Ministry of Communications & Information Technology

Risk Management Framework

Table of Contents

Introduction

To ensure the Government of Samoa (GoS) and the Ministry of Communication and Information Technology (MCIT) is able to appropriately manage threats and opportunities when they arise and prevent any negative or undesired effects, risk management practices and a risk management framework needs to be in place.

Understanding the risks and recognising any weaknesses within the ICT environment allows us to prepare and mitigate any negative outcomes in the event that the likelihood of a risk is realised. Therefore, having in place a well-defined risk management methodology will ensure and see that when risks arise, they are able to be assessed appropriately and a commensurate risk mitigation strategy (treatment plan) will be implemented and the degree of risk posed is brought to a level that meets or is lower than, the communicated tolerable risk appetite.

1.1 Purpose and Scope of the risk management framework

The purpose of the Risk Management Framework is to define the methodology for the assessment and treatment of information risks in the GoS and identify and communicate the acceptable level of risk an organisation.

This document:

- Defines what risk management is and provides a structured and consistent approach to identifying, rating, mitigating, managing, and monitoring risks;
- Communicates the risk appetite and tolerance levels of the GoS;
- Provides resources to assist staff carrying out risk assessments; and
- Establishes clear roles and responsibilities for identifying and managing risk.

The scope of the Risk Management Framework applies to all ministries, divisions and any other business units operating within the Government of Samoa.

1.3 Risk Management Framework Principles

The following principles provide the overarching requirements to manage risks that are identified at GoS.

Agencies identify their risk profiles and and appetites and apply relevant risk management practices

- Agencies and the GoS establish and identify their risk profiles, and put in place commensurate risk management practice.

Risk management is considered part of all organisational processes

- Risk management is incorporated and taken into consideration in all projects and operational processes across the organisation by all staff. When considering risk, both internal and external factors are taken into account.

Uniformity and Consistency

- Information security risk assessments are conducted following the outlined risk management approach here, and communicated to stakeholders consistently.

Proportionate Response

- The treatment of risks will be prioritised according to exposure and urgency, and will be performed so as to ensure the treatment is proportionate to exposure, considering both likelihood and potential impact.

Risks are documented and reviewed at regular intervals

- When risks are assessed and identified, they are then documented, communicated and owned. Risk is not static and cannot be a 'set and forget' activity. Risks should be documented at each stage of their assessment to allow for reviews and improvements in procedures. The risk assessment process should be reviewed regularly to ensure the ongoing usefulness of the risk management framework and its assessment procedures.

1.4 Roles and Responsibilities

Roles	Responsibilities
Senior Leadership	Senior Leadership will: • Establish and put forward the risk management appetite for the Government of Samoa in alignment with strategic objectives and key drivers; • Identify potential internal and external risk factors and the impact that these may when establishing strategic objectives; • Provide strategic leadership and governance for risk management and promote the implementation of risk management across the GoS. • Ensure roles, responsibilities and accountabilities are designated and assigned from the top and communicated at all levels of government; • Promote a risk aware culture and risk management practices as a core responsibility for all agencies within the government; • Demonstrate ongoing commitment to sustaining risk management resources and practices. This will be done by ensuring the allocation of appropriate, skilled personnel and training is made available, tools, processes and procedures, and continual improvement and review mechanisms are in place; • Monitor and review the established risk appetite to account for changes in the environment and strategic objectives; and • Communication and consultation on the risk management framework and it's processes are made accessible, contextualized and in place in a manner that is able to be carried out across all ministries.
MCIT CEO / ACEO	The MCIT • Promote the implementation of risk management across the GoS and it's agencies; • Help implement and provide oversight over the risk management processes as desired and established by senior leadership. This will involve: o Establish and maintain a culture of risk awareness and management; o Provide governance and oversight in regards to the implementation and assessment of risks and risk mitigation activities; o Advise government agencies on changes or fluctuations in the risk environment that may impact them; • Ensuring all risk management related training opportunities made available to staff are undertaken and reported on; • Communicate risks and risk management activities (including those that are escalated and may require input) that are reported to them to senior leadership for ongoing oversight and transparency;

