum. Electrostatic drums can retain an image of recently printed documents providing opportunity for unauthorised access to information.
- **Sanitise televisions and monitors** - visually inspect video screens by turning up the brightness to the maximum level to determine if any classified information has been burnt into or persists on the screen. If information is persistent, sanitise it by displaying a solid white image on the screen for an extended period.
- **Sanitise ICT equipment and media** – consult best practice guidance on methods for sanitising media. Note that hybrid hard drives, solid state drives and flash memory devices are difficult or impossible to sanitise effectively. In most cases safe disposal will require destruction.
    - NIST Guidelines for Media Sanitisation 2014 ○ GCSB NZISM Media Management Decommissioning and Disposal.
- **Destroy ICT equipment and media** - remove classification labels, markings and serial numbers and destroy within an approved facility and using approved destruction methods. Contact MDNS for recommended destruction services.

4.2 Securing information

Information security principles

Key principles

- All information has value and requires an appropriate degree of protection
- Access to classified information should only be granted based on a genuine 'need to know'. Do not over-classify. This will ensure those who need it, have access to it
- Information and assets received from or exchanged with external partners should be protected in accordance with any relevant legislative, regulatory, or international agreement requirements
- Use sound online security practices. Stay abreast of best practice online behaviours when using mobile devices and working online.

Use multiple layers of security – 'defence in depth'

Effective security for an information asset can be achieved by using several different layers of security measures. This approach is referred to as 'defence in depth' — the security of an asset is not significantly reduced with the loss or breach of any single layer of security.

A ‘defence-in-depth’ strategy:

- reduces the likelihood of a successful malicious attack
- minimises the damage that results from an attack.

A simple example is preventing malware from infecting IT systems. Three or more layers of defence may be applied:

- a network monitoring and intrusion detection system (IDS)
- an intrusion prevention system (IPS)
- a computer or server anti-malware protection system.

If any single system fails to detect a piece of malware, another system will detect it and prevent the malware from running. It is important to use a diverse and complementary range of capabilities so each layer can catch and prevent an intrusion that another layer may have missed.

Model good security behaviours

Everyone plays a vital role in helping to protect organisational assets and keeping the organisation and its people safe and secure. By following good security behaviours, individuals will make a big difference to help reduce the organisation’s vulnerability to threats.

> **MORE INFORMATION**
>
> - Model good security behaviour

Designing information security measures (INFOSEC-1)

> **INFOSEC-1**
> **Design your information security**
>
> Design information security measures that address the risks your organisation faces. Your security measures must be in line with:
>
> - the Cook Islands Government Security Classification System
> - the Cook Islands Security Handbook
> - best practice standards
> - any privacy, legal, and regulatory obligations that you operate under.

Adopt a framework to manage information security

Organisations should establish a framework to direct and coordinate the management of your information security.

Frameworks should be appropriate to the level of security risk faced and consistent with organisational needs and legal obligations.

The framework should cover how the organisation will ensure that it :

- understands and follows security policies and processes
- is alerted to changes to systems, risks, or standards
- marks, accesses, and declassifies protected information correctly
- manages and controls access to information.

Examples of best practice frameworks include:

- ISO/IEC 27001:2022 Information technology -- Security techniques -- Information security management systems -- Requirements
- US National Institute of Standards and Technology (NIST) Cyber Security Framework

Address critical risks

When you design security measures, address critical information security risks and vulnerabilities including cyber-security threats, information security culture, security products, and processes.

Design and adopt policies such as:

- **ICT usage policy** – to communicate the requirements for proper use of corporate ICT assets including a policy on Bring Your Own Device (BYOD).
- **Clear desk and clear screen policy** to ensure classified information is not left unattended
- **Administrative security policy** to reduce the risks relating to elevated information and asset rights and accesses. This policy should include password management, administrative account controls, key management, audit and inspection, and monitoring and rapid response
- **Mobile and remote working policy** to reduce the risks relating to people using mobile technology and working away from the office such as from remote sites, home office, or while travelling.

Design appropriate access controls

Organisations must have measures in place for controlling access to all information, ICT systems, networks (including remote access), infrastructure and applications.

Areas to consider include:

- user access management — who should be able to access what
- user responsibilities and segregation of duties to protect information
- network access control — what resources can be accessed on a network
- system access control — secure logins
- application and information access control.

Resources for designing information security measures

Ensure that all defence layers have adequate security measures. Use the GCSB New Zealand Information Security Manual (NZISM) resources below to support the design of your security measures:

Network and perimeter security

- NZISM: Network Security
- NZISM: Gateway Security
- NZISM: Enterprise System Security

Security monitoring

- NZISM: Information Security Monitoring

System security

- NZISM: Physical security of servers and IT equipment
- NZISM: Communication Systems and Devices

Application security nzism: product security

- NZISM: Software Security
- NZISM: Email Security
- NZISM: Using the Internet

Data security

- NZISM: Access Control
- NZISM: Cryptography
- NZISM: Data Management

Consider the trade-off between ultimate security and effective operation

Meeting the minimum standards is often not enough, but the cost of ultimate security can be prohibitive. Any information security framework should be pragmatic while still ensuring that critical risks are adequately addressed.

Add to business continuity and disaster recovery plans

The security requirements identified during the design phase should also be in business continuity and disaster recovery plans.

Business continuity management defines the actions to take to continue operating during a significant service interruption, attack or other incident, and then to return to normal operation after the incident.

It is important to develop and regularly test plans to prepare an organisation for smooth operation during an incident and ensure that it can resume normal operations as soon as possible after the incident. An organisation's resilience depends directly on its ability to confront the hazards and continue to achieve its defined outcomes.

Given the increasing dependence on information systems to deliver products and services, it is critical to consider the resilience of the ICT systems that hold and process critical information. Key metrics for ICT disaster recovery plans should include:

- recovery point objective (RPO) — how much data might be lost, considering the frequency of backups taken
- recovery time objective (RTO) — the length of time required to recover and restore to normal function after a disaster ends.

MORE INFORMATION

- Managing business continuity

Build secure solutions and supply chains

Work with suppliers to ensure that they understand and can meet organisational security requirements. Build security requirements into contractual arrangements. Security weaknesses in suppliers can compromise otherwise robust security measures in other parts of a business. Remember to account for the information risks involved in the ICT system development lifecycle, such as development providers accessing and using test data or defect tracking systems.

Consider separating development, test and operational facilities to reduce the risk of unauthorised access or changes to systems.

MORE INFORMATION

- Working with others (GOVSEC-6)

Checking your information security (INFOSEC-2)

This step provides senior executives with the confidence that information and its associated technology are well-managed, risks are properly identified and mitigated, and governance responsibilities can be met.

Conduct the appropriate certification and accreditation processes required for the type of security measures being implemented.

> **INFOSEC-2**
> **Check your security measures**
> Confirm that your information security measures have been correctly implemented, are fit for purpose and meet your needs.

Test and control changes

Establish and use a process for reviewing and testing that security measures have been correctly implemented in processes and procedures. This should also include supply chain processes and procedures as well as testing of building and physical security measures.

Establish and use a process for ensuring that ICT systems (whether bespoke, off-the-shelf, cloud, mobile app, or supply chain delivered) are fit-for-purpose and approved for use for classified information.

Involve supply chain suppliers in the testing and acceptance process.

Only do system testing after all security measures have been implemented and before acceptance. Use an effective change control process to ensure that changes conform to relevant standards.

Use a formal management process to control changes to all information systems.

> **MORE INFORMATION**
> - NZISM: Penetration Testing
> - NZISM: Gateway Testing
> - NZISM: Software Testing
> - NZISM: Product selection and acquisition / assurance
> - NZISM: Change Management

Maintaining information security (INFOSEC-3)

Threats, vulnerabilities, and risks evolve over time as technology, business, and information demands change. Security measures must keep pace with this change to remain relevant and effective.

INFOSEC-3
Keep your security up to date

Ensure that your information security remains fit for purpose by:

- monitoring for security events and responding to them
- keeping up to date with evolving threats and vulnerabilities
- maintaining appropriate access to your information.

Analyse evolving threats and vulnerabilities

To manage vulnerabilities in information security, take the following action:

- Monitor systems, networks, and processes for security vulnerabilities. Observe system and network events, configurations, and processes to detect suspicious or unauthorised events.
- Be proactive to stay on top of vulnerabilities or flaws in the technical environment.
- Assess security measures against best practice and known security threats.
- Analyse, prioritise, and report on vulnerabilities that pose the most immediate risk to the organisation.
- Apply fixes and track them to completion to mitigate the risk of information being compromised.

Threats are continually evolving. The CSO should use the following threat catalogues to stay abreast of emerging threats:

- Critical Controls — CERT NZ — check this page for frequent updates
- Cyber threat reports — New Zealand National Cyber Security Centre
- Cyber alerts and advisories — Cyber & Infrastructure Security Agency (CISA)
- Internet Storm Center
- Software Engineering Institute — Carnegie Mellon University

Keep information security measures up to date

Security measures are only effective if they reflect actual assessed risks and are kept up to date as risks and threats emerge.

- Document and maintain operating procedures and make them available to all users who need them.
- Maintain a user access control systems as people (including contractors and suppliers) join, change jobs, and leave the organisation, and when access controls are introduced or changed.
- Protect the organisation's ICT equipment from malware, including personal devices that have access to your organisation's information.

- Apply security patches and updates regularly to ensure that information is protected from identified and addressed security vulnerabilities.
- Test business continuity and disaster recovery plans when new processes, systems, and capability are introduced. Make sure the organisation is adequately prepared for a significant service interruption, attack or other serious security incident.

Respond to information security incidents

Good management is critical to reducing the impact of security incidents and recovering quickly. Incident response should be a key part of the overall security framework.

Provide people with the guidance and resources to act in a timely, coordinated manner to prevent or respond to security incidents that could compromise critical and sensitive information. Develop and regularly test these processes and procedures as part of the business continuity and disaster recovery planning.

Follow the right process for managing security incidents.

> **MORE INFORMATION**
>
> - Managing security incidents (GOVSEC-7)

Conduct periodic reviews and assure compliance

To minimise the risk of disruption to organisation business processes, carefully plan and agree on suitable audit requirements for operational systems.

Minimise the opportunity for unauthorised access to information system audit tools to limit the potential to misuse or compromise them.

Regularly monitor, review, and audit security measures to understand the degree to which information security policies are being implemented and followed. This should include:

- use of operational procedures
- handling of protectively marked materials
- supply chain and partners services, reports and records
- compliance with relevant legislation, requirements and standards.

> **MORE INFORMATION**
>
> - NZISM: Assurance Guidance
> - NZISM: Assurance Standards

Identify changes required to information security

Change is a given. Identify which changes in the environment might affect information security.

Consider these questions to inform changes and improvements.

- Are we using information in new ways? Think about information collected from others (inputs), information provided to others (outputs), work and information flows inside or outside the organisation (processes), information interfaces between organisations or systems (connections).
- Are we bringing in a new supplier, provider, or partner to fulfil a specific need?
- Are we planning improvements to internal or external security services?
- Have we identified new security threats or vulnerabilities?

The review will identify required changes to the information security requirements. These changes may trigger a requirement to retire information or systems or to refresh the security risk assessment defined in GOVSEC-2.

MORE INFORMATION

- Retire information securely
- Understand what you need to protect (GOVSEC-2)

Retire information securely

When information and supporting ICT systems are no longer required, they need to be archived, destroyed, repurposed, or disposed of securely.

Consider these questions:

- How will your information and equipment be declassified when it no longer needs to be protectively marked?
- How will sensitive information and related equipment be disposed of?
- Is checking with the originator needed?
- Is information stored in the cloud that needs to be archived or disposed of?

Make sure to take into account relevant legislation and best practice standards.

MORE INFORMATION

- Archive or disposal
- Retire information and assets securely

4.3 Specific information security scenarios

Mobile and remote working

Consider the situations that people might face when they are working away from the office. Will they be working at home? In remote locations? In someone else's building? Overseas?

People are using portable computing and mobile communications devices to work remotely in a variety of ways and places, such as:

- taking work home
- working in the field
- working from vehicles
- working from hotels or conference venues
- visiting client offices
- working while on public transport.

Mobile and remote working is becoming more common, yet many people are unaware of the threats that they face.

Organisations must take all reasonable steps to ensure the personal security of their employees when they are working away from the office.

Use the risk assessments to work out when it is needed to increase protection for people. In some cases, it may be necessary to extend protection to family members and others.

Mobile working increases the risks of compromise. It can result in the loss of sensitive, high value, corporate or personal information, affecting the information's confidentiality, integrity, and availability. The types of risks are:

- **Loss or theft:** Portable devices are easy to lose or steal, and sensitive information stored on the device can be exposed.
- **Confidentiality:** When devices are used in public spaces, information can be overheard or overseen, leading to loss of confidentiality.
- **Electronic interception:** Devices used over wireless and public networks are vulnerable to electronic interception. Malicious software can disable security features and activate inbuilt microphones and cameras, giving attackers access to private or privileged content and conversations.
- **Tracking:** Built in GPS receivers and transmitters may allow tracking of the precise location of the user.
- **Malicious software (malware):** Just like any home or office computer, portable devices are susceptible to malware, which can be passed on to connected networks and other computing equipment.

- **External storage devices:** USB devices, portable storage devices, CDs, and DVDs are an easy way to distribute malware and data exfiltration.

These risks may be increased when privileged users have remote access to systems. For example, systems are at greater risk when a system administrator has access to remotely manage systems from home or a mobile device.

Also consider how to secure and manage use of personal devices in bring-your-own-device (BYOD) scenarios. Today, more people are using their personal devices for corporate purposes or their corporate devices for personal purposes, increasing the risks of compromise. User education is crucial to managing an organisation's risks.

Before approving mobile or remote working, conduct a mobile work risk assessment. Reduce risks when using mobile devices using these procedures.

