Ministry of Communications & Information Technology

Cyber Security Incident Response Standard

Table of Contents

1 Introduction 4
1.1 Purpose and Scope 4
2 Roles and Responsibilities 5
3 Logistics and Communications 8
3.1 Communications Plan 9
4 Definitions and Incident Types 12
4.1 Cyber Security Definitions 12
4.2 Cyber Security Incident Categories 13
5 High Level Incident Response Process 14
6 Phase: Prepare 16
6.1 Prepare for an Incident 16
7 Detect & Analyse 17
7.1 Detect 17
7.2 Analyse 18
8 Containment, Evidence Collection & Eradication 19
8.1 Containment 19
8.2 Evidence Collection 20
8.3 Eradication 21
9 Recover 23
9.1 Recovering from an incident 23
9.2 Reporting an incident 24
10 Learn and Improve 25
10.1 Learn 25
10.1.1 Post Incident Review (PIR) 25
10.2 Improve 26
10.2.1 Implement the lessons learned 26
10.2.2 Implement the lessons learned 26
Appendix A – Contact Lists 28
SamCERT and Wider Incident Response Team / Stakeholders 28

Senior Leadership 28
External Stakeholders 28
Appendix B – Incident Classification 29
Appendix C - Evidence Collection and Document Preservation SOP 31
Appendix D – Evidence Register 33
Appendix E – Remediation Action Plan Template 35
Appendix F – Chain of Custody Template 36
Version Management 38

1 Introduction

The Cyber Security Incident Response Standard has been developed to protect the Government of Samoa's information assets and people from cyber security incidents that impact their confidentiality, integrity, or availability.

Cyber incidents have the potential to cause severe impacts to the Government of Samoa (GoS), which highlights the importance of having effective, tested, and consistent processes in place that allow for any impact to the GoS or its citizens to be mitigated and minimised.

1.1 Purpose and Scope

The purpose of the Cyber Security Incident Response Standard is to define the need for an overall approach to cyber security incident response at the GoS. As such, the objectives of this document are to:

- Define cyber security events and incidents.
- Define the category and severity of an incident.
- Identify the steps required to respond to cyber security incidents within GoS.
- Outline the roles, responsibilities, accountabilities and authorities of personnel and teams required to manage responses to cyber security incidents.
- Outline internal and external communication processes when responding to cyber security incidents.
- Outline legal and regulatory compliance requirements for cyber security incidents.
- Provide guidance on post-incident activities to support continuous improvement.

Several Standards and Frameworks have been leveraged to support the development of the Cyber Security Incident Response Standard, including:

- Australian Government Information Security Manual (ISM)[1]
- Protective Security Policy Framework (PSPF) [2]
- NIST Computer Security Incident Handling Guide (NIST SP800-61 Rev 2)[3]

These documents present best practice guidance from both regional neighbours and internationally recognised publications.

This Standard sets out the expected response for cyber security incidents that affect the IT systems managed by the GoS – including GoS systems and data in externally hosted networks (if and where applicable).

[1] https://www.cyber.gov.au/acsc/view-all-content/ism

[2] https://www.protectivesecurity.gov.au/

[3] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

2 Roles and Responsibilities

In the event of an incident, Staff will be assigned temporary, incident-specific roles to enable an effective response to security incidents. These roles are outlined in Table 1.

Contacts Lists for members of SamCERT and other relevant internal and external stakeholders are identified in Appendix A – Contact Lists

.

Table 1: Roles and responsibilities for incident response at GoS

Role	Responsibilities
SamCERT / ICT Teams	• Receive reports of confirmed or suspected cyber security incidents from staff via means including but not limited to the dedicated SamCERT email, phone number, or website and other reporting alerts or mechanisms. • Triage activity and information from the reports of a given event and if deemed to be a cyber security incident, escalate and assess and rate the severity of the incident.
GoS Staff	• Responsible for notifying the SamCERT or ICT Team of any confirmed or suspected cyber security incidents via the above reporting methods, as soon as possible. • Be open and transparent when providing information about potential incidents and cooperate with incident responders and other key stakeholders.
Senior Leadership	• Senior leadership at the GoS and Ministry of Communication, Information and Technology (MCIT) will ensure that they receive advice from the Incident Response Team for cyber security incidents assessed as High and Critical in severity. • Report information regarding incidents upwards (e.g., to personnel such as Ministers or Digital Transformation committee) as required.

Incident Response Roles for the immediate SamCERT team:

Table 2: Roles and responsibilities for immediate incident response

Role	Responsibilities
SamCERT	SamCERT will be the primary response body and is led by the Cyber Security Incident Response Manager (IRM). Other members of the incident response team, who will support SamCERT in the incident response efforts include: • Other external parties from incident response teams / CERTs • Technical leads from the relevant GoS Ministries and agencies with the required skills and knowledge to support the investigation and remediation of cyber security attacks.

Incident Response Manager (IRM)	The IRM is the member within the SamCERT who leads the incident and coordinates with business owners and managers to authorise SamCERT's actions to ICT systems and works with business managers to make appropriate decisions to remediate the incident. • The IRM will report to the CEO of the MCIT and other senior leadership or security forums throughout the GoS (as appropriate) during and following the closure of an Incident.
Incident Responders	Incident Responders will lead the technical, analytical and response actions through all incident response phases. • Incident Responders will be dedicated to their role within the team. Other duties (such as communications) will be assigned to the broader team members, subject matter experts (SMEs), or other staff delivering responder BAU responsibilities.
Technical Leads (SMEs)	Technical leads are SMEs or specialists from other Ministries or Agencies (most likely the infrastructure, network, database, application development or other ICT teams) who have significant knowledge or understanding of an IT system or data asset impacted by a cyber security incident. These personnel may be needed during certain stages of an incident and during incident handling to support the activity of the immediate incident responders.