MCIT	The MCIT will: • Reporting on risk management activities and effectiveness to the MCIT CEO; • Demonstrate a commitment to supporting the GoS agencies needs and aid their implementation of risk management activities and the framework; • Coordinate and promote risk management awareness and training initiatives at the MCIT and across the GoS agencies; • Maintain a repository (e.g. risk register) that is able to be used to effectively document, review and report on identified risks from other ministries and communicate these at regular intervals to senior leadership and relevant stakeholders;
MCIT Policy Division	The MCIT Policy Division will: • Develop, put through the appropriate policy acceptance process and monitor risk management policies and strategies;
Heads of Ministries / Government Agencies	All agencies will: • Determining their agency's risk tolerance and appropriately managing assets commensurate to this determined appetite against relevant threats; • Ensure staff are aware and comply with the relevant policies and procedures, and have the necessary skills to identify risks related to their particular areas of work • Report on the results and attendance of risk management training and awareness activities; • Reviewing their agency's risk management framework implementation; • Evaluate risks on a regular basis, taking into account the relevance of risk, understand the effect it will pose (both positive and negative), monitor the effectiveness of existing controls and treatments, and sign off and report upwards on risks that are identified; • Make risk management resources available to staff; • Ensure risk management considerations are incorporated into all projects; • Undertake risk assessments and document each stage of the risk management and assessment procedure; • Ensure that where risks within their ministry are identified, these are documented and allocated a risk owner to ensure mitigation measures are effectively applied; • Where risks and risk treatments are brought to their attention, appropriately document and communicate upwards to the MCIT and SamCERT;
SamCERT	SamCERT will: • Be responsible for maintaining a risk register of risks escalated to them by the ministries that exceed the risk appetite of the Government, and/or they are unable to track or remediate themselves;

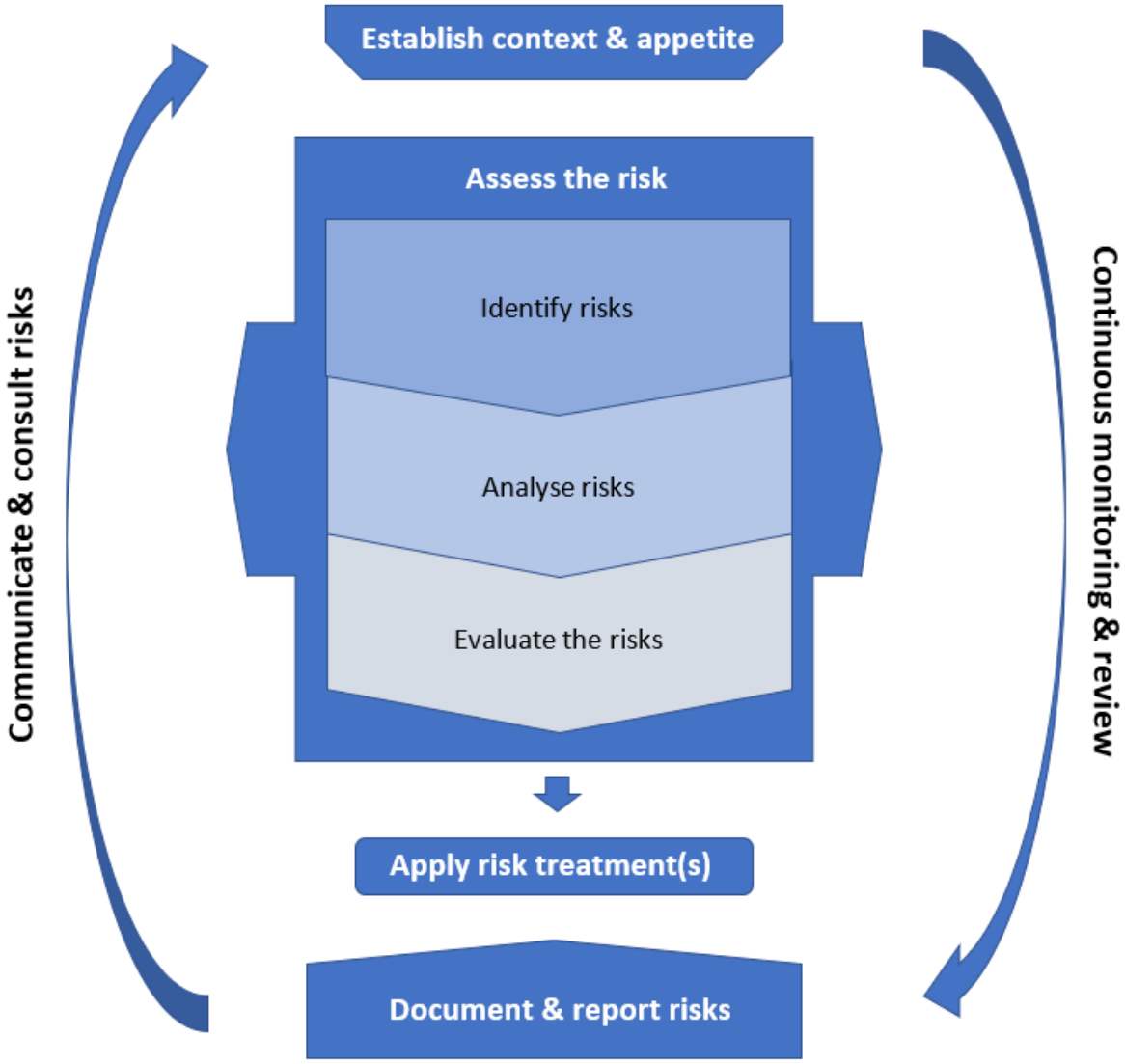
	• SamCERT to collaborate closely with the Ministry of Police Cyber Crime Unit to update and maintain the risk register of risks.
Audit Committee	The audit committee will: • Provide oversight and monitor that the risk management framework is being acknowledged and implemented by the Ministries of the GoS; • Receive and audit risk management reports and documentation as it is provided to them by the MCIT and ministries; • Report on the effectiveness and adherence of the risk management processes to the MCIT and senior leadership in regular risk meetings/forums; • At a regular interval, sample and test risk management controls to ensure that they are suitable, effective and meeting the expected standards established by the GoS and commensurate with their relevant ministry; • Review the risk management framework and monitor it's implementation; • Discuss risk management intervals and encourage the attendance and input from all ministries and relevant stakeholders at the GoS; • Ensure risk management activities and appetite are aligned with and enable the GoS to maintain and comply with any regulatory, legal or other compliance commitments and requirements.
Risk/ System/ information Owners	Risk owners will: • Undertake risk assessments on the information, systems or assets that they have responsibility over; • Follow the risk management process from identification to risk treatment and ongoing monitoring (where required) that aligns with the GoS and agency risk appetite; • Communicate and implement requirements to manage risks at their agency and the Government more broadly; • Assist with timely reporting and escalation of risks to most relevant party;
All Staff	When it comes to Risk Management, all staff will: • Review and be aware of the risk management framework and understand how it applies to them; • Monitor their day to day operational tasks, being aware of how and where there may be opportunities for risk to arise; • Not engage in activities that would place the ministry at an unacceptable level of risk; • Report on any risks if they are identified to their manager and/or the information/system/risk owner; and • Take part in risk management awareness and training opportunities as required.