MORE INFORMATION

- Checklist for mobile computing and communications/remote working

Before deployment or travel

- Ensure that mobile devices have been updated with security and application updates.
- Enable mobile device security features.
- Change PINs and passwords. Always use complex passwords containing upper and lower case letters, numbers and symbols.
- Reduce the risk of information exposure by removing any information that is not required for the deployment or period of travel.
- Back up information stored on the device. If the device becomes compromised, the user may not be able to recover information from it.
- Be aware of the emergency security procedures for the mobile device.

Device handling

- Maintain physical control of mobile devices at all times. Do not leave mobile devices unattended in places where they may be stolen or tampered with.
- Avoid taking mobile devices into situations where sensitive or private conversation is likely. Where this cannot be avoided, turn off the device and, where possible, remove the battery.
- If it is required to give someone else the mobile device or it is lost (for example, if required to hand it over for secure storage outside a meeting), check with the organisation's Information and Communications Technology (ICT) security people for guidance before you use it again.

Secure usage

- Ideally, use only corporate devices with all relevant security measures enabled for storing, processing, and communicating sensitive or private information.
- Only use personal mobile devices for official business when a risk assessment process, enabling policy, and suitable security controls are all in place.
- Be vigilant at all times. When using a mobile device, make sure that others cannot overhear the conversation or see the screen.
- If the risk of tracking is a concern, disable any GPS capability. For extra security, turn off the mobile device and, where possible, remove the battery.
- Disable any features or capabilities that are not required. For example, disable wireless, Bluetooth, and location services if they are not needed. Consider doing this before having confidential conversations.
- Always confirm the integrity of any new storage media with ICT security staff before connecting it to a mobile device. Have storage media scanned regularly for threats.

Email usage

- Never use private email accounts to store or communicate official information.
- Never forward email from corporate email systems to personal email accounts. For example, Gmail.
- Where you need additional security, ensure that email connections are encrypted.
- To reduce the risk of downloading hidden malware, disable image loading in all email applications.

Internet usage

- Activate the privacy mode in the internet browser.
- Set an internet browser to prompt before installing cookies.
- Turn off auto-fill to prevent the browser from storing usernames and passwords.
- Never join or connect to wireless networks where the integrity is unknown. Make sure wireless settings require manual confirmation before connecting to a wireless network.

After deployment or travel

- Change all mobile device passwords when the deployment or travel is over.

Transacting online with the public

Online services offer the public a convenient, efficient way to access government and other services. However, as the demand for online services grows, so too does the scale and sophistication of cybercrime and malicious activities.

Cyber threats and cyber security should be considered a top-tier priority when the government transacts online with the public.

Organisations should adopt mitigation strategies to reduce the public's exposure to cyber security risks online. If online services are compromised, services may expose the public to harm. Malicious software posted on online services could result in:

- corruption of the users' device and loss of information
- propagation of malicious software and infection to other websites and devices
- theft of users' identity or financial details
- users being blackmailed or drawn into illegal activities.

Consider the impacts of unintended information disclosure. For example, unintentionally disclosing location information about the people the organisation is transacting with.

Organisations that provide online services should maintain skilled, in-house IT security staff who work closely with the organisation's CSO.

Mitigate risks when transacting online with the public

Ensure that users are aware of the risks surrounding the use of public-facing systems and how to mitigate them.

Provide training and documentation on how to use systems and services safely and appropriately for each of the usage scenarios described in this section. Develop policies for usage and ensure that all system users follow them.

Take care with insecure browsers. Restrict access to browser versions that are known to have security weaknesses, are out of date or unsupported, or warn users about them.

Protect online accounts

If public users need to set up an online account to transact with the organisation, use the following measures to protect their security.

Keep users up to date with terms and conditions

- Require users to accept account terms and conditions before they open an account, and the first time they use a different computer.
- Include in terms and conditions a warning that simply explains the specific risks associated with using the online service and give details of alternative channels for service or support.
- When updating terms and conditions, require account holders to accept the new conditions.
- Link a query button to the organisation's privacy policy page to provide more information about the conditions of acceptance.

Keep public users' data safe

- Do not use transaction processes that put the user at risk of unnecessary harm. For example, by requiring a public user to reduce their security protection measures.
- Use a secure connection for online transactions that transfer personal details to the government and only transfer the required details.
- Only collect the information from users that is necessary for delivering the service.
- Provide guidance to help users select a secure password.

Also see NZISM: Access Control

Protect the security of on-site kiosks where the public can access information and services

- Provide ICT resources and information intended via an unclassified standalone system. If this is not possible, the host system should be connected to an unclassified network that is separated from other networks and systems by a suitable gateway.
- Site the kiosk where it can be monitored by people from the host organisation.
- Employees should watch users and promptly investigate suspicious behaviour.
- Lock down kiosk functionality to just what is essential for the services on offer.
- Refresh kiosk sessions when a user logs out, or after a period of session inactivity that indicates the kiosk has been left unattended.
- Minimise physical access to a kiosk and its ports, allowing only what is essential.
- Protect the security of wireless network access
- If you provide wireless connectivity to the organisation's network, use strong security for authentication and encryption. Change wireless keys and pass phrases regularly. Only provide wireless access outside office hours if necessary.

Also see NZISM: Network Security

Warn public users about downloading information

- Provide a warning before the download starts, identifying the potential risk. For example, 'Warning, you are about to download information across an unsecured connection'. Give the options 'Proceed', 'Cancel' and '?'.
- Link '?' with information on associated risks. For example, with a hover tag.

Use gateway technology to separate public network services from corporate systems

- Monitor the gateway for any unauthorised activity.
- Use a web proxy server to control access to external websites and to limit public access to permitted internal web services. You can configure a web proxy server as a web guard to check internet traffic and content for malware.

Also see NZISM: Network Security

Audit and monitor activity

- Log all successful and unsuccessful user activity. Investigate repeated unsuccessful attempts to perform actions.
- Notify users about unusual or higher risk online activity on their accounts.
- Analyse patterns of online user interactions for unusual activity that could indicate a security compromise.
- Profile user access devices to detect unusual access vectors that could suggest a security compromise.

Also see NZISM: Event Logging and Auditing

Control authentication and access

- Use authentication methods that are proportionate to the service or information you are making publicly available. A registered user account with an associated password is the minimum authentication requirement for accessing sensitive, private or protectively marked information.
- Apply access controls to all information repositories, folders and files. Restrict access in line with user rights and privileges.
- Display the previous login time and date when a user next logs in. If the transaction is high-value or high-risk, consider sending the user a follow-up email telling them that their account has been accessed, with details of the associated Internet Protocol (IP) address.
- Where warranted, offer or impose higher level security credentials such as one-time passwords, digital certificates, or tokens.

Also see NZISM: Access Control

Perform code audits

- Perform a code audit of any web application used on the organisation's web site, to ensure there are no security vulnerabilities that could be exploited.

Also see NZISM: Conducting Audits

Take measures to keep email secure

- Organisational emails should carry clear messages about what the organisation would not do via email, such as asking the user to provide logon credentials or other sensitive information.
- Use a reputable mail guard to check email content and attachments.
- Block unapproved file types and sizes.
- Detect and block spam and malware.
- Enforce mandatory protective marking for all email.

- Restrict the sending of protectively marked or sensitive emails to external addresses in line with policy.

Also see NZISM: Email Security

Protect data when uploading or downloading files

- Ensure that read and write operations and the use of media types is appropriately restricted.
- Control device usage and data flow in line with usability requirements by using device disabling, device whitelisting, and by write-blocking devices.
- To ensure data integrity, restrict the size and types of files that may be uploaded or downloaded to or from the system. Use a reputable security suite.
- Use application whitelisting to prevent unauthorised or unwanted execution of files.
- For sensitive or protectively marked information, consider a 'review and release' process to control inadvertent, inappropriate or unauthorised data transfers.

Also see:

- NZISM: Data Management
- NZISM: Media Usage
- NZISM: Application Whitelisting.

Consider privacy if you use social media

- If the organisation uses social media platforms to interact with the public, consider privacy. Carefully evaluate privacy and security implications when collecting and holding personal information as part of a service.

Prioritise patching and maintaining online services

- Have the organisation's IT support give priority to applying patches for online services (including the maintenance of information-only web pages) and associated web servers. Delays in patching may create cyber security vulnerabilities for public users.

Also see:

- NZISM: Product Patching and Updating
- NZISM: Software Security

5.0 Physical security

This section has information and tools to help organisations set up effective physical security measures to protect their people, information, and assets.

Ensure the organisation is providing and maintaining a safe and secure working environment.

5.1 Securing the working environment

Physical security principles

Deter, Detect, Delay, Respond, Recover

Physical security measures aim to protect people, information, and assets from compromise or harm through the following techniques.

Deter	Deter or discourage unauthorised people from attempting to gain unauthorised access to your facility. Implement measures that unauthorised people perceive as too difficult or needing special tools and training to defeat.
Detect	Detect unauthorised access as early as possible. Implement measures to work out whether an unauthorised action is occurring or has occurred.
Delay	Delay an unauthorised access attempt for as long as possible to allow an effective security response to be activated. Implement measures to slow the progress of a harmful event.
Respond	An effective response counters the anticipated activity of an unauthorised person within a time appropriate to the delay measures. Prepare measures to prevent, resist, or mitigate the impact of an attack or event.
Recover	Take the steps required to recover from a security incident. Plan to restore operations to as near normal as possible in a timely manner following an incident.

Security in depth

Design a multi-layered system of security measures to increase protection.

Layering physical security measures means the security of people, information, and assets is not significantly reduced with the loss or breach of any single layer. By designing security measures that combine to support and complement each other, it makes it difficult for an

external intruder or an employee to gain unauthorised access. This method is called 'security in depth'.

To ensure security in depth, an organisation must:

- use a combination of measures to protect and control access to people, information, physical assets, and premises
- select physical security products that provide the right levels of protection (as determined by a risk assessment).

Designing physical security (PHYSEC-1)

> **PHYSEC-1**
> **Design your physical security**
> Design physical security measures that address the risks your organisation faces. Your security measures must be in line with relevant health and safety obligations.

Understand physical security risks

Identify the relevant risks for each site the organisation operates in and use the following considerations in a risk assessment: the neighbourhood, visitors received, site access and parking, building access points and windows, floor layout, classification of information accessed, and security areas for the site.

As part of the risk assessment, consider the following questions:

How are the facilities used?

It is important to understand how the facilities are used, who uses them, who may visit them, and what is stored in them.

Remember to include any classified information or assets stored, and legislative requirements that need to be met.

Are people working away from the office?

Consider the situations that people might face when they are working away from the office.

Will they be working at home? In remote locations? In someone else's building? Overseas?

Have you taken health and safety needs into account?

Organisations are required to take all reasonable steps to minimise the risk of harm to employees, clients, and the public.

Is the organisation co-locating?

If co-locating, work in partnership with the other parties to build a shared understanding of physical security issues and each other's security requirements.

Know vulnerabilities

You need to know of any vulnerabilities and how the organisation would be affected by breached security.

Here are some questions to answer.

- What hours will people be working at each site? When will they be arriving and leaving?
- How many people will be working at each site?
- Which third parties have access to the facilities?
- What are the risks associated with collections of information and physical assets held?
- What are the risks associated with higher concentrations of people in certain areas?
- Which activities does the organisation undertake at each site?
- Are there threats that arise from its' activities?
- What threats arise from the location and neighbours?

Evaluate the likelihood and impact of each risk to help understand where further action is needed. For any risks that can't be accurately assessed internally, call on external sources such as local police or other authorities.

Physical security measures can be more expensive and less effective if they are introduced later. Consider physical security requirements at the earliest stages — preferably during the concept and design stages.

> **MORE INFORMATION**
>
> - Understand what you need to protect (GOVSEC-2)

Define your site security areas

Use security areas to match physical security to the risks facing your people, information or assets.

Extra security measures apply to areas where protectively marked information and other official or valuable resources are processed, handled, discussed, and stored. These areas are called, security areas. Each security area has minimum security controls that an organisation must implement.

The Cook Islands Government has three physical areas for handling information and people.

Public areas

These are unsecured areas including out-of-office working arrangements. They provide limited access controls to information and physical assets where any loss of information would be unlikely to damage the security or interests of the Cook Islands or the privacy of its residents. They also provide limited protection for people.

Examples of public access areas are:

- building perimeters and public foyers
- interview and front-desk areas
- temporary out-of-office work areas where the organisation has no control over access
- field work, including most vehicle-based work
- public access parts within multi-building facilities.

PERMITTED USES

In public access areas organisations can:

- store information and physical assets needed to do business with UNCLASSIFIED or agreed OFFICIAL information
- use information and physical assets with classification up to RESTRICTED with safeguards in place to protect the information from being overseen or overheard.
- Storage is not recommended unless unavoidable.
- It is not recommended for use of information with classification of SECRET or TOP SECRET classification unless unavoidable. Storage is not permitted.

Work areas

These are low-security areas with some controls. They provide access controls to information and physical assets where any loss could result in prejudice to the maintenance of law and order, impede effective conduct of government or adversely affect the privacy of residents. They also provide some protection for people.

These areas allow unrestricted access for employees and contractors. Public or visitor access is restricted.

Examples of work areas are:

- normal office environments
- normal out-of-office or home-based worksites where you can control access to areas used for business
- interview and front-desk areas where people are separated from clients and the public
- airports and airside work areas with a security fence around the perimeter and controlled entry points

- vehicle-based work where the vehicle is fitted with a security container, alarm, and immobiliser
- exhibition areas with security controls and controlled public access.

PERMITTED USES

In work areas, the organisation can:

- store information and physical assets with a classification up to RESTRICTED
- use information and physical assets with a classification up to SECRET but this information should not normally be stored in the area and approved security containers must be used
- use information and physical assets with a classification of TOP SECRET only under exceptional circumstances to meet operation imperatives with approval of the originator. No storage is permitted.