Incident Response Roles for the broader Incident Management Team (IMT):

Table 3: Roles and responsibilities for broader Incident Management

Role	Responsibilities
Incident Management Team	The Incident Management Team (IMT) is a broader subset of stakeholders who make up the IRT, but do not necessarily play a hands-on technical role in the response efforts. The IMT is responsible for managing the holistic response to cyber security incidents to allow for the immediate responders to conduct technical activities. IMT members include: • CERT E.g., SamCERT Chief Cyber Security Officer (CCO) • Observers, Ad-hoc members • Ministry ICT Officers (as required) Other interested parties may include: • Human resources and/or legal representatives • Media/communications advisor • Any other relevant parties
Cyber Security Incident Manager (CSIM)	Due to the size of the Incident Response Team, the CSIM responsibilities may be delegated to the Incident Response Manager. The CSIM reports to the Cyber Security Executive and provides support to the IRM, as well as making decisions relating to containment of cyber security incidents. The CSIM will be responsible for coordinating the involvement of interested parties described above, e.g., media, legal, HR and other teams.

Observers/Ad-Hoc Members	These members of the IMT include Senior Executives (e.g. CEO's, Ministers) who may be consulted for incidents impacting GoS ICT systems and assist on an ad-hoc basis, for example, to coordinate assistance for incidents impacting GoS systems.

3 Logistics and Communications

SamCERT's core logistical and communications protocols, and mechanisms to support incident response are as follows:

- Operations Room located at/on Ministry of Communications and Information Technology (MCIT), TATTE Building Level 6, Apia, Samoa
- Fit for purpose PCs, network connectivity and security log/SIEM access, including contingencies in the event the loss of availability of GoS's network.
    - To ensure devices are fit for purpose they should have processes for updates, patching and other service and operational packages to ensure they are current, correct and up to date – ready and able to be immediately deployed.
- Multiple methods of communicating between groups and individuals as set out in Table 4 below, including:
    - Phone/SMS
    - WhatsApp
    - Zoom
    - Email
    - In person

  It is important that at least some forms of communication are out of band (OOB), which means it does not require or rely on infrastructure or systems that form part of, or otherwise connect to, a compromised system or network.

  Incident response and management teams should primarily leverage OOB communication methods internally to protect their discussions and any information, as threat actors may compromise internal networks and systems, giving them the ability to eavesdrop on communications.

3.1 Communications Plan

The Communications Plan in Table 4 supports the Government of Samoa in ensuring a coordinated and efficient approach for notifying relevant internal and external stakeholders in the event of cyber security incident.

Table 4: The communication requirements for Incident Response

ROLE	Type	Purpose	Stakeholders	Method* Ensure that those used are not compromised. Assume compromise if unable to verify	Timeframe/Frequency
Cyber Security Incident Manager (IRM)	Internal	To notify Senior Cyber Security Stakeholders, relevant Senior Leadership, and key security personnel that a **High** or **Critical** severity cyber security incident has occurred.	CEO, Minister, Cabinet Subcommittee for ICT, Digital Transformation Unit	Phone, email, Zoom and in person.	Within 30 minutes of determining a **High** or **Critical** severity cyber security incident has occurred.
	Internal / External (if affected parties are external)	Provide status updates on **High** or **Critical** severity cyber security incident response activity.	IMT (and where applicable, other external responding bodies)	Phone, email, Zoom and in person	As determined by the head of SamCERT and if the CSIM is a different person, as agreed with the CSIM.
	External	Report cyber security incidents and if required, request assistance.	Trustwave, APNIC, ACSC, PACSON, NZCERT	Phone, email, Zoom	Within 12 hours for **High** or **Critical** severity cyber security incidents.
Chief Cyber Security Officer	Internal	Notify stakeholders of **Critical** severity Cyber Security Incident and ongoing incident response status.	CEO, Minister, Cabinet Subcommittee for ICT, Digital Transformation Unit, Cybercrime Unit, Cabinet	Phone, email, Zoom and in person	Within 30 minutes of being notified that a cyber security incident has occurred, and the incident severity has been assessed.

ROLE	Type	Purpose	Stakeholders	Method	Timeframe/Frequency
SamCERT	Internal	Notify stakeholders of incident causing outage or performance reduction	SamCERT Team and CCO	Email, Phone and in Person	Within 60 minutes of being notified that a cyber security incident has occurred, and the incident severity has been assessed.
	Internal	If a media release is required, must provide technical context of the incident. Technical context may include systems/services affected, steps being taken to resolve the incident & who incident responders are working with to support incident remediation.	Communication Team / personnel	Email and in Person	As directed by the IRM/CSIM.
	Internal	Notify stakeholders of Data Breach cyber security incident	Privacy (or other related) Team or SME.	Phone, email and in person	Upon confirmation that a data breach has occurred by the IMT.
Chief Cyber Security Officer	Internal	Notify / consult	System Owners (inclusive of Ministries who own Systems)	Phone, email and in person	Where an incident is affecting systems owned by Systems Owners and to seek expertise from Technical Leads to support incident responders.
Communication Team / personnel	External	Notify Minister's office	Minister, Public	Phone and email	Where an incident is assessed as having high reputational damage, per Appendix B – Incident Classification

Privacy Team or SME	External	Notify external stakeholders of a Data Breach incident.	SamCERT Privacy SME Team Affected individual(s)	Phone, email and in Person	As soon as a Data Breach is determined to have occurred (this may or may not be determined by legislation)

4 Definitions and Incident Types

4.1 Cyber Security Definitions

Cyber security definitions have been derived from industry best practice publications, agencies and frameworks.