What is Risk Management?

Risk management is the process of managing threats and opportunities when they arise. By putting in place risk management activities, we are able to prevent consequences to agencies, staff and citizens. It allows for our departments to confidently ensure that they are undertaking activities that will maximise opportunities and benefits and simultaneously minimise negative impacts on organisational objectives.

Therefore, risk management requires people, policies and processes to ensure that a consistent process is in place to ensure that risks are identified, contextualised, analysed and evaluated, treated appropriately and then communicated and reviewed.

The risk management process can be summarised in the following diagram:



Risk Assessment Process

The risk assessment process is comprised of six (6) key phases as outlined in the risk management framework diagram below:

2.1 Establish the Context

Before and during a risk assessment, it is important that the context in which the assessment is going to take place in is understood. This will allow the assessment to be meaningful as it will ensure that any risks identified are relevant and the subsequent assessment and treatment plans are most appropriate to mitigating any risks.

Once the context is established, and in order to establish the context effectively, you will need to consider the organisational (internal) and external context – which sets the scope and considerations for the rest of the assessment.

1. Organisational Context

Establishing the internal context for which risk management will (and is required to) take place in involves cross-functional and multi-stakeholders to provide input. This will require consideration and understanding of the government and/or agency's:

- **Risk appetite and tolerance –** the level of risk it strives to maintain, what it's risk tolerance and risk threshold is.
- **Government or Ministry strategies, objectives and policies -** High level goals and objectives (both current and future), the key drivers and strategies in place to achieve these, and the policies and procedures developed to assist staff in being aware of and delivering appropriately against objectives.
- **Information classification, flows and systems** - The information stored, processed and/or transmitted by systems and assets, how these are transmitted, and what the value of information is (based on aspects such as confidentiality, integrity and availability). This requires an understanding of core and critical systems and information.
- **Contractual, compliance and other legal obligations -** the requirements that the government must abide by to comply with contractual, regulatory or other legal obligations.

- **Key and relevant stakeholders**: Identification of the internal and external stakeholders who may be involved, require consultation, or fall within scope of the risk context. This will also include understanding resourcing requirements, governance structures, roles and accountabilities.
- **Supporting networks and dependencies** – understanding the interdependencies and interconnections of the government or agency and its operations.

2. External Context

The external context is the external environment in which the organisation seeks to achieve its objectives. Some of the aspects considered important to the organisation in establishing external context would include:

- **Citizens** - Citizens are considered to be the most important stakeholders from a risk management perspective because it is them and their data who are directly impacted by the operations of the Government of Samoa.
- **Regulatory** - GoS needs to adhere to several regulatory compliance requirements which have an impact on how it does business, and also on its business risk profile.
- **Legal** - GoS is subject to several regulatory and legal obligations and laws across various jurisdictions.
- **Environment** – in what sort of environment does the agency or government operate in? Understanding the context includes being aware of factors such as natural disasters, competition and strategic influences, and other social, or operational influences.