Secure areas

These are security areas with higher levels of security measures in place. They provide access controls to information where any loss could result in serious (SECRET) or exceptionally grave (TOP SECRET) damage to national interests. They may also provide additional protection for people.

Access should be strictly controlled with identification (ID) verification, key/card access, and logging of access. People with ongoing access should hold an appropriate security clearance. Visitors and contractors must be closely be controlled and have a business need to access the area.

Examples of security areas are:

- secure areas within a building, for example the IT server room or secured meeting rooms
- secure safes and cabinets where access is strictly restricted, monitored, and controlled areas used to store high-value items or items of cultural significance when not on display
- areas storing SECRET and TOP SECRET information and assets
- armament storage.

PERMITTED USES

In security areas, the organisation can:

- use and store information and physical assets with a classification up to TOP SECRET with strict controls in place to log access and usage.

Develop site security plans

Organisations must assess whether the physical security environment is acceptable as part of their regular security risk assessment.

- Use a site-specific risk assessment to help prepare site-specific security plans.

Create site security plans

A site security plan document measures to counter identified risks to the organisation's functions and resources at the site.

For each site security plan, ensure that physical security measures:

- provide enough delay to allow planned responses to take effect
- meet business needs
- complement and support other operational procedures
- include any necessary measures to protect audio and visual privacy
- do not unreasonably interfere with the public.

What to include in a site security plan

In the plan, document the answers to the following groups of questions.

LOCATION AND OWNERSHIP

- What is the location and nature of the site?
- Does the organisation have sole or shared ownership, or tenancy of the site?

PEOPLE

- What hours do people work at the site?
- Who else visits the site (for example, the public, service providers)?
- What hours is it open to the public or other visitors?

PROTECTIVELY MARKED INFORMATION

- What protectively marked information is stored, handled, processed, or otherwise used in each part of the site? Which protective measures will be needed for that information?
- Which protective measures are needed for sensitive discussions and meetings (including those that involve protectively marked information)?

ICT ASSETS AND RESOURCES

- Which information and communications technology (ICT) assets and resources are on the site? (Including, but not limited to, data, software, hardware, workstations, servers, frames and cabling, and portable devices such as laptops and tablets.)

WHOLE SITE, AREAS WITHIN THE SITE, SCALABLE MEASURES

- Which protective measures are needed for the site as a whole?
- Which protective measures are needed for certain areas within the site? For example, part of a floor that will hold information of a higher classification than the rest of the site.
- How will security measures be scaled to meet increases in threat levels?

Protect security plans too

Remember that the site security plans contain valuable information about the organisation's security and operations. Assess the impact of any loss or harm to the plan and apply a protective marking if necessary.

Include security requirements in briefs and contracts

Include all relevant security measures from the site security plans in building design briefs and requests for tender and contracts, so they are included in the completed facilities.

Designing physical security measures

Perimeter access controls

Restricting access to facilities with perimeter access controls can help an organisation to reduce threats.

Some types of perimeter access controls are:

- fences and walls
- pedestrian barriers
- vehicle barriers.

Work out if the organisation needs perimeter access controls during the security risk assessment and before completing any site selection process.

Fences and walls

Fences and walls are used to define and secure the perimeter of a facility.

Fences might not be practical in urban environments, particularly in central business districts.

The level of protection a fence gives depends on its:

- height, construction, material, and access control method
- any additional features used to increase its performance or effectiveness, such as topping, lighting, or connection to an external alarm or CCTV system.

If choosing to use fences or walls to deter unauthorised access, develop supporting procedures for:

- monitoring and maintaining the fences or walls
- monitoring the grounds for unauthorised access.

Make sure any access points are at least as strong as any fence or wall used.

MORE INFORMATION

- BS 1722-12:2016 Fences - Specification for steel palisade fences
- BS 1722-14:2017 Fences - Specification for open mesh steel panel fences
- AS 1725.1-2010 Chain-link fabric security fencing, Part 1; Security fences and gates – General requirements
- AS/NZS 3016:2002 Electrical installations - Electric security fences

Pedestrian barriers

Pedestrian barriers are used to restrict access through fences or walls by controlling the entry and exit points.

Examples of pedestrian barriers are:

- locked gates
- gates connected to electronic access control systems (EACS) or alarm systems • guard stations
- turnstiles.

Vehicle barriers

Vehicle barriers are used to prevent hostile vehicle attacks. Vehicle related threats range from vandalism to sophisticated or aggressive attacks by determined criminals or terrorists.

Examples of vehicle barriers are:

- gates
- retractable barriers or bollards
- fences and walls
- bunds and berms.

MORE INFORMATION

- PAS 69:2013 Guidelines for the specification and installation of vehicle security barriers
- Hostile vehicle mitigation

Alarm systems

Alarm systems can provide early warning of unauthorised access to facilities.

However, an alarm system is only of value when it is used alongside other measures designed to detect an intrusion attempt, delay an intruder's progress, and give time to respond. An alarm system must be monitored and linked to a predetermined response.

TYPES OF ALARM SYSTEMS

Alarm systems can be broadly divided into two types:

- a perimeter (or external) intrusion detection system (PIDS) or alarm
- an internal security alarm system (SAS).

Alarm systems may be single sector or sectionalised to give coverage to specific areas of risk. Sectionalised alarm systems allow greater flexibility because highly sensitive areas can remain secured when not in use and other parts of the facility are open.

A PIDS can be valuable for organisations with facilities enclosed in a perimeter fence because it will give early warning of unauthorised breaches.

Organisations should seek specialist advice when designing and installing PIDS.

MANAGING ALARM SYSTEMS

Procedures for using, managing, monitoring, and responding to an alarm system must be developed.

Any contractors employed to maintain a SAS should be security cleared.

Use a suitably qualified designer or installer to design and commission any commercial alarm systems.

Make sure each different security area is a separate alarm section or have a separate alarm system for each area.

When possible, configure the alarm systems to continuously monitor detection devices in high-risk areas. For example, irregularly accessed areas, roof spaces, inspection hatches, and under-floor cavities.

> **MORE INFORMATION**
>
> - AS/NZS 2201.1:2007 Intruder alarm systems - Client's premises - Design, installation, commissioning and maintenance
> - AS/NZS 2201.5:2008 Intruder alarm systems - Alarm transmission systems

MANAGING ALARM SYSTEMS IN SECURITY AREAS

For alarm systems in Security areas, the organisation must have:

- direct management and control
- appropriately cleared and trained staff as privileged operators and users.

Guard patrols may be used instead of an alarm system outside of usual work hours. For more information, go to Visitor Control (Out-of-hours guarding).

MANAGING ALARM SYSTEMS IN PUBLIC AND WORK AREAS

In Public and Work areas, organisations should manage and administrate alarm systems directly, operational functions, such as monitoring, and maintenance can be outsourced.

Guard patrols can be used instead of an alarm system outside of usual work hours. For more information, go to Visitor Control (Out-of-hours guarding).

KEEPING PERSONAL IDENTIFICATION NUMBERS (PINS) SECURE

Organisations should ensure all personal identification numbers (PINs) for arming and disarming alarm systems are:

- uniquely identifiable to an individual
- not recorded by the individual
- regularly changed in line with your risk assessment.

Employees must advise the CSO straight away if they suspect any PINs have been compromised. The CSO must disable the PIN and investigate any potential security breach.

For more information, go to Reporting incidents and conducting security investigations.

> **MORE INFORMATION**
>
> - Managing security incidents (GOVSEC-7)

DEALING WITH ENGINEERING/INSTALLER CODES SECURELY

The default/engineering/installer user codes must be removed from alarm systems at commissioning.

For Security Areas, the engineering/installer codes must only be known to security cleared personnel who have access to the zone.

When the code needs to be provided to others for maintenance purposes, it is important to change the codes as soon as the maintenance work is finished.

Organisations should develop appropriate testing and maintenance procedures to ensure an alarm system is continually operational.

CHOOSING A SECURITY ALARM SYSTEM (SAS)

Security alarm systems are used to protect information and assets. To choose the right SAS, consider the:

- level of the area you need to protect
- complexity of the area's layout

- security level of the information or assets you need to protect.

INDIVIDUAL ALARM OPTIONS

Individual alarms can protect people and vehicles from harm.

In some situations, building alarm systems or other facility-wide measures might not give all the protection people and assets need. For example, when you need to protect:

- people working away from the office
- areas with a high potential for personal violence valuable physical assets in public areas
- valuable assets stored in vehicles used for work purposes.

Several individual alarm options are available to supplement security measures, including:

- duress alarms (fixed, hidden, and mobile options)
- individual item alarms or alarm circuits
- vehicle alarms.

DURESS ALARMS

Duress alarms enable people to call for help in response to a threatening incident.

To get fewer false alarms, choose duress alarms that are activated by dual-action buttons (users need to press two separate buttons to trigger the alarm).

FIXED AND HIDDEN DURESS ALARMS

Fixed duress alarms are individual alarms that are monitored remotely. They're normally hardwired and fixed to a location.

Consider equipping public contact areas with duress alarms if the organisation's risk assessment has identified a potential problem. Public contact areas include reception areas, counters, and interview rooms.

Hidden duress alarms should:

- enable people to raise an alarm discreetly
- be augmented by procedures that provide an appropriate response.

> **MORE INFORMATION**
>
> - AS/NZS 2201.1:2007 Intruder alarm systems – Client's premises – Design, installation, commissioning and maintenance

TRAINING YOUR PEOPLE

You need to ensure that employees are aware of any duress alarms, have regular training, and participate in trials so they know what to do in a real situation.

MOBILE OR INDIVIDUAL DURESS ALARMS

Mobile or individual duress alarms help to deter violence towards people. They're suitable for times when they are outside the office or circulating in public areas.

Personal duress alarms fall into two broad categories:

- alarms that are monitored remotely
- alarms that produce loud noise when activated.

ALARMS THAT ARE MONITORED REMOTELY

These alarms are suitable for use within facilities where there is a dedicated monitoring and response force. The alarms consist of a personal alarm transmitter linked to the facility or a separate alarm system.

NOISE-PRODUCING ALARMS

These alarms rely on the response of bystanders. They are more suitable than monitored duress alarms when there could be considerable delay in response to the alarm.

You can use noise-producing alarms within a facility to ensure people in the immediate area notice an incident as soon as it happens.

INDIVIDUAL ITEM ALARMS AND ALARM CIRCUITS

When it is impossible to protect valuable items using normal alarm systems (particularly when they are in public areas, such as exhibitions) two options to consider are:

- installing a separate alarm system to monitor individual items
- installing an individual item alarm circuit.

Some alarm sensor types that may be suitable are:

- pressure switches
- motion sensors
- closed-circuit television (CCTV) activated alarms
- radio frequency identification (RFID) tag systems.

Seek specialist advice when designing alarm systems for individual items.

VEHICLE ALARMS

Consider installing vehicle alarms if people need to work from vehicles and those vehicles contain large amounts of valuable equipment.

NOISE-PRODUCING ALARMS

Most vehicle alarms rely on noise to deter intruders. However, if the vehicle driver is outside hearing range, these kinds or alarms rely on a response from bystanders.

REMOTE ALARMS

Consider fitting vehicle alarms that are monitored remotely when the asset value is very high or where information stored in the vehicle is classified as TOP SECRET.

Remote vehicle alarms can also be linked to remote vehicle tracking and immobilisation systems.

Access control systems

Use access control systems to prevent unauthorised access.

An access control system is a measure or group of measures designed to:

- allow authorised personnel, vehicles, and equipment to pass through protective barriers
- prevent unauthorised access.

ACHIEVING ACCESS CONTROL

Access control can be achieved in several ways. The most common ways are:

- using psychological or symbolic barriers – for example, Crime Prevention Through Environmental Design (CPTED)
- positioning security staff at entry and exit points positioning security staff at central points and having them monitor and control entry and exit points using intercoms, videophones, CCTV cameras, and similar devices
- installing mechanical locking devices operated by keys or codes
- using electronic access control systems (EACS).

VALIDATING IDENTITY USING AUTHENTICATION FACTORS

Access control systems should provide identity validation using authentication factors about:

- what you have – keys, identity (ID) cards, and passes
- what you know – personal identification numbers (PINs)
- who you are – visual recognition, biometrics, and so on.

USING DUAL AUTHENTICATION

Dual authentication requires the use of two authentication factors.

Organisations must use dual authentication to control access to Security areas.

Also use dual authentication when the risk assessment identifies a significant risk of unauthorised access.

USING ELECTRONIC ACCESS CONTROL SYSTEMS (EACS)

Organisations should use EACS when there are no other suitable identity verification and access control measures in place.

EACS can be used along with other personnel and vehicle access control measures.

GET EXPERT HELP

Organisations should:

- seek specialist advice before selecting EACS
- use a designer or installer recommended by the manufacturer to design and commission EACS.

FOLLOW GOOD PRACTICE

Verify the identity of every potential cardholder before issuing them with access cards for EACS.

Audit regularly to check who has access to EACS. It is important to find out who still needs access and, disable or remove access for people who no longer need it or have left the organisation.

Use sectionalised EACS to control access to specific areas in the facility. The sections of EACS are normally the same as the sections of the alarm systems, but they may have extra operational access control points not covered by individual alarm sections.

EACS should typically start at Work Area perimeters but may be used in Public Access Areas (for example, to control access to car parking).

Keep EACS software and hardware up to date. Ensure software is updated to address known vulnerabilities. Consider updating EACS cards and readers as they age and become vulnerable to new threats.

Relevant standards

- ULC 60839-11-1 – Standard for Alarm and Electronic Security Systems – Part 11-1: Electronic Access Control Systems – System and Components Requirements

MEET THE HIGHEST THREAT AND RISK LEVEL

When implementing EACS to cover a whole facility (on their own or with other access control measures), design them to meet the highest perceived threat and risk level.