Term	Definition
Cyber security threat	Any circumstance with the potential to adversely (negatively) impact GoS operations, organisational assets, individuals, or Samoa through a system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service. Examples of cyber security threats include: • Phishing emails and related impersonation scams • Ransomware • Exploitation of security vulnerabilities • Software supply chain compromise • Business Email Compromise (BEC)
Cyber security event	A cyber security event is an observable occurrence of a system, service or network state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security. A cyber security event has the potential to become, but is not confirmed to be, a cyber incident. Examples of cyber security events include but are not limited to: • Anti-virus being disabled on a computer • System files being modified or deleted from a computer • A server having an unscheduled restart • A detection of a possible scan of a machine or machines in the IT environment • A server receiving a request for a web page • An employee connecting to a file share • An employee sending email
Cyber Security Incident	A cyber security incident is a cyber security event, or a series of such events, that have a been determined to have had an impact on the GoS and requires the need for response and recovery Examples of cyber security incidents include but are not limited to: • Denial of Service (DoS) or Distributed Denial of Service (DDoS) Attacks • Unauthorised access or attempts to access a system • Unauthorised access to sensitive information that exposes it to the risk of exfiltration • Virus or Malware outbreak (including Ransomware) • Any activity that threatens the confidentiality, integrity, or availability (CIA) of the GoS information assets or people.

4.2 Cyber Security Incident Categories

The following table outlines the type of categories incidents may fall into. The purpose is to assist incident responders in identifying and classifying the activity that they are experiencing.

Type	Description
Credential Based Unauthorised Access	Attempts to access systems using breached credentials, brute-force attempts, or bypassing multi-factor authentication.
Data Breach	Unauthorised access, exfiltration, and sometimes disclosure of information.
Denial of Service (DoS)	An event where a computer-based service or network is overwhelmed with traffic, sometimes impacting the availability of the resource. Attacks of this nature intend to overload the target and its ability to operate by consuming the available bandwidth or processing capacity of the server hosting the service.
Distributed Denial of Service (DDoS)	A type of Denial of Service (DoS) where the attack source is comprised of multiple, distributed unique IP addresses used to flood the bandwidth or resources of a targeted system or network.
Exploitation of Security Vulnerabilities	Malicious actors exploiting security vulnerabilities either known or unknown (zero day) to gain unauthorised access to devices and systems.
Malware	A Trojan, virus, worm, or any other malicious software that can harm a computer system or network.
Phishing	Deceptive messaging designed to elicit users into responding and divulging sensitive information (such as banking logins or business login credentials). Phishing can also be used as a method to have a user execute malicious code to enable unauthorised access
Ransomware	A tool or malware used to lock or encrypt victims' files until a ransom is paid.
Software Supply Chain Compromises	Events where malicious cyber actors exploit cyber supply chains (e.g., in supplier hosted software) to gain access to your organisation's devices and systems[4].
Spoofing or Impersonation	A malicious actor purports to represent the GoS or one of its programs via email, SMS or some other medium.

Note: *This list is not exhaustive of cyber security incident types and should only be considered a point of reference.*

[4] https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21

5 High Level Incident Response Process

SamCERT follows a five-step incident response process. The following section provides a high-level summary of the activities that support and make up each phase.

Phase 1: Prepare

SamCERT has:

- Prepared plans, processes and supporting documentation, including this Standard, Incident Response Playbooks, operating procedures for systems and the Information Asset Register.
- Established, through this Standard a Cyber Security Incident Response and Team (e.g. SamCERT and supporting personnel) with management responsibilities (e.g.IMT) to respond to and manage cyber security incidents.
- Developed arrangements to reduce the impact of key cyber security personnel unavailability on the workforce should a cyber security incident require prolonged staff engagement or additional incident response specialist resources.
- Planned arrangements for maintaining the incident response capability in the event of a loss of, or compromise of the network used by SamCERT – including non-domain joined laptops and a segregated cloud environment (if resources permit) to investigate, communicate and case manage the incident.
- Developed mandatory security awareness training for staff and ensured that the Standard and any relevant Playbooks have been reviewed and tested to ensure they remain current and that responsible personnel are aware of their roles, responsibilities, and processes.

Phase 2: Detect and Analyse

SamCERT:

- Has implemented and maintains cyber security incident detection capabilities, including alerts generated from centralised logging tools, internal reporting from staff, provisioning of threat intelligence from threat intelligence sources and groups, email gateway logs, firewall logs, intrusion detection or Intrusion prevention systems (IPS/IDS), and SIEM technologies.
- Will assess and triage incidents or reports, using the incident classification process in Appendix B – Incident Classification

- **Error! Reference source not found.**
- Has established means for internal and external individuals and organisations to report cyber security incidents to the SamCERT team**.**

Phase 3: Contain, Eradication and Evidence Collection

- Activity to contain and remediate a cyber security incident will be coordinated by SamCERT**.** This activity involves containing the effects of the incident on the targeted system(s), putting in place controls to remediate the system(s) and continuing to monitor the compromised system(s) for signs of further unauthorised activity. Containment actions may include disabling of internet access, disabling user accounts, isolating devices, isolation environments, and blocking Indicators of Compromise (IoCs).
- It is critical that during this time, the Incident Response team and SamCERT will collect and securely store event logs and evidence in accordance with the Evidence Collection and Preservation SOP (See **Error! Reference source not found.**. If required, other third-party a ssistance with incident response activity will be requested.
- Depending on the nature of the incident being faced, the IRM (the primary lead authority of the incident) sets the timeframe and coordinates remediation activities and actions.