If using multiple EACS along with other access control measures, design each system to meet the highest perceived threat and risk level in the areas covered by the system.

Using a two-person access system to protect highly valuable information and physical assets

Some EACS can be enabled to only allow access to areas when two people are present and will activate an alarm if one leaves the area. This feature is known as a ‘no-lone-zone’. It requires two authorised people to access and exit a designated area.

Consider using a two-person access system when needing to protect very highly or extremely valuable information and physical assets.

Implementing an identity card system

Identity (ID) cards allow the quick recognition of people who work for an organisation. Use ID cards in all facilities in Security Areas.

Issue ID cards to all people who have regular access to facilities and meet personnel security requirements.

ESTABLISH HIGH-QUALITY PROCESSES FIRST

Building an ID system of high integrity requires robust processes for verifying identities, and for registering, enrolling, issuing, and auditing ID cards. Consider conducting a privacy impact assessment.

VERIFY ALL IDENTITIES

Before issuing an ID card, verify the person's identity.

Sight each person's:

- government-issued credentials with photographic or biometric identity features and a signature
- evidence of other identity verification documentation
- evidence of residential address.

If the organisation already has information that verifies a person's identity, the process can be streamlined. However, make sure the potential ID cardholder provides government-issued credentials with a photo and a signature.

VERIFY SECURITY CLEARANCE HOLDERS

When an ID card will grant access to areas requiring a security clearance, or indicate that the holder has a security clearance, it is important to independently verify the details of their clearance (including when it expires or is due for revalidation) before issuing an ID card.

FOLLOW GOOD PRACTICE

ID cards should:

- be worn and clearly displayed at all times in the premises
- be uniquely identifiable
- include a return address for lost cards
- not identify the facility to which the card gives access
- not be worn outside your premises
- be audited regularly in line with the risk assessment.

Within a Work Area or higher area, remember to protect:

- card making equipment
- spare, blank, or returned cards.

Other information can be included on ID cards to improve control of access, such as names, photographs, and colours.

Using EACS access cards as ID card is not recommended, particularly in high security or high-risk areas.

Integration of physical control systems

Integrated systems must be designed carefully to avoid creating vulnerabilities.

Implementing integration between security alarm systems (SASs) and other building management systems can increase the threat of unauthorised system access and penetration.

Examples of other building management systems or external integrated systems (EISs) are:

- building management systems (BMSs)
- closed-circuit television (CCTV)
- electronic access control systems (EACS).

When interconnecting systems, ensure the SAS cannot be controlled or disabled by any of the interconnected systems.

The IT security team should review the implementation of any interconnection.

INTEGRATION IN PUBLIC AREAS AND WORK AREAS

SASs suitable for Public Areas and Work Areas applications may include fully integrated EACSs as a single system.

INTEGRATION IN SECURITY AREAS

For Security Areas, SAS and EISs should be separate and independent from each other. Any interoperability must not allow the SAS to be controlled or disabled by the EIS.

INTEGRATION WITH EISS

Designers of EIS or sub-systems need to secure the EIS to prevent unauthorised access or manipulation, especially when it is interconnected with an SAS. EISs should be designed with appropriate logical and physical controls.

Locks, key systems, and doors

Choose the right hardware to protect information and assets.

Organisations must secure all access points to premises, including doors and operable windows, using commercial grade locks and hardware. These locks may be electronic, combination, or keyed.

Combinations, keys, and electronic tokens must be given the same level of protection as the most valuable information or physical asset contained by the lock.

LOCKS

Locks can deter or delay unauthorised access to information and physical assets.

However, locks are only as strong as the fittings and hardware surrounding them. So, assess the level of protection needed from doors and frames when selecting locks.

Protecting lock combination settings

The CSO should manage the security of your lock combinations.

Employees must memorise lock combination settings, and make sure only one written record of each setting is kept for use in an emergency.

Keep the record of the combination in an appropriately sealed envelope and protect it in a container. Protectively mark the envelope with the highest security classification of the material protected by the lock.

Follow the lock manufacturer's instructions when using or servicing combination locks.

When to change settings

Lock combination settings must be changed:

- when a container is first received
- after a lock is serviced
- after a change of custodian or other person who knows the combination
- when there is reason to believe the setting has been, or may have been, compromised
- at least every 6 months
- when a container is disposed of by resetting the lock to the manufacturer's settings.

USING KEYING SYSTEMS

If using a keying system, design it to prevent unauthorised people from making duplicate keys or using common techniques to compromise it.

Keying systems should include security measures. For example:

- legal controls, such as registered designs and patents
- physical controls that make it difficult for people to get or manufacture blank keys or the machinery used to
- cut duplicate keys

- controls that protect against techniques like picking, bumping, impressioning, and decoding.

CHOOSING A KEYING SYSTEM

When choosing a keying system, consider the following questions.

- What level of protection does the system provide against common forms of compromise?
- What is the length of legal protection the manufacturer offers?
- What level of protection can the supplier provide for keying data within their facility?
- How transferable is the system and are there any associated costs?
- What are the costs for commissioning and on-going maintenance?

COMPLYING WITH SECURITY AREA REQUIREMENTS

In Public Areas, use restricted keying systems when there is a risk of theft.

In Work Areas and Security Areas, it is a requirement to use commercial restricted keying systems. That means using keys that are not easy to copy or combination locks.

USING MASTERED KEY SYSTEMS

If using a mastered key system, it must have enough levels to allow separate area master keys to control any:

- locks within an electronic access control system (EACS)
- alarm system control points.

MANAGING YOUR KEYS

Maintain a register of all keys that are held and issued. Ensure the key register is secure and only allow authorised employees to access it.

The key register should include the following details:

- key number
- name, position, and location of person holding the key
- date and time issued
- date and time returned or reported lost.

KEEPING MASTER KEYS SECURE

Strictly control master keys and limit the number of them.

Because grand master keys may give access to all areas of a facility, the CSO should control the issuing of them.

Audit the key register regularly to confirm the location of all keys. Losing a master key may mean a need to re-key all locks under that master.

REMOVING MASTER KEYS FROM YOUR FACILITIES

Keys to Security Areas should not be removed from facilities.

Keys to security containers must not leave facilities, except in cases of emergency.

For Public and Work Areas, base any decisions about allowing keys to be removed from the facilities on the risk assessment. Removing keys significantly increases the risk of loss.

When allowing a key to be removed, make sure:

- a manager approves the removal
- the frequency of key audits are increased

Ensure everyone in the organisation knows and follows the key management policy.

PROTECTING YOUR KEY CABINETS

Locate key cabinets within the facility's secure perimeter and, where possible, within the perimeter of the zone where the locks are located.

Key cabinets may be either manual or electronic.

Commercial grade key cabinets provide very little protection from forced or covert access.

Electronic key cabinets

Electronic key cabinets may have an automatic audit capacity and replace the need to maintain a key register.

In some cases, electronic key cabinets can be integrated into an EACS. Most commercial grade electronic key cabinets are not suitable for high security applications. However, there are currently no electronic key containers suitable for high security applications, unless they’re used along with other control measures, such as locating the key container within a security room or area covered by a security alarm.

DOORS

Select doors that provide a similar level of protection to the locks and hardware fitted.

TYPES OF DOORS

Commercial office doors vary significantly. Some examples are:

- solid core timber
- composite timber
- metal framed insert panel
- metal clad solid core or hollow core

- glass swing opening
- rotating glass
- glass sliding: single and double.

Solid core wood or metal clad doors may have glass or grill insert panels. The panels and fixings must provide the same level of protection as the door.

Automatic sliding glass doors normally operate through an electric motor and guide fitted to the top of the door. Some of these doors, particularly when unframed, may be levered open either at the centre joint for double sliding doors or sides for double and single sliding doors. This can make them difficult to secure without fitting drop bolts, lower guides, and/or door jambs.

Domestic hollow core doors (used for most internal domestic doors) and **domestic sliding glass doors** provide negligible delay as they are easily forced. However, if you fit them with appropriate locks, they'll give some evidence of an intrusion when broken.

Closed-circuit television

Consider using CCTV when an organisation is developing 'security in depth' for a site.

CCTV is a visual deterrent to unauthorised access, theft, or violence. It can be used to cover:

- site access points, including internal access to higher security zones
- site perimeters
- access to specific physical assets or work areas.

CCTV also gives a visual record of access for audit purposes.

CONSIDERING CCTV

The benefits of CCTV may include being able to:

- monitor event-activated alarms
- use it along with a security alarm system (SAS) to help those responsible for responding to the alarm
- use it along with an access control system to aid personal identification for remote site entry control
- use motion detectors
- use visual analytics (suspicious package detection).

However, a CCTV system can be a significant capital cost. On-going monitoring, maintenance, and support costs may also be high.

It requires compliance with all relevant jurisdictional legislation governing CCTV usage.

Other considerations on the use of CCTV include:

- how its use fits into the overall security plan for the site
- which types of security incidents are anticipated and what the expected response to those incidents might be
- how people and visitors will be advised that CCTV is in use on the premises
- what the functional requirements are.

If using CCTV to support criminal proceedings, the quality of images or data should be suitable for use as evidence.

Be aware that:

- computers used to store CCTV images may require significant memory space.
- excessive compression of data may severely affect the quality of images stored.

Also consider how long you will need to retain the images.

Seek specialist advice before designing and installing a CCTV system to ensure the proposed system meets needs.

SECURITY LIGHTING

Using lighting to enhance physical security at the site.

Lighting can make an important contribution to physical security. It can be used inside and outside a facility to reduce risks and increase safety.

When designing a site, consider what needs to be achieved with security lighting. For example, to:

- deter unauthorised entry
- help guards conduct patrols
- illuminate areas with CCTV coverage
- provide employees with safety lighting in car parks.

Motion detection devices can also be set up, so any detected movement activates lighting or CCTV (or both). Make sure any lighting you use meets the illumination requirements of any CCTV systems you have installed.

MORE INFORMATION

- IES-G-1-03 Guidelines on security lighting for people, property and public spaces
- National Guidelines for Crime Prevention through Environmental Design Ministry of Justice, 2005
- Designing out Crime: Crime Prevention through Environmental Design Australian Institute of Criminology

Security containers and cabinets

Choose the right containers and cabinets to keep information and assets secure.

Secure official information, valuable physical assets, and money in containers that are appropriate to their classification level.

EVALUATE SECURITY NEEDS FIRST

When selecting security containers and cabinets, evaluate the potential risks to the information or assets they will hold. Risks such as theft, damage, or unauthorised access.

Factors that will affect the class of security container needed include:

- the level of protective marking on information or assets
- the location of the information or physical assets within a facility (e.g. public area, Work area, or Security area)
- the structure and location of the building
- access control systems
- other physical protection systems in use (for example: locks, alarms, and outer zone security).

CAREFULLY CONSIDER WHERE TO PUT CONTAINERS

Whenever possible, avoid placing security containers against security area perimeters with lower levels of protection. Doing so could allow an intruder to bypass the additional security features of the more secure area.

PROTECT IN LINE WITH THE HIGHEST INFORMATION CLASSIFICATION

Ensure valuable physical assets that contain official information, such as computers and other ICT equipment, are protected from whichever has the higher risk rating:

- the compromise of all information in the physical asset
- the loss of the physical asset itself.

When possible, store protectively marked information separately from other physical assets. This separation will:

- lower the likelihood of information being compromised if physical assets are stolen
- help investigators determine the reason for any incidents involving unauthorised access.

CONSIDER REQUIREMENTS FOR CONTAINERS

Containers provide different levels of protection to the contents that they hold.

- Some are extremely heavy and may not be suitable for use in buildings with limited floor loadings – often suitable for storing TOP SECRET classified information

- heavy types may be suitable for use where there are minimal other physical controls available – suitable for storing SECRET and TOP SECRET classified information
- lighter models designed for use along with other physical security measures such as a restricted keyed lock or padlock – suitable for OFFICIAL and RESTRICTED classified information.

Secure rooms, safes, and vaults

Consider using a secure rooms, safes, or vaults instead of containers to protect large quantities of official information or valuable physical assets.

USING STRONG ROOMS

Strong rooms are suitable for storing large quantities of official information.

CHOOSING SAFES AND VAULTS

Store unclassified material in commercial safes and vaults designed to give a level of protection against forced entry.

Commercial grade security safes and vaults provide varying degrees of protection, seek the advice of a qualified locksmith or manufacturer. They will tell you which criteria to use when choosing a commercial safe or vault.

Safes and vaults can be fire-resistant (either document or data), burglary-resistant, or a combination of both.

Seek advice from a reputable manufacturer before installing a commercial safe or vault for protecting valuable physical assets.

For items that can't be secured in safes or vaults (such as large items), use other controls that give the same level of intrusion resistance and delay.

FITTING VEHICLE SAFES

Consider fitting vehicle safes to vehicles used to carry valuable physical assets or official information.

Vehicle safes provide some protection against opportunistic theft. However, they're not designed to protect vehicles left unattended for prolonged periods (for example, overnight).

Vehicle safes are of similar construction to low-grade commercial security containers.

The risk assessment may show that additional treatments are needed to mitigate some risks when vehicles are used to transport protectively marked material or valuable assets.

To ensure the effectiveness of a vehicle safe, consider:

- bolting the safe to the vehicle (preferably out of sight)
- fitting anti-theft controls such as immobilisers and alarms.

FOLLOWING BEST PRACTICE: INTERNATIONAL STANDARDS

The Australia / New Zealand Standard AS/NZS 3809:1998 Safes and strong rooms provides advice on design criteria for safes and strong rooms used to protect valuable physical assets.

It categorises safes and vaults as:

- basic – suitable for homes, small businesses, offices
- commercial – suitable for medium retail, real estate agents
- medium security – suitable for large retail, post offices
- high security – suitable for financial institutions, clubs
- extra high security (vaults only) – suitable for high-volume financial institutions.

> Also see the following international standards:
>
> - BS EN 14450:2017 - Secure storage units. Requirements, classification and methods of test for resistance to burglary
> - UL 687 - Standard for burglary-resistant safes
>
> These international standards provide advice on testing for fire resistance in safes:
>
> - UL 72 - Tests for fire resistance of records protection equipment
> - JIS S 1037 - Standard fire test
> - KSG 4500 – Fire-proof safes

VISITOR CONTROL

Follow clear, consistent processes for controlling visitor access to your facilities.

A visitor means anyone in a facility or area who:

- is not an employee
- has been granted normal access to the facility or area as a visitor.

This definition may include employees from other parts of an organisation.

Whichever entry control method is used, people should only be given unescorted entry if they:

- show a suitable form of identification
- have a legitimate need for unescorted entry to the area
- have the appropriate security clearance.

AUGMENTING VISITOR CONTROL WITH AN ELECTRONIC ACCESS CONTROL SYSTEM

Visitor control is normally an administrative process. However, it can be augmented by using an electronic access control system (EACS). This allows visitors to be issued with EACS access cards enabled for the specific areas they may access.

In more advanced EACSs, it's possible to require validation from the escorting officer at all EACS access points.

CONTROLLING ACCESS TO SECURITY AREAS

In Security Areas, organisations should issue visitors with visitor passes and record details of all visitors. Consider policies to restrict use of electronic devices at sensitive meetings or Security Areas. (e.g. leave electronic devices outside of the meeting room or secure area).

In Work Areas, when no access controls are in place, issue visitors with visitor passes and keep a visitor record.

Passes should be:

- worn at all times
- collected at the end of the visit
- disabled on return if the passes give access to any of your access control systems
- checked at the end of the day and, when the passes are reusable, disable and recover any that haven't been returned.

An employee should escort visitors.

Based on the risk assessment you may record visitor details at the:

- facility reception areas
- entry to individual security areas.

KEEPING A VISITOR REGISTER

Visitor registrations should be utilised by organisations.

The visitor register should include the:

- name of the visitor and their signature
- visitor's organisation or firm or, in the case of private individuals, their private address
- name of the person to be visited
- times the visitor arrived and departed
- reason for the visit.

A visitor register is normally kept at the reception desk, unless the desk is unattended, in which case it should be held by a designated employee within the facility.

If an organisation manages access into specific areas at the entry to the area, those areas should have their own visitor registration process.

Visitors into Security Areas or sensitive areas should provide government-issued credentials embodying photographic identity features and a signature.

REMOVING PEOPLE FROM YOUR PREMISES

Have documented procedures for dealing with members of the public who behave unacceptably on premises or who are present in a restricted area without authorisation or escort. Employees must be informed of these procedures.

If a member of the public behaves in an unacceptable manner, a duly authorised person should take the following steps when they consider it necessary for the person to leave the premises. Consider whether theft may have taken place.

No employee or guard should attempt to physically remove a person from premises unless permitted to do so under legislation. This would normally be left to a police officer.

The contact number for the police should be available to all employees.

MANAGING ACCESS TO PREMISES BY THE MEDIA

If anyone in an organisation is considering giving access to media representatives, they should consult the CSO before they grant access.

Add the following procedures to standard visitor control procedures:

- a designated employee should accompany media representatives throughout the visit
- protectively marked information should be locked away (preferable) or at least protected from view
- additional restrictions are considered when appropriate, such as handing in mobile phones and other recording and communications equipment
- the media liaison unit or public affairs area is consulted about the arrangements.

Additional controls may be necessary for particular sites.

If an organisation grants permission for a visit to areas where protectively marked information is being used or handled, the employee responsible for the media representatives should remind them that no photographs or recordings of any type can be taken at any time during the visit, except with specific approval.

ACCESS BY CHILDREN TO AREAS WHERE PROTECTIVELY MARKED INFORMATION IS STORED OR PROCESSED

An organisation should develop policies to cover when children are allowed into areas where sensitive or protectively marked material is held or used.

Parents or guardians are responsible for getting prior approval for children to enter official premises.

Remember to keep a log of children who enter in case there is an emergency situation.

PRE-SCHOOL CHILDREN

Pre-school children may be permitted short-term access if the parent or guardian (being a staff member):

- has approval from the relevant manager
- is with their) children at all times.

Some pre-school children can read, but they're less likely to fully understand protectively marked material than older children. They're also less likely to recall details, such as names and identities.

SCHOOL-AGED CHILDREN

School-aged children are often able to understand written material and have well developed long-term memory. They should only be allowed access under extenuating circumstances and only at the discretion of an organisation's HOM.

Extenuating circumstances under which access may be granted are:

- a staff member is called in for emergency duty and no childminding is available at short notice
- a staff member is recalled from leave and a child requires unique parental care
- a staff member is required to sign papers, arrange posting activity, or other administrative tasks while in sole charge of a child
- normal childcare arrangements end without notice and a staff member, who is required to report for duty, is unable to make alternative arrangements
- a staff member is required to attend for duty when a child is injured (but not suffering from infectious illness) and requires monitoring.

The parent or guardian is responsible for the safety, wellbeing, and behaviour of the child while on the premises (including emergency evacuations). They must not leave the child unattended, noting:

- children (as with any other uncleared individuals) must not be given access to corporate IT systems or protectively marked material
- work areas should, as much as possible, be cleared of any sensitive or protectively marked material while children are present
- children should not be present at meetings or during discussions where sensitive or protectively marked material is discussed
- children who are suffering from, or convalescing after, an infectious illness must not be granted access (in line with occupational health and safety requirements).

RECEPTIONISTS AND GUARDS

Control visitors and deter threats with receptionists and guards.

If your organisation has regular public or client contact, have receptionists or guards to greet, assist, and direct visitors.

Guards deter threats to information and physical assets and can provide a rapid response to security incidents.

FOLLOW GOOD PRACTICE

Receptionists and guards:

- should be able to easily lock all access to the reception and non-public areas in the event of an emergency or increase to the threat level
- may only perform other duties, such as CCTV and alarm monitoring, if it does not interfere with their primary function of controlling building access through the reception area. If performing other duties, they should be suitably trained and competent
- should be able to lock away all valuable or sensitive material (for example, paperwork, keys) if they need to temporarily leave the vicinity
- should have a method of calling for immediate assistance if threatened, for instance a duress alarm or radio, as they are most at risk from disgruntled members of the public
- should hold security clearances (and briefings) at the highest level of information to which they may reasonably be expected to have incidental contact with and in line with the facility with which they work.

Organisations should:

- provide receptionists and guards with detailed visitor control instructions and training
- identify any security concerns for receptionists, guards, and people using your reception areas in a security risk assessment and mitigate those concerns.

Out-of-hours guarding

Guards and patrols may be used separately or along with other security measures.

Base the requirement for guards on the level of threat and any other security systems or equipment that are already in place. That will guide decisions on what their duties are and how often they need to carry out patrols.

Security area requirements

Organisations can use out-of-hours guarding or patrols instead of alarm systems in Security Areas. These guards may be permanently on site or visit facilities as part of regular mobile patrolling arrangements.

Out-of-hours guard services may be used in response to alarms. The response time should be within the delay period given by the physical security controls.

The highest level of assurance is given by 24 hours a day, seven days a week on-site guards who can respond immediately to any alarms.

Where guard patrols are used instead of an alarm system, patrols should be performed at random intervals. For Security Areas, base the intervals on the risk assessment but make sure they are within every 4 hours. For other areas, base the intervals on your risk assessment.

Guards should check all security cabinets and access points as part of their patrols.

MORE INFORMATION

- Working with others (GOVSEC-6)

OTHER PHYSICAL SECURITY MEASURES

Work out which other physical security measures your organisation might need to address specific risks.

Use the following examples to help you work out which physical security measures will best meet your specific requirements. (Note: This list is indicative not exhaustive.)

Measure	Used to
Hidden and/or fixed duress alarm	Address personnel safety concerns for reception areas and meeting rooms. Maybe of value for home-based workers
Individual duress alarm	Address personal safety concerns for personnel in the field or unpatrolled public areas
Individual item alarm and/or alarm circuit	Provide extra protection for valuable physical assets in your premises or physical assets on display
Vehicle alarm	Deter vehicle theft or theft of information and physical assets from vehicles
Two-person access system	Provide extra protection for extremely sensitive information
Vehicle safes	Deter theft of information and physical assets from vehicles
Vehicle immobilisation	Prevent vehicle theft

Front counters, and interview or meeting rooms	Restrict access by aggressive clients or members of the public Allow regular meetings with clients or members of the public without accessing security areas
Mailrooms and delivery areas	Provide a single point of entry for all deliveries Prevent mail-borne threats from entering a facility without screening
Technical surveillance counter and audio security	Reduce vulnerability to, or detect, the unauthorised interception of sensitive or protectively marked information Reduce vulnerability to electronic eavesdropping on sensitive conversations
Conference security	Prevent unauthorised people gaining access to protectively marked information and ensure the proceedings are conducted without disruption

Using vehicle immobilisation techniques

Vehicle immobilisation can reduce the loss of vehicles to theft. Vehicle immobilisation can be broadly divided into two types: automatic and remote.

With automatic immobilisation, a vehicle can be immobilised when not in use and requires a key or electronic token to start the vehicle.

With remote immobilisation, a vehicle can be immobilised while in use and this technique is normally used along with a remote tracking and alarm system.

Protecting front counters, and interview or meeting rooms

If your employees interact with the public or clients who may become agitated, your organisation must install measures to reduce the risks to their safety.

These measures might include:

- a specialised front counter that limits or delays physical access
- interview or meeting rooms monitored by guards or fitted with duress alarms (or both)
- interview or meeting room desks that act as a barrier.

If employees regularly interact with clients or the public, consider establishing interview or meeting rooms that are accessible from your public areas.

Reducing threats to mailrooms and delivery areas

Mailrooms and parcel delivery areas are areas of significant risk from improvised explosive devices, and chemical, radiological, and biological attacks.

Organisations must assess the likelihood of mail-borne attacks and, if warranted, apply suitable physical mitigations. For example:

- mail screening devices
- a standalone delivery area
- a commercial mail receiving and sorting service.

Educate and train your people

Make sure employees are aware of mail handling policies and procedures.

Give your mailroom staff training – they must know mail handling procedures and how to use any screening equipment available.

Surveillance countermeasures

Technical Surveillance Countermeasures (TSCM) is a process used to:

- survey facilities and detect any surveillance devices
- identify technical security weaknesses that could be exploited (including controls such as locks, alarms, and electronic access control systems).

TSCM provide a high level of assurance that sensitive information is free from unauthorised surveillance and access.

TSCM is mainly a detection function that seeks to locate and identify covert surveillance devices:

- before an event
- as part of a programmed technical security inspection or survey
- because of a concern following a security breach (for example, the unauthorised disclosure of a sensitive discussion).

When you must carry out a TSCM survey

Organisations must carry out TSCM surveys for:

- areas where TOP SECRET discussions are regularly held, or the compromise of other discussions may have a catastrophic business impact
- before conferences and meetings where TOP SECRET discussions are to be held.

Protecting sensitive discussion, in person or on the phone

To protect discussions about content that is protectively marked, your organisation should meet the logical controls in the New Zealand Information Security Manual - Telephones and Telephone Systems.

Managing security for conferences and events

Carry out a risk assessment before holding a conference or event to identify risks and mitigate them. If warranted, develop a specific conference security plan.

The aims of conference security should be to:

- prevent unauthorised people gaining access to official information, protectively marked information, or physical assets
- protect the people attending the conference
- protect property from damage
- ensure the conference is not disrupted.

Implementing physical security measures

During this phase, you implement the agreed physical security measures, including policies, processes, and technical measures.

Build physical security into business relationships and contracts

Work with suppliers, co-tenants, and landlords to ensure they understand and can meet the organisation's security requirements. Build good physical security into your contracts and partnerships.

Remember to include all relevant measures or outcomes identified in site security plans, in building design briefs, requests for tender, and contracts.

Manage your planning and building processes

It is necessary to account for the risks involved in the planning and building lifecycle. Make sure physical security measures are implemented when there are new builds, refurbishments, or assets shifted from one workplace or area to another. Take the implementation process right through to when assets and information are retired or destroyed.

Maintain records

It is important to maintain records throughout the planning, building, and implementing process to support the assessment and checking that the security measures are fit for purpose. These records may include:

- photographs showing construction techniques
- certificates confirming equipment has been installed by a certified installer.

Checking security measures (PHYSEC-2)

PHYSEC-2
Check your security measures

Confirm that your physical security measures have been correctly installed and are fit for purpose.

Ensure your physical security measures are used correctly by people.

The CSO decides whether the measures are right for the risks your organisation faces. These risks may vary from site to site.

This step gives senior executives confidence that:

- physical security is well managed
- risks are properly identified and mitigated
- governance responsibilities can be met.

Establish a process for inspecting, testing and ensuring that physical security measures have been correctly implemented across the different security areas: Public areas, Work areas, Security areas. This should also include supply chain processes and procedures.

Also establish and conduct a process for testing and ensuring that physical security systems (e.g. alarm systems, perimeter security systems, physical access control and monitoring systems) are fit for purpose.

Sight, review and consider the following material when checking the physical security measures:

- Facility or site risk assessment conducted
- Site security plan
- Certifications from designers and installers of your security systems
- Site inspection reports
- Site and procedure testing results
- Change control plan.

Maintaining security (PHYSEC-3)

PHYSEC-3
Maintain your security

Ensure you keep up to date with evolving threats and vulnerabilities and respond appropriately.

Ensure that your physical security measures are maintained effectively so they remain fit for purpose.