Phase 4: Recovery

- The incident response team, including Technical Leads, will recover the affected system(s) and services back to a BAU state.
- The IRM/Incident Responder(s) will determine and implement solutions to prevent and detect a repeat incident.
- The IRM will report the incident to the Government agencies (if required), the IMT (if this is a separate person) and where applicable, other senior stakeholders or security committees.
- Other reporting and notification required to go to external individuals and organisations in accordance with the Communications Plan and any other relevant reporting obligations.

Phase 5: Learn & Improve

- SamCERT will conduct a Post Incident Review, including input from internal and external stakeholders involved in the incident handling process.
- The incident will be closed and any recommendations arising from the review will be documented in the SamCERT Action Register.
- The Incident Response Standard is updated along with any templates and playbooks, and any changes are communicated to broader staff.
- Targeted education to impacted users or broader department regarding threats identified during an incident will be provided.

The next sections of this Incident Response Standard will go into each of these phases in more detail and explain the necessary steps followed by SamCERT when responding to a cyber security incident.

6 Phase: Prepare

Derived from regional sources he GoS has defined the baseline definitions and incident categories in **Section** 4 Definitions and Incident Types. These definitions are designed to assist the GoS in understanding and preparing for incidents, understanding what they may be and subsequently aiding the preparation of the government to respond to an incident.

6.1 Prepare for an Incident

Preparation for an Incident needs to be done prior to the incident taking place. Therefore, it is required that the GoS, MCIT and SamCERT have undertaken the following actions to prepare for a potential incident:

- Developed and maintained an Incident Response Standard (this document) and any associated playbooks or detailed procedures.
- Implemented hardening practices (reduced vulnerability in technology applications, systems, infrastructure, firmware, and other areas) and conducted regular reviews on its effectiveness (such as email filters, logging, and monitoring).
- Identified and documented IT assets, government assets, government network components and connections, and any third-party IT arrangements.
- Ensured that effective methods are made available to internal and external parties to report events or incidents, and that this platform is maintained and routinely tested.
- Assessed the risk of IT systems and provided authorisation for systems to operate prior to go-live, including the evaluation of the effectiveness of a system's security controls and architecture.
- Ensured that SamCERT team members are aware of and have access to all tools and equipment required to carry out their incident response tasks.
- Ensured processes are in place for GoS's ICT staff to regularly review all critical asset data backups and disaster recovery plans to ensure resilience during a ransomware attack.
- Developed training for employees on how to effectively identify and respond to common incidents such as phishing.
- Ensured processes are in place to review recent cyber incidents that have affected the GoS and mitigating gaps in detection and response to malware infections.

7 Detect & Analyse

The objectives of the Detect and Analyse phase are to ensure that:

- SamCERT is alerted to the breach or compromise of the confidentiality, integrity, or availability of a system or data asset.
- An initial assessment and investigation are completed to confirm the event is in fact an incident.
- The scope and nature of the incident has been determined.
- The potential impact of the incident has been analysed to assign an incident severity. (This triage will leverage the Government of Samoa Risk Management Framework and augmented by the understandings of cyber security incident types/profiles, and Appendix B – Incident Classification
-).

SamCERT is activated to manage incidents. If further assistance or technical expertise is required, other stakeholders within the GoS, third-party incident response arrangements or other support arrangements may be called upon (with appropriate approval).

7.1 Detect

When a staff member or external party notices an anomaly or other event in data, a system, the network, or a system alert generates an event - ICT managers or SamCERT must perform an initial investigation and verification of the event.

SamCERT will receive reports from GoS staff when they become aware of the presence of a compromise of a system/IT infrastructure or receive suspicious emails. Incidents may also be detected via alerts generated on systems such as network scanners, systems not responding or running slow, an abnormal and high amount of network bandwidth allocation, excessive Active Directory access attempts or alerts regarding suspicious files or processes.

SamCERT will validate whether a Cyber Security incident has occurred and determine the incident scope and timeline. During this initial detection and identification phase, the team will:

- Determine if an incident has indeed occurred or if it is a false positive. This will require an investigation of events and data available, potential IoCs and other symptoms present at the time of the report.
- Assemble the broader incident response team once an incident is confirmed.
- Use the SamCERT incident management / ticketing system to track the response process for all incidents – an incident ticket should be raised for ALL events, and each should be managed as an incident until proven otherwise.
- Update the Incident response run sheet and communication plan as soon as an incident is declared by the SamCERT.
- Store all the information, documentation and evidence related to the incident (collected throughout the lifecycle of the incident) in a secure location only accessible by authorised

personnel. Further guidance can be found in Appendix C - Evidence Collection and Document Preservation SOP

7.2 Analyse

To eliminate doubt, and to prevent other non-malicious events being pushed down the analysis path, SamCERT will investigate and analyse the extent of the cyber security incident(s) to understand their impact or potential impact to GoS assets.