Raise awareness of your physical security measures

An important part of maintaining security is providing security awareness training and support.

Let employees know about any security risks that may affect their personal safety or security.

Communicate the physical security policies to employees and to the people your organisation works with. Let them know when physical security arrangements change, and, when possible, say why.

Encourage employees to report emerging concerns or near misses as part of being good corporate citizens (rather than troublemakers). Make sure they know that if they respond to a security incident, they shouldn't do anything that unreasonably jeopardises their personal safety.

Give each employee a summary of your emergency and security procedures.

MORE INFORMATION

- Building a security culture (GOVSEC-4)

Analyse evolving threats and vulnerabilities

Keeping people, information, and assets secure involves ongoing activity to detect and manage evolving threats and vulnerabilities.

To manage vulnerabilities in your physical security, take the following action.

- Monitor your systems, assets, and people
- Review and audit your logs and access control systems
- Observe events and processes to detect suspicious or unauthorised events
- Be proactive to stay on top of vulnerabilities or weaknesses in your layers of security
- Assess your security measures against best practice and known security threats

- Analyse, prioritise, and report on vulnerabilities that pose the most immediate risk to your organisation
- Apply and track fixes to completion.

> **MORE INFORMATION**
>
> - Managing security incidents (GOVSEC-7)

Keep physical security measures up to date

To be effective, physical security measures must reflect actual risks. Stay up to date and prepared by:

- proactively maintaining the user access control systems (for example as people join, change roles, and leave the organisation)
- testing and maintaining security systems (for example, by testing duress alarms and checking batteries every 6 months)
- testing procedures to ensure they are fit for purpose.

Respond to physical security incidents

It is a requirement to manage security incidents well to reduce their impact. Aim to both reduce the impact of any incident and recover quickly.

Responding to security incidents should be part of the security plan.

> **MORE INFORMATION**
>
> - Managing security incidents (GOVSEC-7)

Handle physical assets securely

Ensure that physical assets are handled securely and in line with the Cook Islands Information Classification System.

Note that when physical assets are transported outside of premises, they must be -protected in line with the potential business impact of loss, compromise, or damage.

Most physical assets are more at risk from theft during transport than when they're housed in a facility. Seek advice from insurers to help you develop robust processes.

Consider control measures such as escorts or guards or employing secure transport specialists.

> **MORE INFORMATION**
>
> - Handling information

Conduct periodic reviews and assure compliance

Regularly monitor, review, and audit physical security measures.

Ascertain if:

- physical security policies are being followed
- physical security controls are working as planned
- any changes or improvements are necessary.

Identify changes in the security environment

Be prepared to restart the physical security lifecycle whenever the security environment changes.

Consider these questions to inform changes and improvements:

- Are we using our information and assets in a different way?
- Are we using our facilities in a different way?
- Are our people working in a different way?
- Are we planning improvements to internal or external security services?
- Have we identified new security threats and vulnerabilities?
- Will our existing security measures be effective against the new threats and vulnerabilities?

Retire information and assets securely

When building, facilities, information, or assets are no longer needed, make sure to consider the security implications during the decommissioning phase.

Have a plan for destroying, redeploying, or disposing of facilities, information, or assets securely. For example:

- safes or filing cabinets containing classified information
- printers / multi-function devices.

Organisations must destroy protectively marked information and equipment, so that the waste cannot be reconstructed or used.

> **MORE INFORMATION**
>
> - Archive or disposal

5.2 Specific physical security scenarios

Managing public events

Whether the organisation is hosting or attending events, physical security and safety risks must be assessed and measures put in place to reduce them.

Before the event

Consider protective security and safety requirements in the earliest stages of event planning.

To plan an event well it will require the organisation to:

- appoint qualified people to security roles
- consider the threats
- develop a security plan
- inspect possible venues
- manage event preparation.

Appointing an event manager and event security officer

The event manager is responsible for overall event security. The manager must appoint an event security officer (ESO) as early as possible, so they can be included in the planning process.

The ESO is responsible for implementing security for the event and the event venue and should be competent in security management.

The ESO should:

- be senior enough to exercise the necessary authority
- have direct access to the event manager
- have a sound knowledge of protective security.

For a large or long-running event, the ESO might need a support team.

Common duties of an eso

The duties of the ESO should include, but are not limited to:

- seeking advice on possible threats to the event
- completing a security risk assessment for the event or venue(s)
- preparing any security plans based on the risk assessment activity
- making necessary security preparations for the event
- coordinating security during the event
- liaising with appropriate people from the organisation, or external agencies and authorities before, during, and after the event.

Considering the possible threats

Considering possible threats to the event and preliminary work on the event plan usually happen at the same time.

The ESO should seek advice on possible threats from:

- the part of the organisation that is coordinating the event and any other relevant parts
- external agencies, such as the New Zealand Security Intelligence Service (NZSIS), Interpol and other police services, such as New Zealand Police, when relevant.

Identify, assess, and manage the risks to an event in line with the principles in:

- Manage your security risks.

Assessing threats to national security

The ESO should have an independent security threat assessment if:

- the event could be the subject of terrorism or violent protest
- previous similar events have been subject to terrorism or violent protest
- the information to be discussed at the event is protectively marked SECRET or above, and there may be a risk of compromise
- previous experience indicates this is appropriate.

Developing an event security plan

The ESO should develop a security plan based on a risk assessment of the event.

The plan will evolve as details of the event become clearer, and preparations for the event develop. It will also depend on the duration, location, and size of the event.

Remember to include any event security arrangements in the event costings.

Use the following questions to prompt thinking and planning. Add any special requirements to the plan.

WHAT NEEDS PROTECTION AND WHEN?

Think about the need to protect the proceedings themselves, any documents (both those provided, and notes taken during the event), and people who attend.

What kinds of threats are there? What is the appropriate level of security for the event?

How long will the event last? Will the protection needs stay constant throughout the event or vary? When might the organisation need to increase protective measures?

Will attendees be making visits to other sites or activities as part of the event?

WHICH IS THE BEST SITE FOR THE EVENT?

There may be different sites to choose from — some within organisational facilities and others at external venues. Questions to answer include:

- How much control is needed over the event? (The less control, the more likely it is that extra security measures will be needed.)
- How sensitive is the information that will be present?
- What are the unique risks posed by each site?
- How will the flow of the event affect venue choice?
- What are the transport options?
- Will the organisation be able to protect the attendees?

Inspect possible venues before making any decision.

For events where sensitive and protectively marked information will be present, it is best to choose a venue controlled by a Cook Islands Government organisation.

WHO WILL BE INVOLVED IN RUNNING THE EVENT AND WHAT ARE THEIR ROLES?

How will communication between different parts of your organisation be managed, or with other organisations involved in running the event?

What are the roles and responsibilities of event staff?

Who is responsible for liaising with the Cook Islands Police Service if necessary? For example, if the event might attract protest action.

WHO WILL ATTEND THE EVENT?

Who are the attendees? Who do they work for or represent? Will any overseas people attend? Any Cook Islands or overseas office holders? Any media representatives or members of the public?

Are there any security clearance or character check requirements for attendees?

Will any VIPs attend and need personal protection?

Will the organisation need to arrange accommodation for VIPs or other attendees? What are their accommodation security requirements?

WHAT ARE THE CONTINGENCY PLANS?

Contingency plans might include communications, command and control arrangements, and alternative venues for incidents (for example, bomb alerts and public demonstrations or protests).

HOW WILL THE EVENT BE PROTECTED?

Detail the identified threats and the planned measures to manage the risks.

Think about any special protective security measures that might be needed. For example, audio countermeasures, or security containers and other security equipment.

Then state in the event plan what measures will be put in place. For example, it might be needed to:

- strictly limit the number of invitees to the overall event
- strictly limit the number of invitees to particular sessions
- limit the duration of the event to as short a period as practicable
- keep handouts to a minimum
- secure the meeting room from audio-visual recording devices.

Inspecting possible venues

Inspect possible venues at the earliest opportunity. Find out what security is already available and what might have to be put in place. Note any potential risks that haven't already been identified.

The ESO should accompany the event organiser during a preliminary inspection or provide advice on security requirements if they cannot attend.

If protest activity is a possibility, involve the local police at an early stage of the event planning. A more detailed inspection might be required later, once a venue is selected. At both stages contact with the police and venue management can be useful for gaining local knowledge.

When inspecting a venue, consider the following questions.

WHAT MIGHT ADVERSELY AFFECT PHYSICAL SECURITY?

- Would it be easy or hard to fix problems? For example, door locks and window catches, curtain fittings, exterior lights, and light fittings.

CAN ACCESS TO THE VENUE BE CONTROLLED?

- Include entry to the venue, rooms within the venue, and any onsite parking.
- Is there an area where suspicious articles can be examined?
- If it were needed to detonate an explosive device, it would need to be done in an area where it will cause minimal damage to property and no injury to anyone.

HOW VULNERABLE IS THE VENUE TO OVERHEARING, OVERLOOKING, AND ELECTRONIC EAVESDROPPING?

- The risk assessment will inform the level of security needed for these aspects.
- Once a venue is selected, a more detailed survey might be needed.

Managing event preparation

Based on the security plan and inspection of the venue, it may be necessary to address several matters before the event.

These include processes, arrangements, security controls, and logistical matters.

There may be a requirement for processes for:

- controlling keys
- controlling entry
- managing an emergency evacuation
- reporting security incidents
- receiving and escorting visitors
- storing, handling, and disposing of official or protectively marked information.
- It may also be necessary to arrange or prepare:
- event set up schedules
- a communication plan
- event security instructions
- supply and delivery of security containers and other security equipment
- event access and identity passes
- security clearances
- event security exercises
- technical surveillance counter measures
- employees or guards to control access
- searches to sanitise the premises.

During the event

The event security officer oversees security and is responsible for many important tasks during the event.

As well as overseeing security arrangements at the event, the event security officer (ESO) may have to conduct or oversee many tasks to ensure event security is well managed.

Communication, awareness, and advice

The CSO may need to:

- liaise with the event manager on communications, command, and control issues
- maintain awareness of, and consistency with, health and safety requirements
- provide event attendees and venue employees with security advice, including security and emergency procedures
- advise attendees of the protective marking of the subject matter and the security arrangements and facilities available (the security classification of topics to be

discussed should be displayed at the start of the event and again before each protectively marked segment of the event).

ID and entry control

The CSO may need to:

- ensure accredited attendees are issued access and identity passes, including ensuring identities are verified if necessary
- control entry to ensure that no unauthorised persons gain access to the building or event, or can observe or listen to proceedings
- supervise security aspects of visitor control

Safety of protectively marked information

The CSO may need to manage arrangements for protectively marked information used and produced at the event, including how it is received, recorded, distributed, transmitted, returned, and stored. Ensuring its secure storage may include coordinating:

- the use of security containers
- waste collection and disposal.

Personnel coordination

The CSO may need to:

- coordinate security procedures for cleaning and maintenance personnel
- coordinate the physical security and storage of equipment (for example, cameras, recording devices, audio-recording devices, and mobile phones)
- supervise people employed on security duties
- supervising any necessary searches to sanitise the premises.

Note: An ESO should seek advice from their organisation's CSO when needed to help with investigating any security incidents.

Managing event accreditation

Event accreditation documents provide speedy validation of a person's right to attend an event.

Major events should have:

- a master list of participants, including event management and support staff (where possible, featuring photo identification and information covering roles, contact details, etc)
- accreditation passes for participants, featuring:
    - photo identification
    - the dates of validity

    - the category of participants
    - any restricted area access rights
- a design and layout that can be visually checked by guards or event staff.

Accreditation passes should be designed so that they are comfortable for participants and can be worn at all times.

When an event is sensitive and you need to avoid publicity, consider using a unique but unobtrusive identification article, such as a lapel pin or badge.

Controlling access to restricted areas

The ESO should decide which event areas need to have restricted access — areas within the venue to which only certain attendees, authorised officials, and security staff will have unescorted access.

Clearly label restricted access areas and control access to them.

Managing information security

Information used at an event could be in a variety of forms, including the proceedings themselves, documents brought to or produced at the event, and audio-visual presentations.

PROTECTIVELY MARKED INFORMATION

Based on the event risk assessment, the ESO should consider not allowing attendees to bring any protectively marked information.

If protectively marked information is needed at the event, consider the following protective measures:

- distributing the necessary number of copies at the beginning of the event, or if possible, at the session where they will be needed
- increasing accountability by numbering and recording the distribution of each copy
- arranging for attendees to leave all protectively marked documents, including any notes taken, at the end of the session or day, and send the documents by safe hand to each delegate after the event

Whether these measures are practical will depend on the circumstances of the event.

Whatever arrangements are made, the ESO should inform attendees of them as early as possible and, if necessary, remind attendees during the event.

PROTECTIVELY MARKED WASTE

If protectively marked waste will be generated at the venue, the ESO is responsible for ensuring there are adequate facilities to collect and dispose of it.

For some protectively marked information, it might be necessary to use an approved shredder or removal/destruction procedure at the venue.

MORE INFORMATION

- Handling information

Security containers

At times, it may be necessary to store protectively marked information onsite either during the event or between proceedings if the event runs for more than one day.

In this case, the ESO may need to ensure suitable security containers are provided and will be responsible for controlling access to them.

Considering guards and guard patrols

The event risk assessment should outline if guards and guard patrols are needed during an event.

If an event runs for longer than one day, the ESO should consider regular guard patrols during hours the venue is not attended.

Reporting security incidents

Advise event attendees to report any security incident to the ESO or security staff straight away, so the situation can be dealt with swiftly.

Security staff should report any incidents to the ESO as soon as practical after becoming aware of the incident.

Issuing security and emergency instructions

Everyone who will be attending or working at the event needs to know what the security and emergency instructions are. However, it might be necessary to separate instructions for staff and participants.

The ESO should issue the security and emergency instructions for attendees at the event either before they arrive or on arrival.

Receiving mail

Make sure the necessary requirements for receiving mail or goods that may be delivered to an event are considered, including procedures for scanning, and handling suspicious items.

Controlling demonstrations

The Cook Islands Police Service have ultimate responsibility for controlling demonstrations.

If the event security risk assessment indicates that demonstrators may be a problem, seek advice from the police at an early stage to ensure they can respond or are available to discuss other mitigation strategies, including the deployment of security guards.

The ESO is responsible for ensuring proper arrangements are in place before the event begins.

Handling media attention

Media attention might be focused on the event. This attention could be because of event publicity, attendance by VIPs, or the subject matter.

DEVELOPING A MEDIA PLAN

If organising the event, consult the ESO when developing the media plan. The plan may include, based on the risk assessment:

- accreditation of, and passes for, media representatives
- a designated room at the venue for media representatives
- procedures for issuing media releases and statements
- a requirement that, on arrival, media representatives report to the event security or reception area.

MAKE SURE TO:

- consider carefully whether any media representative is to be permitted into the venue or event rooms at any time while the event is in progress, and if so, under what conditions
- ensure any release to the media is in line with the organisation's media liaison processes
- ensure any media access is under controlled conditions and with appropriate escort arrangements
- ensure to take particular care to prevent unescorted access to any room where protectively marked information could be left unattended (prevent access until the room has been checked for protectively marked information).

After the event

The ESO carries out tasks that ensure the event is wrapped up securely.

Following the event, the event ESO completes the following tasks when necessary:

Retrieving or disabling access and identity passes

If event access and identity passes give unescorted access to the organisation's venue, the ESO coordinates retrieving all passes. If that is not possible, the ESO must disable any access provided by the passes.

Searching the venue

The ESO coordinates a thorough search of the venue to ensure no official information or assets that belong to the organisation have been left behind.

For example, items such as documents, audio-visual recordings, whiteboards, projection equipment, and electronic media equipment.

Returning security containers (if used)

The ESO coordinates the return of any security containers used at the event, including changing combination settings for container travel and storage.

SUBMITTING A SECURITY REPORT

The ESO submits a security report to the event organiser.

Reporting any unreported security incident

For any security incidents that occurred during the event that have not already been reported, the ESO reports them.

> **MORE INFORMATION**
>
> - Managing security incidents (GOVSEC-7)

Returning protectively marked material

The ESO arranges the secure transmission of any protectively marked event papers and documentation to all attendees.

Securely transporting sensitive items

To protect sensitive items, follow the four stages of secure transportation.

The tasks for securely transporting sensitive items fall into four broad stages:

- assessing the risks
- planning security before moving the item
- managing security during the move
- confirming the item has arrived safely and wrapping up the transport process.

Assessing the risks

Sensitive items can be transported in several ways. For example, when people in the organisation:

- carry items with them (by hand or in a bag)
- work remotely or abroad (for example, from home or a hotel)
- transport items in a vehicle.

Understand the threats you need to manage

Whichever way an item is transported, many potential threats exist. For example, an item could be:

- accidentally lost or damaged
- stolen by an opportunist theft
- abandoned because of an emergency
- taken from a hijacked or stolen vehicle
- attacked by someone inside your organisation
- targeted through espionage.

Carry out a risk assessment

Use a risk assessment to help understand:

- the value of the item needed to be transported
- the business impact on the organisation if the item was lost or damaged
- the likely threats to the item during transport.

Based on the assessment, consider which security measures will achieve the best balance between robust security and operational effectiveness.

> **MORE INFORMATION**
>
> - Security Risk Management Handbook

Planning security for the item

To plan effectively, answer the following questions.

What is the nature of the item?

Describe the item's size, purpose, value, and any significant features that might affect how it is transported.

If the item has a security classification with associated security requirements, ensure to include those requirements in your plan.

Who is involved?

Identify everyone involved in the transport process and what they are responsible for.

Will the process involve getting sign-off from a manager, liaising with a courier, or arranging an escort? Who will receive the item when it is delivered?

How and when will the item be moved?

Describe how and when the item will be moved.

What mode of transport will be used? Which routes will be involved? Are there any waypoints to consider? What is the destination?

When is the move happening? Does the intended date and time pose any risks? Consider things like traffic volumes, predicted weather, and major events.

What are the likely risks to the item?

Based on the risk assessment, consider risks from the local environment and the planned route.

What is security like at the sites the item is moving from and to? What is the terrain like on the planned route? Is traffic a concern? Will border security be involved?

Which security measures will best protect the item?

Detail the security measures to be used. Ensure the measures are proportionate to the risks identified in the assessment and enable everyone involved to effectively manage the transport process.

What are the contingency plans?

If the item is compromised, how will the organisation respond to and manage the situation? Are there alternative transport plans?

Does everyone involved know what to do?

Make sure to provide the right training and task-specific briefings to the relevant people. They must know how to protect the item and what to do if anything goes wrong.

Managing the item's security during travel

Keep the following practices in mind when managing security while items are being moved.

Maintain awareness

Scan surroundings and be alert to potential threats, especially when escorting others.

Keep a low profile

Be discreet. This practice includes the people involved being discreet and the equipment being used to protect an item being discreet.

Communicate as planned

Be prepared to provide status updates as planned or to call for assistance when needed.

Check physical security solutions

Ensure security solutions are working as intended. For example, solutions designed to mitigate threats such as opportunist theft, forced entry, or covert attempts to gain unauthorised access.

Confirming the item's safe arrival and wrapping up the process

Once an item has been transported, it is important to:

- check the item has arrived intact and has not been compromised
- confirm its delivery with the recipient or owner (for example, with a receipt)

It is also important to:

- assess the entire procedure to find out if it was carried out safely (or at least risk managed)
- record details of the transfer for auditing purposes.

6.0 Security Risk Management Handbook

This risk management method is intended specifically for the assessment of security risks and focuses on vulnerabilities and threats.

Step 1: Assess vulnerabilities and threats (likelihood)

The likelihood of a security risk being realised depends on vulnerabilities and the threats the organisation is exposed to.

Obtain information about potential vulnerabilities and threats by:

- Surveying staff and interviewing management
- Physical spot checks and inspections
- Examining previous security incidents
- Consulting security expertise and monitoring international emerging threats
- Identifying specific targets of interest.

Assess vulnerability

Assess vulnerability by identifying and reviewing the effectiveness of the protective security measures in place including personnel, information, and physical security.

How likely are the security measures to withstand an opportunistic or planned attack and prevent a breach?

Level of likelihood / vulnerability

Slight vulnerability. The asset is well protected; the security measures are robust, and a breach is unlikely to succeed.	**LOW**	**4**
Moderate vulnerability. The asset is protected; the security measures will resist most forms of attack.	**MODERATE**	**3**
Significant vulnerability. Light security measures are in place; but these are unlikely to withstand a determined attack.	**HIGH**	**2**
Full vulnerability. The asset is currently unprotected; or security measures are unlikely to withstand an attack of any kind.	**VERY HIGH**	**1**

Assess the threats

Assess the threats by determining the likelihood that a deliberate action by others will be taken against the organisation's people, assets, or interests. Consider the threat source's capability:

- Do they have the **knowledge** of people, information, assets, security measures, vulnerabilities or have the ability to obtain the knowledge?
- Do they have the **resources** and means to undertake an attack?
- Do they have the **opportunity, determination and intent** to undertake an attack? What level of intelligence do you have that an attack is possible?
- What is the **likelihood of success** based on the above plus the vulnerability assessment previously completed?

Level of likelihood / threat

Slight threat. Unlikely to occur.	**LOW**	**4**
Moderate threat. Reasonable chance of occurrence	**MODERATE**	**3**
Significant threat. Will likely occur.	**HIGH**	**2**
Extreme threat. Almost certain to occur.	**EXTREME**	**1**

Step 2: Assess the impact

Analyse the impact and possible consequences of harm by asking :

- What would constitute harm?
- What would happen if the risk were realised?
- What would be the effect on the organisation's people or stakeholders?
- What would be the effect on customers or the public?
- What would be the effect of information compromise?
    - OFFICIAL – minimal or only slight effect on the conduct of government, organisations, or individuals
    - RESTRICTED – prejudice the maintenance of law and order, impede the effective conduct of government, or adversely affect resident's privacy
    - SECRET - seriously damage law enforcement capabilities, international relations or the investigation of serious organised crime
    - TOP SECRET – widespread loss of life or threaten the security or economic wellbeing of the country or friendly nations.

Level of impact / harm

Slight adverse impact. Slight harm to the efficiency or effectiveness of government but could be dealt with internally by middle management.	LOW	4
Moderate adverse impact. Could prejudice the maintenance of law and order, impede the effective conduct of government, or adversely affect resident's privacy. Senior management intervention required.	MODERATE	3
Significant adverse impact. Could seriously damage law enforcement capabilities, international relations or the investigation of serious organised crime. Top level management or ministerial involvement required.	HIGH	2
Catastrophic adverse impact. Could inflict catastrophic harm to the organisation, threaten widespread loss of life or the security or economic wellbeing of the country or friendly nations. Prime Minister and Cabinet involvement required.	EXTREME	1

Step 3: Assess the security risks

Using the information from the vulnerability and threat assessments above and any countermeasures currently in place to manage the risks, assign a security risk rating based on the following matrix:

IMPACT (Harm)

LIKELIHOOD Vulnerability / Threats	**4: LOW**	**3: MODERATE**	**2: HIGH**	**1: EXTREME**
1: VERY HIGH	**3: MODERATE**	**2: HIGH**	**1: EXTREME**	**1: EXTREME**
2: HIGH	**3: MODERATE**	**3: MODERATE**	**2: HIGH**	**1: EXTREME**
3: MODERATE	**4: LOW**	**3: MODERATE**	**2: HIGH**	**2: HIGH**
4: LOW	**4: LOW**	**4: LOW**	**3: MODERATE**	**2: HIGH**

Step 4: Determine levels of acceptable risk

Once the security risk ratings of all risks are understood, assess, weigh, and prioritise them against one another and determine the risk that the organisation is willing to accept based on the importance of:

- Organisational goals and expectations
- Critical functions and capabilities
- Stakeholder (including Ministers) and customer expectations
- Personal security of staff and visitors
- General expectations about confidentiality
- Continued availability of resources.

The prioritisation can help to determine which risks are acceptable or unacceptable and where resources must be allocated to address unacceptable risk. You should determine a threshold for risk response as shown in the example table below.

Example management risk response levels

1: EXTREME	Senior management owned. Immediate action is required to reduce the risk impact and/or likelihood through treatment. Formal risk management plan. Reviewed at least monthly at senior management meetings.
2: HIGH	Senior management owned. Urgent attention is required to reduce the risk impact and/or likelihood through treatment. Reviewed quarterly at senior management meetings.
3: MODERATE	Senior management input required. Management responsibility is specified. Risk response should be to treat but may be accepted with a contingency plan in place. Regularly monitored and reviewed annually.
4: LOW	Management responsibility is specified. Risk can be accepted with routine procedures in place. Occasionally monitored.

Step 5: Treat the risks

Establish the possible treatment appropriate to the risk and its risk level. Treatments are generally aimed at reducing the likelihood (vulnerability, threats) of occurrence or the level impact or harm, or both.

Key questions to ask when identifying the risk treatments are:

- What processes and controls are needed to reduce risk to an acceptable level?
- Are the measures cost effective for the level of impact if the risk is realised?
- Does the risk warrant the asset's information security classification?
- What resources are needed?
- Who has responsibility for managing the risk?

Treatments may include design and implementation of:

- New or altered procedures
- New equipment
- ICT security controls
- Physical security arrangements
- Training or security awareness campaigns
- Security clearing particular staff or positions

Security risk management plan

Prepare a security risk management plan that combines the information from the previous steps including the risk management plan purpose, objectives, risk strategies, timetable, resources, monitoring and reporting, and review and evaluation processes.

A risk register is a key tool used in the plan:

- Risk ID – unique reference to identify each risk
- Risk description – brief description or name
- Risk owner – the person accountable for the risk and its treatment
- Impact description – describe the harm that will occur if the risk is realised
- Impact rating – untreated impact level
- Likelihood description – describe the vulnerabilities and threats that contribute to the likelihood of the risk being realised
- Likelihood rating – untreated likelihood level based on current vulnerabilities and threats
- Untreated risk rating – rating based on the untreated impact and likelihood
- Risk response – select Treat, Transfer, or Accept
- Treatment plan – describe how the risk will be treated
- Treatment resources – define the resources allocated to treat the risk
- Treatment cost – estimate of the cost of treatment
- Treatment status – to what extent has the treatment been put in place – 0% means not yet started, 100% fully operational.
- Treated impact level – after treatment, the target impact level of the risk
- Treated likelihood level – after treatment, the target likelihood of the risk
- Target risk rating – after treatment, the target risk rating (impact and likelihood product)
- Notes – notes about the risks, treatments, or other aspects pertinent to the current status of the risk
- Last checked date – date that the risk was last reviewed, updated and/or approved.

Step 6: Monitor and evaluate the risks

It is important to monitor and evaluate the effectiveness of the security risk management plan and specific treatments in place to ensure that the treatments are still effective and/or necessary.

Monitoring

Monitor the environment for changes and indicators that the risk management plan and specific treatments need re-examining. The CSO and security team should conduct regular audits, inspections and monitoring of:

- Audit and inspection logs and findings
- Security alerts from security experts and suppliers
- Insider risk indicators
- Security incident registers and investigations
- Feedback on security treatments or procedures
- Implementation progress and effectiveness of treatments

Changes to organisation goals, plans, functions or responsibilities

- Increased public attention to any policy or service.