To determine the incident scope, SamCERT will need to take into consideration the following factors:

- How many systems are currently impacted?
- What type of data / information / networks / systems assets are involved? Are they confidential or protected?
- Potential likely entry vector(s) from which the incident was able to originate (e.g., did the incident occur via the internet or other web-client/server, did it come from a physical source, did it originate on/in the network)?
- What is the potential damage that the incident has/could cause?
- Based on the information at hand, what is the approximate time that recovery from the incident could take place within?
- What resources are required to manage the situation?

Once the scope has been determined and logged, the potential impact needs to be agreed on. When determining the impact of a cyber security incident, the team should consider (with guidance from the risk management framework impact table) the current and potential functional and informational impact of the incident, and its likely recoverability.

Once an impact assessment has been completed, an Incident Classification (as per Appendix B – Incident Classification

) must be assigned/revised and logged in SamCERT's incident tracking / ticketing tool.

8 Containment, Evidence Collection & Eradication

The objectives of the Containment, Eradication & Evidence Collection phase are to ensure that:

- The effects of the incident are contained on targeted system(s) and do not spread to other assets.
- Artefacts and evidence of the incident are identified, collected, and preserved securely for analysis and any legal requirements or purposes.
- The incident is eradicated from the network through mitigation measures as defined by the incident response team (depending on the level of severity of the incident).

8.1 Containment

SamCERT will implement containment actions to minimise the damage, prevent the incident from spreading or escalating, and prevent attackers from destroying evidence of their attack. The focus of containment actions is primarily to prevent further impacts to systems while eradication measures are determined.

Containment involves both short-term and long-term measures. Short-term containment measures focus on mitigating immediate impacts and preventing their spread to other systems, either by a short-term fix or, for example, by isolating the network segment.
After the initial impacts have been mitigated a long-term containment measure must be put in place which includes (but not limited to) temporary fixes to allow systems to be used in production while rebuilding clean systems.

> It must be ensured that any production systems made available during the rebuilding of clean systems, are thoroughly isolated and protected from any impacted (or potentially impacted) system(s). Additional monitoring may be implemented to for assurance – i.e. full segregation from an issue or infected areas.

When planning containment actions, the Incident Response Manager (IRM) considers the following factors, which may vary based on the type of incident before approving an appropriate course of containment action to SamCERT:

- Any additional impacts there could be to systems/services
- Time and resources required to contain the incident
- Effectiveness of the containment solution (e.g., will it result in partial vs full containment of the incident)
- Duration that the solution will remain in place (e.g., temporary vs permanent solution)
- Any additional assistance required from a third party or other specialist and their response time

Prior to initiating Eradication measures, the team will need to consider whether the containment action that was taken was able to:

- Effectively control / stop the attacker or incident's ability to affect the network.
- Identify the affected system(s).
- Collect the compromised system(s) volatile data, memory image, and disks are imaged for analysis.

8.2 Evidence Collection

Incident responders will collect event logs and evidence in accordance with the Evidence Collection and Preservation SOP (See Appendix C - Evidence Collection and Document Preservation SOP

A detailed log will be maintained that documents all the evidence collected which includes:

- Who collected or handled the evidence
- When the evidence was collected and handled
- The details of each item collected which should include:
    - The location
    - Serial number
    - Model number
    - Hostname
    - Media access control (MAC) address
    - IP address, and
    - Hash values.

See Appendix D – Evidence Register

for further guidance.

As the team works to contain, eradicate, and recover from the incident, the investigation will be ongoing. As the investigation proceeds, you may find that the incident is not fully contained, eradicated, or recovered. If that is the situation, it may be necessary to revisit earlier phases.

While the investigation and evidence will vary by incident type, commonly collected sources of information include the below, and may be stored for some time post incident for further analysis:

- Configuration files
- IP Addresses
- Disk/hard drive/host images
- Log files
- Screenshots
- Known Indicators of Compromise (IoCs)
- Memory/RAM images

8.3 Eradication

Following successful containment and the collection of all necessary evidence and data, incident responders will remove and eradicate malicious artefacts from compromised systems. SamCERT will ensure that as part of the remediation process, all relevant evidence will be collected following the process outlined in Section 8.2 Evidence Collection to ensure that complete investigations are carried out.

SamCERT will use a Remediation Action Plan to allocate and track the actions that will be taken to resolve the incident. To identify the steps required for eradication, the team will need to consider:

- Actions required to eradicate/resolve the incident
- What resources are required to resolve the incident (if not already included within the team)
- Whether additional external resources are required
- Personnel responsible for undertaking remediation actions
- What systems/services should be prioritised
- What systems/services will be affected during the remediation process and how these systems will be affected
- The expected resolution time
- How to test that the remediation steps are appropriate to prevent any recurrence of the incident, and that protective measures have been implemented successfully

Appendix E – Remediation Action Plan Template

contains the Remediation Action Plan that should be used to plan out the steps that the team deem necessary. This will identify:

- The date and time the action is/will be taken
- What purpose that action serves (e.g., to contain, eradicate or recover)
- A description of the action
- The person responsible for that action (action owner)
- The status of that action (e.g., is it yet to begin, in progress, closed)

Although eradication measures vary by incident type (sometimes not even being required), common measures taken include:

- Deleting malware and disabling breached user accounts
- Identifying and mitigating all vulnerabilities that were exploited
- Resetting active sessions for breached accounts
- Adding additional authentication controls (e.g. MFA, location black-listing)
- Closing all ports that are no longer necessary
- Implementing suitable monitoring and alerting if gaps were identified

Prior to beginning the Recovery phase, a number of key actions need to be considered:

- Has the investigation identified the root cause(s) and remediated identified vulnerabilities?
- Have all the impacted accounts (including any accounts created by the incident response team) had their credentials reset?
- Are the network and systems configured appropriately to prevent recurrence?
- Is there any evidence of repeat events or incidents?
- Have all notes and process issues been captured for review during the lessons learned phase?

9 Recover

The objective of the Recover phase is to ensure that affected system(s) are returned safely back into production and operations are restored. Once system(s) are restored, SamCERT will continue to monitor these for malicious activity that escaped detection, utilising methods such as network and host-based intrusion detection systems, intrusion prevention systems and checking operating system and application logs (to ensure that the attacker is not resident in the system).

All activities undertaken must be reported – both internally and externally (as appropriate).

9.1 Recovering from an incident

Following containment, the Recovery phase focuses on bringing the affected system(s) back online carefully. Reaching this step in an incident lifecycle does not mean the incident is over however, and SamCERT will continue monitoring affected system(s) to ensure they are back to normal activity and that the threat has been mitigated.

The methods of recovery will vary depending on the incident that has taken place, a system-specific recovery plan should be used to guide the approach to recovering key IT/OT systems, networks and applications following containment and eradication. Any such Recovery Plan must include:

- How systems will be restored to normal operation and expected timeframes.
- How systems will be monitored to ensure they are no longer compromised and whether they are functioning as expected.
- How identified vulnerabilities will be managed to prevent similar incidents.

If it is feasible, the system, application or network should be installed and trialled in a test environment to determine appropriate functionality, prior to being re-introduced to production.

Not all systems and applications will have documented Recovery Plans. Where one does not exist, the SamCERT and the incident response team must agree upon (and document) what recovery for a certain system or application will look like and execute steps to achieve this.

Typical steps that are taken during recovery include:

- Restoring a system from a clean and tested backup and replacing any corrupt data from a clean and tested backup.
- Restoring system, network or application connections, functions, and access.
- Implementing additional and appropriate monitoring activities on the network, application and or relevant systems (and determining how long these will continue).
- Communicating internally and externally (e.g., about monitoring, possible changes, resolution).

9.2 Reporting an incident

SamCERT use an Incident Response Tracking system to track the incident response process for all incidents. At this stage, where possible the incident responders will attach documents and notes to the initial ticket that was raised.

Although incidents will be reported internally in a Post Incident Report, the broader IMT must consider whether any other actions are required, including whether an incident needs to be reported to a regulatory body or external party.

For further information on reporting requirements please see Section 3.1 Communications Plan.

10 Learn and Improve

The final step in the incident response handling process is determining the lessons learned during an incident. The objective of the Learn and Improve phase is to document what happened, reach agreement on the facts, and improve SamCERT and the broader GoS's capabilities to prevent and respond to incidents in future.

SamCERT will conduct a Post Incident Review (PIR), including input from key stakeholders. The teams involved in the incident will reflect on their experience and openly communicate areas where improvements can be made.

The PIR may result in changes to the Incident Response Standard, SOPs and playbooks (along with procedural or network/application changes). Any changes will be documented and communicated to the relevant stakeholders and GoS staff.

10.1 Learn

The actions in the Learn and Improve phase involve evaluating the incident, taking any lessons learned and communicating these appropriately. The incident will be declared as formally closed upon ensuring that affected systems are fully restored and all actions and notifications are complete.

10.1.1 Post Incident Review (PIR)

To learn, the SamCERT will need to collate and gather all relevant details of the incident, the evidence collected, and the responses taken by the team. These will need to be formally documented and stored in a secure location – being held only for as long as is necessary (e.g., per evidentiary requirements).

The team will then conduct a Post Incident Review (PIR) which should typically be led by a knowledgeable resource from outside of the incident response team. A PIR is a detailed analysis conducted after a cyber security incident has been experienced, to ensure that the incident has been contained and removed from the system, and reflection upon the response and root cause can take place.

The PIR will reflect on what the documentation demonstrates and SamCERT observed when responding. This review should ask, establish and document:

- What happened and when?
- How well all staff (not just SamCERT) responded to and dealt with the incident
- Whether documented procedures were followed (or if any were missing)
- What information may have been needed sooner
- Were any steps taken that inhibited any of the response processes
- What things would you do the same, and what procedures/processes should be different or updated the next time a similar incident occurs?
- What information mechanisms were sufficient / need improvement (internal & externally)

- Are there any corrective controls that should be implemented now to prevent similar instances in the future?
- With respect to personnel capabilities, tooling and infrastructure, was the team sufficiently equipped to deal with the incident (from detection, analysis, mitigation, and recovery)?

Following the PIR and reflection of the incident, the incident response team will need to produce an Incident Report, which will need to document at a minimum:

- A timeline of all events from identification to recovery
- The method of recovery that was utilised
- The attack vector(s) and impact of the attack
- Preventative measures and mitigation steps implemented by SamCERT and others
- An assessment that determines whether the recovery undertaken is a temporary fix, and if additional recovery actions need to be taken
- Any other recommendations that should be considered

The purpose of this report is to identify potential areas of improvement and document the incident in its totality (including any broader recommendations and requests for resources).