Ask the following questions:

- Are the assumptions, including those about the environment, threat, vulnerabilities, technology, and resources still valid?
- Are the treatments being implemented properly or fully?
- Are stakeholders impacted by the treatments satisfied?
- Is the risk management plan being effectively maintained as risk treatments are implemented?

Evaluation

Evaluate the security risk management plan at least annually to determine whether security objectives are being achieved in the most cost-effective way.

Ask the following questions:

- Do the security measures comply with legal, regulatory and policy requirements including access, equity, ethics, and accountability?
- How has the organisation's risk appetite changed?
- How effective have current and previous countermeasures been?
- What improvements can be made? How can they be implemented?

7.0 Security Incident Investigation Handbook

This handbook provides good practices you should use when undertaking security incident investigations.

Step 1: Interim measures while an investigation is underway

In some circumstances it will be appropriate to take interim security measures while an investigation is underway. What is appropriate will be different in every case. It is important to balance the need to protect people, information, or assets with the employment obligations of natural justice.

Interim measures to consider may include:

- conducting an audit of relevant information
- monitoring computer usage
- monitoring building access
- limiting computer access
- removing computer access
- limiting after-hours access to place of work
- removing access to a place of work (following decision to suspend having followed due process).

Any response must be justifiable and proportional to the concern held, and appropriately directed to protect any people, information, or assets potentially at risk. It must be an interim step to protect people, information, or assets while the security investigation is underway.

Step 2: Determine who needs to be involved and select an investigator

If a security investigation is initiated, get advice from the CIPS or Chief of Staff, Office of the Prime Minister as Chair of the National Security Committee when a violation may involve national security or criminal behaviour.

If an incident requires more than one type of investigation, work with the other organisations to determine priorities and an investigative approach.

Select an investigator

Appoint an investigator who is appropriately trained and qualified. They should be impartial. They must not have a conflict of interest, real or apparent, in the investigation.

If the investigator you appoint does not have the power or authority to collect any evidence, or if a conflict of interest comes up, refer the investigation to a person or organisation with the necessary delegations.

An investigator's key tasks should include:

- understanding the incident and the terms of reference
- identifying the relevant law, policy or procedures
- gathering all relevant facts
- verifying whether the incident is an offence
- reporting the findings, and the reasons for the findings
- making recommendations.

Step 3: Set procedures for investigating security incidents

The organisation should set policy and procedures for investigating security incidents. It should include these requirements:

Your organisation's investigation processes:

- general and organisation-specific legislation and powers
- inter-organisation relationships and agreements
- methods for managing and supporting investigations
- investigation practices
- investigation report or brief of evidence
- information privacy rules
- investigation result and review
- recovery actions.

Responsibilities and actions:

- Responsibilities of the investigator and senior management
- What to do when receiving a complaint or allegation, including anonymous allegations and reports from whistle-blowers
- Terms of reference for the investigation
- When to refer security investigations to the CIPS or other outside organisations.

Procedures:

- Standards of ethical behaviour by investigators, recording activities, and how you manage investigation cases
- Procedures for operations like holding interviews.

Requirements for reporting:

- Maintaining detailed file notes

- Keeping senior management informed of the progress
- A final report that includes background information
- Summary of major findings and recommendations.

Step 4: Plan the investigation

At the start, assess:

- whether the investigation is likely to be a criminal, security or other type of investigation
- resources needed
- legal boundaries for the investigation
- authorisation needed
- nature of the possible outcome.

Set the terms of reference for investigations

The terms of reference should be clear, comprehensive, and include any limits. They could include:

- the background
- resources allocated (for example, people, financial)
- timeframes
- types of inquiries to be conducted
- powers of the investigating officer to collect evidence
- the format for reporting
- any special requirements or factors specific to the investigation.

Also cover how the investigator will collect evidence, such as:

- from policies, processes, and practices
- from relevant records and material
- through interviews
- by search and surveillance.

At the start of an investigation, appoint a senior staff member to approve the terms of reference and the investigation plan.

Assess the incident

The investigator should assess:

- relevant laws
- the nature of the incident

- the incident's seriousness and its possible level of harm to the organisation or government
- whether the incident shows there is a systemic problem
- whether it is part of a pattern
- whether it may breach Cook Islands law.

Develop an investigation plan

Use the incident assessment to prepare an investigation plan that identifies:

- the key issues to be investigated
- any relevant legislation, provisions of a code of conduct, organisation policy and procedures, standards and requirements
- required evidence
- methods for collecting the evidence
- legal requirements and procedures to be followed in collecting evidence
- allocation of tasks, resources
- timing.

If the terms of reference and the investigation plan need to change during the investigation, the investigator should consult the person who authorised the investigation.

Step 5: Undertake the investigation

Gather information

An investigator identifies, collects and presents information proving or disproving the facts relating to the incident. Types of information are:

- physical
- documentary
- oral
- expert advice.

Record and store all evidence

Investigators should keep a separate file for each investigation. Store it, and any physical evidence, securely.

The file should be a complete record of the investigation. Document every step, including dates and times, all discussions, phone calls, interviews, decisions, and conclusions. Include how physical evidence was handled.

If any protectively marked information was gathered or created during the investigation, investigators must meet the standards for storage.

Prepare the investigation report

The investigator should report findings to the Senior Staff Member who authorised the investigation or the HOM. They should identify the reasons for the findings according to the terms of reference, use supporting material, and make recommendations.

Close and review the investigation

An investigation is closed when all reports are completed, and evidence is documented and filed.

An independent person, ideally more experienced than the investigator, should review the closed investigation. They should impartially assess the investigation, and identify how to improve requirements for future investigations.

8.0 Supply Chain Management Handbook

This supply chain management method is intended specifically for the assessment and management of security risks when working with others across your end-to-end supply chain.

Step 1: Know who you do business with and understand the risks

Conduct an analysis of your supply chain to understand the organisations involved (including who supplies to them or supports them) in the delivery of your organisation's products and services.

Understand your suppliers' current security arrangements and practices and how well they comply with your security requirements.

Try to establish the answers to the following questions.

- How effective are your suppliers' current security arrangements? How long have their arrangements been in place?
- Which security measures have you asked your immediate suppliers to provide? Which measures have they, in turn, asked their sub-contractors to provide?
- Have your suppliers and their sub-contractors provided the security requirements you asked for?
- What access (physical and technological) will your suppliers have to your systems, facilities, and information? How will you control that access?
- When suppliers are working on your facilities, what other information (beyond the information you have granted them explicit access to) might they be able to access or view?
- How will your immediate suppliers control their subcontractors' access to, and use of, your information and assets? (Remember to include your systems and facilities).

Understand what access your suppliers have

Understand what access your suppliers have to your systems, facilities, and information and how control it. You should know:

- the sensitivity of contracts and agreements you have
- the value of the information or assets that suppliers hold, access, or handle as part of their contracts and agreements with you
- the impact on your organisation of loss or harm to information or assets that suppliers hold, access, or handle.

Think about the level of protection your suppliers need to provide for your assets and information as part of the contract, as well as the products or services they will deliver.

Step 2: Define & communicate your protective security requirements to others

Identify your supply chain protective security requirements based on the classification of the information and assets used.

Specify the minimum employment checks you expect your suppliers to conduct for their personnel including any sub-contractors that they use. Align your suppliers' minimum checks with the base employment checks conducted by you and your partners. Make sure your suppliers and their personnel understand their responsibility to protect your information. Make sure they understand the implications of failure.

Step 3: Build security considerations into your contracting processes and require your suppliers to do the same

Build security considerations into your normal contracting processes. This approach will help you manage security throughout the contract, including terminating and transferring services to another supplier.

Before contracts are signed

If you are a contract manager, work with your CSO or their delegate, to identify essential security requirements when you are developing tender documents, and for the life of the contract. This step also applies to anyone who is evaluating proposals or tenders.

Get prospective suppliers to provide evidence of their approach to security and their ability to meet the minimum-security requirements you have set. If the supplier is unable to meet your minimum-security standards, you should not select them.

If you award a contract subject to a supplier meeting your requirements, ensure you follow through and verify they meet requirements before allowing their contract to start.

Consider including the right to terminate the contract if your supplier fails to comply with your security requirements. Failure to comply should include the supplier being unwilling or unable to remedy security breaches.

Ensure you clearly understand which information and assets your supplier will hold on to on your behalf. Reach and document an agreement on how your information and assets will be managed and disposed of. Include conditions that protect information from risk.

It is best to seek legal advice when developing contracts.

Contract terms and conditions

Consider including relevant terms and conditions in your contracts based on the nature of the contract and the level of access that they will have to your information, assets, and facilities.

Handling protectively marked information

- Explicitly identify the highest level of protectively marked information the supplier will access during the contract.
- The supplier must ensure their people are cleared to the appropriate level before they are given access to protectively marked information.
- The supplier must prevent all access to protectively marked material by people whose security clearances have lapsed, been downgraded, or revoked, or are no longer needed.
- Where relevant, include conditions requiring the supplier to report to you when any of their people who do not have a security clearance have any incidental or accidental contact with protectively marked material. This condition is particularly important in contracts for security guards, cleaning, and ICT services.
- The supplier's site and facilities must meet the minimum standards for storing and handling official information.
- Consider the impact of any loss or compromise of your information held by a supplier, especially collections of information. Include contract conditions to mitigate any assessed risks.

Permission for subcontracting

- The supplier cannot subcontract a service or function that may require access to official information without your organisation's written approval.
- Once a subcontracting agreement is in place, the supplier cannot change the subcontractor without your written approval.

Conflicts of interest

- The supplier must disclose any potential conflicts of interest that would affect security when they work on behalf of the Cook Islands Government.

Information security

- The supplier must have systems that meet agreed information security standards for processing, storing, transmitting, and disposing of official information that is in electronic formats.

Confidentiality

- The supplier must follow directions included in the contract for keeping your information confidential. Confidentiality obligations may extend beyond the end of the contract.

During the contract

Provide or develop supporting guidance, tools, and processes, so you and your suppliers can effectively manage security at all levels throughout your supply chain. Train all parties in their use.

Require contracts to be renewed at appropriate intervals and reassess risks at the same time.

Seek assurance that your suppliers understand and support your approach to security. Only ask them to act or provide information when it's needed to manage supply chain security risks.

Step 4: Meet your own security responsibilities as a supplier and consumer

You may supply products and services to others. Ensure that you enforce and meet any requirements on you as a supplier.

Report to your senior management team so they know how security is being managed.

Pass security requirements down to your suppliers and sub-contractors.

Welcome your customer's audits, tell them about any issues you encounter, and work proactively with them to improve security.

Challenge your customers if they do not provide guidance about their security needs. Seek assurance that they are happy with the measures you are taking.

Step 5: Build education, assurance, and support activities in your supply chain management

Communication and education

Supply chain management is a shared issue, so build strategic partnerships with your key suppliers. They are more likely to follow your approach to supply chain security when it takes account of their needs as well as your own. Encourage and value their input and share security issues with them. Maintain regular and effective communication.

Supplier relationships can interact with many of your organisation's touchpoints. So, it is important to educate your people about how contracts will operate and what the associated security arrangements are.

Explain security risks to your suppliers using language they can understand. Encourage your suppliers to explain the risks to their people (especially if they work in procurement, security, and marketing), so they know their responsibilities to help manage them.

Your supplier's people may change over time due to staff turnover or role changes. Work with your suppliers to ensure that:

- people who accessed official or protectively marked information are reminded of the continuing need to maintain confidentiality
- new people understand your security requirements.

Share security information and lessons learned across your supply chain to keep them up to date with emerging security attacks. Help to stop them become victims of 'known and manageable' attacks.

Assurance

When suppliers are key to the security of your supply chain, make it a condition of their contracts to:

- report to your senior management team on security performance
- follow any risk management policies and processes you specify.

Build the 'right to audit' into all contracts and exercise it. Require your suppliers to do the same for contracts they sub-let. Audits may include accessing the supplier's premises, records, and equipment. (However, this may not always be possible or desirable, particularly when a service is cloud-based.)

When you assess suppliers that offer services to more than one government organisation, consider sharing the assessment to avoid duplication.

Where justified, build assurance requirements into your security requirements. For example, assurance reporting, penetration tests, external audits, and formal security certifications.

Establish key performance indicators to measure the performance of your supply chain security management.

Review and act on any findings and lessons learnt.

Encourage suppliers to promote good security behaviours.

Provide support for security incidents

It is reasonable to expect your suppliers to manage security risks according to their contracts. But be prepared to provide support and assistance if necessary. For example, when security incidents could potentially affect your business or the wider supply chain.

In your contracts with suppliers, clearly set out requirements for managing and reporting security incidents or breaches.

Clarify their responsibilities for advising you about incidents. For example, make it clear how soon after an incident they need to report to you, who the report should go to, and so on. It is particularly important to ensure your service providers report incidents or suspected incidents that affect:

- their ability to deliver their contracted services
- your organisation's information.

You should also clearly state what support your suppliers can expect from you following an incident. For example, support with clean-up and handling losses.

Consider clarifying how your supplier will manage security incidents or breaches.

Consider including contract conditions that require providers to report to you about breaches of ICT security that involve other clients' information.

Step 6: Encourage continuous improvement of security within your supply chain.

Encourage your suppliers to continuously improve their security arrangements. Advise and support your suppliers as they work on improvements.

Emphasise how improving security may help them to compete for and win future contracts with you. Taking this approach will help you grow your supply chain and increase your pool of potential suppliers who meet your security needs.

Avoid creating unnecessary barriers to improvements. Be prepared to recognise any existing security practices or certifications they have that demonstrate how they meet your minimum-security requirements.

Allow time for your suppliers to improve security but require them to give you timescales and plans that show how they intend to achieve the improvements.

Listen to and act on any concerns that suppliers highlight — concerns which suggest current approaches are not working. Suppliers might raise issues during performance monitoring, through reporting, or after responding to security incidents.