10.2 Improve

10.2.1 Implement the lessons learned

Any lessons learned identified should be communicated to relevant teams where there is a requirement for process change, and socialised collaboratively outside SamCERT to include others that may benefit. This will also inform security awareness training targeted at the broader staff base.

SamCERT will update the GoS Incident Response Standard and any other documentation (e.g., playbooks, processes etc.) with lessons learned where appropriate. Significant changes may require the GoS Incident Response Standard and supporting Playbooks to be retested, in advance of the established frequency.

Regular testing is important to ensure these documents remain current and accurate, and are familiar to the relevant personnel. Testing methods may include round table discussions of the process or functional exercises and desk based scenarios and simulations (e.g., tabletops).

10.2.2 Implement the lessons learned

To continually improve and ensure that those that have a role in the CSIRT are able appropriately perform their roles, SamCERT will ensure the following training activities are conducted:

- On-the-job role-based training
- SIEM training (e.g., Elastic)
- Attendance of industry CERT / SOC events
- Attendance of relevant conferences e.g., PacSON, ITU trainings

- Simulations / tabletop exercises

Appendix A – Contact Lists

SamCERT and Wider Incident Response Team / Stakeholders

Name	Role	Contact Details (Phone & Email)	SamCERT/IR Responsibilities
Ronnie Aiolupotea	Chief Cybersecurity Officer	r.aiolupotea@mcit.gov.ws	Head of SamCERT
William Lafaele	Principal Cybersecurity Awareness and Engagement Officer	w.lafaele@mcit.gov.ws	SamCERT
Fiapaipai Sakuma	Principal Cybersecurity Incident Coordinator and Analyst	f.sakuma@mcit.gov.ws	SamCERT

Senior Leadership

Name	GoS Role	Contact Details (Phone & Email)
Lefaoali'i Unutoa Auelua-Fonoti	CEO	u.auelua-fonoti@mcit.gov.ws

External Stakeholders

Point of Contact	Organisation	Role	Contact Details (Phone & Email)

Appendix B – Incident Classification

The Government of Samoa's framework and decision-making process for classifying a cyber security incident is outlined in Table 1. Incident Responders and SamCERT can use this to classify the severity of the incident. Classification factors include:

- Effects of the incident (confidentiality, integrity and availability of information and systems)
- Stakeholders affected (internal and external)
- Incident type
- Impact on the government and community

Table 1: Guidelines for incident classification

Incident Classification	Descriptions	Incident Examples
Critical	Government or Ministry investigation with OPMC oversight (Severe impact) OR Government or Ministry investigation with Minister oversight (Major impact) **Information** • Severe or Critical financial impact • An information security breach resulting in serious or grave damage to national interest, the department, or officials • Significant or Severe breach to Whole of Government record management requirements. **Technology** • Causes significant delays or failure to deliver • Client & public dissatisfaction/loss of trust or contracts / agreements • Identified legislative breaches • Major impact on deliverables.	Sustained disruption of essential systems and associated services: • Ransomware • Denial of Service (DoS) and Distributed Denial of Service (DDoS) Exfiltration or deletion/damage of key sensitive data or intellectual property: • Ransomware • Data Breach
High	Ministry / Agency review of processes and systems and or departmental investigation with MCIT CEO oversight and Minister informed (Moderate impact). **Information** • Increased financial impact • An information security breach resulting in significant damage to national interest, the department, or officials. • Substantial breach to Whole of Government record management requirements.	**Malware, or other <u>active</u> network intrusion:** • Malware • Exploit of Security Vulnerabilities • Unauthorised Access • Software Supply Chain Compromises **Temporary system/service disruption**

	Technology • Impacts causes significant delays • Staff or public dissatisfaction/loss of revenue • Identified legislative breaches • Major impact on deliverables.	
Low – Medium	Ministry/Agency area requires a review of processes and systems. ACEO and ICT Team oversight (Minimal-Minor impact) Information • No financial impact or small financial impact • An information security breach resulting in minimal or minor damage to national interest, the department, or officials. • Minor breach to Whole of Government record management requirements. Technology • Impacts result in no insignificant delays, or causes minor delays • Reduced system quality for staff or the public • Nil to minor impact on deliverables.	Low-level malicious attack • E.g., targeted reconnaissance • Phishing • non-sensitive data loss • Spoofing or impersonation Exploitation of Security Vulnerabilities • A single, non-critical component of the application is affected because of a security incursion e.g., Penetration or denial of service attack(s) attempted with minimal to low impact to the organisation Malware • Isolated to widespread instances of a known (non-targeted) computer virus or worm, handled by deployed anti-virus software **Scanning or reconnaissance**

Appendix C - Evidence Collection and Document Preservation SOP

SamCERT records all cyber security incidents in an incident register with restricted access. This ensures that the nature and frequency of these incidents are captured so that corrective action can be taken. This information can subsequently be used as an input into future security risk assessments of systems.

At a minimum, the following data will be recorded in the incident register:

- The date the cyber security incident was discovered
- The date the cyber security incident occurred
- A description of the cyber security incident, including the personnel and locations involved
- The actions taken
- To whom the cyber security incident was reported
- The file reference

Where there is any indication that legal action may be taken concerning the incident, the evidence must be managed such that it is admissible in court.

- Legal advice may need to be sought during the incident response in this regard. It is important to document how all evidence, including compromised systems, has been preserved. All evidence must be collected according to procedures that meet all applicable laws and regulations, developed from previous discussions with legal staff and third-party forensic experts.

The following are some guiding principles regarding electronic evidence:

- Start an investigation by creating a case log, note all dates and times and equipment including serial numbers and model numbers.
- Photograph all relevant equipment.
- Preserve the most volatile data first (RAM contents and non-persistent data)
- Investigation and analysis must only be performed using an exact copy of the evidence, never the source. The original should be securely stored for future reference.
- Computer equipment containing evidence should never be booted as the initialisation process will likely modify the local drive. Attempt to keep the equipment in the same state as received – use hibernate or sleep modes if keeping the equipment powered on is not practical.
- Isolate the device from the network to avoid propagation of any infection.
- Storage devices relevant to the investigation should be installed into another processor that is booted from another drive, to allow copying of the original using appropriate and acceptable forensic tools.
- Specialist software managed by SamCERT or third parties must be used to maintain the reliability of the investigation results and outcomes.
- As the investigation progresses, seek to capture, and document other relevant electronic information (e.g., logs, server backups etc.) of machines targeted in the incident, to allow further independent

verification of incident activity. Again, copies should be made of such data and an investigation performed based on the copies.
- Record all details in the case log.

Evidence must be accounted for at all times; whenever evidence is transferred from person to person, Chain of Custody forms (see Appendix F – Chain of Custody Template

) should be used to detail the transfer and include each party's signature.

A detailed log should be kept for all evidence, including the following:

- Transferal of evidence or equipment as per the use of a "Chain of Custody" form
- Identifying information (e.g., the location, serial number, model number, hostname, and IP address of a computer)
- Name, title, and phone number of everyone who collected or handled the evidence during the investigation
- Time and date (including time zone) and nature of each occurrence of evidence handling
- Locations where the evidence (including controlled copies, e.g., copied data used for analysis) was or is stored
- A brief log of activities and status should be maintained to provide a central point of reference for progress towards resolution. An outline of the details includes:
    - The current incident status
    - A summary of the incident
    - Actions taken by all incident handlers on this incident
    - Contact information for other involved parties (e.g., system owners, digital forensics)
    - A list of evidence gathered during the incident investigation
    - Comments from incident handlers
    - Next steps to be taken (e.g., waiting for a system administrator to patch an application)

Government of Samoa

Appendix D – Evidence Register

Name: Click here to enter text.
Date: Click here to enter text.
Case: Click here to enter text.
Region: Click here to enter text.
Lead Investigator: Click here to enter text.

Use 24-hour time, dates in the format DD/MM/YYYY

Use one Evidence Item table per system

Evidence Item					
System Name	Click here to enter text.		**Date & Time Started**	0000 dd/mm/yyyy	
Description	What function does this system perform?		**System Timezone**	Click here to enter text.	
Acquisition Type	☐ Live-Physical ☐ Live-Remote ☐ Dead ☐ VM ☐ Other:		Click here to enter text.		
Destination Media	Drive ID or destination system & directory path if remote				
Memory	☐ FTK ☐ Lime ☐ TWI ☐ Encase ☐ FastDump ☐ Other		Click here to enter text.		
Memory file name	Click here to enter text.		**Hash**	Click here to enter text.	
Volatile Data	☐ TWI ☐ Flint ☒ Other	Inlcude detailed description of commands/tools used			
Output file/folder	Click here to enter text.				
HDD Imaging Tool	☐DD ☐ FTK Imager ☐ Encase ☐ TWI ☐ EWFAcquire ☐ Other:		Click here to enter text.		
Hard Drives	**ID**	**Size**	**File Name**	**Verified**	**Comments**
	0/sda	GB	<case>-<system>-<ID>.E01	☐	Any issues
	0/sda	GB	<case>-<system>-<ID>.E01	☐	Any issues
	0/sda	GB	<case>-<system>-<ID>.E01	☐	Any issues

Government of Samoa

	0/sda	GB	<case>-<system>-<ID>.E01	☐	Any issues
Database	☐ MySQL ☐ SQL Server ☐ Other		???	**File name**	<case>-<DBName>

Log files	**Type**	**Product**	**Start Date**	**End Date**	**Output File**
			dd/mm/yyyy	dd/mm/yyyy	<case>-<type>
			dd/mm/yyyy	dd/mm/yyyy	<case>-<type>
			dd/mm/yyyy	dd/mm/yyyy	<case>-<type>

Encryption Key/password	Click here to enter text.
Additional Comments	Click here to enter text.
Date & Time Completed	0000 dd/mm/yyyy
NOTES	

Government of Samoa

Appendix E – Remediation Action Plan Template

Date & Time	Category (Contain, eradicate, recover)	Action	Action Owner	Status (Yet to begin, in progress, closed)

Appendix F – Chain of Custody Template

Incident Reference Number				
Item List				
#	**Name / Type** *(e.g., laptop, external hard disk, etc)*	**Serial #, Model #**	**Non-technical Description** *(e.g., The laptop the user performs their daily work on.)*	
Representative				
Name				
Title / Position				
Phone / Mobile				
User or Property Owner				
Name				
Title / Position				
Phone Mobile				
Item(s) transfer Record				
#	**Date & Time** (0000 dd/mm/yyyy)	**Action** (Receive from User, Returned to User)	**<Receiver/Mail> Representative Signature:**	**<Government> Representative Signature:**

Version Management

Version	Date	Comments and Remarks
1.0		