2.2 Risk Identification

Understanding the context (information assets, processes, environment etc) that influence the operational space of a Government or agency, now enables the identification of relevant risks. This step of the risk assessment seeks to identify events to information systems and data that may prevent, degrade, or delay the achievement on the objectives of the Government or an agency/ministry.

It is essential that all possible risks and risk events to the information environment be identified as risks that are not identified at this stage will not be included in the risk analysis phase. This is best done through a collaborative, multi-stakeholder discussion and/or brainstorm situation.

When identifying risks, it is recommended that stakeholders consider:

- What and where events and risks can occur (what are the potential sources/threats and impacts to an agency/government and its systems or information);
- Why these risks/events might eventuate (what are the strengths and weaknesses that would allow this to occur); and
- How and when this event(s)/risk(s) could occur (e.g. attack vectors, likelihood etc.).

All risk events should be documented (e.g. in a risk register)

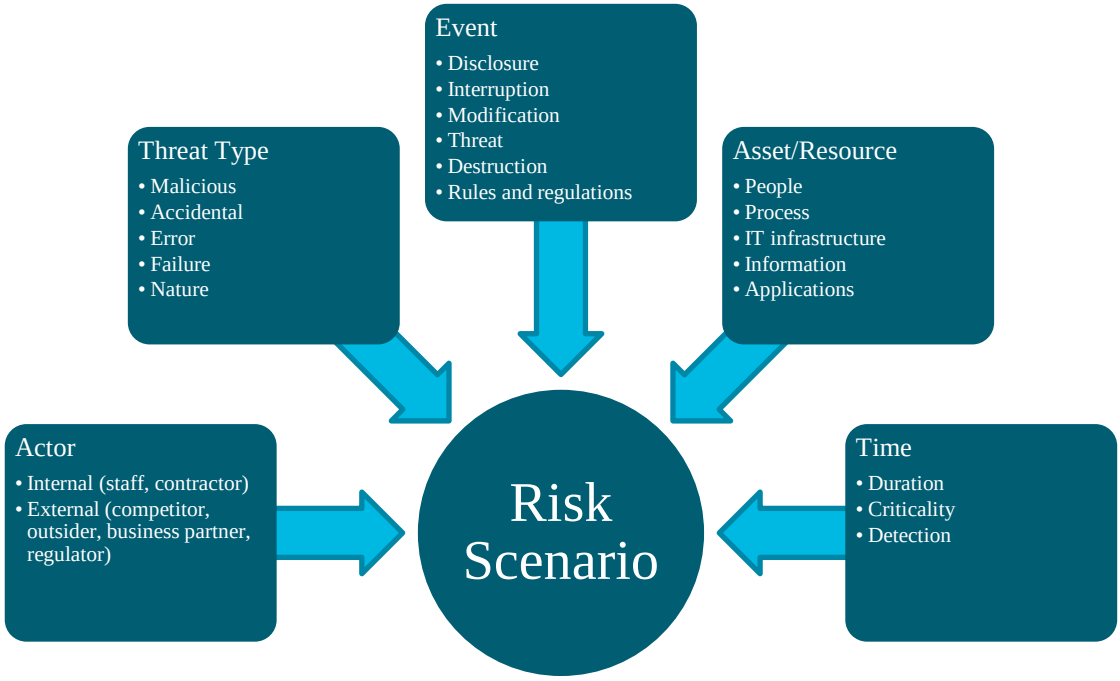
2.3 Risk Analysis

Now that the risks have been identified, risk scenarios should be drafted as part of the analysis phase. Risk scenarios generally consist of a threat exploiting a vulnerability resulting in an undesirable outcome. For example:

> *"A malicious actor executes a successful phishing attack against a system administrator operating within the Government of Samoa, resulting in access to internal systems and data."*

Developing risk scenarios assists determining the potential level of risk that could affect the confidentiality, integrity or availability of the information system and have an adverse effect on the business objectives.

Considerations when developing risk scenarios are identified below:



Doing a risk scenario will allow the organisation to understand the nature of the risk and potential impacts it poses and will assist further down the risk assessment process.

Analysing risks require consideration of the risk(s):

- Existing controls
- Impact
- Likelihood
- Overall level of Risk

The below guidance can assist the appropriate consideration of the analysis phase:

1. Impact Assessment

The inherent risk rating needs to be defined by assessing the impact of the risk eventuating without additional controls being implemented. This will help enable the effectiveness of any new controls that further reduce the impact of a risk event occurring to be assessed.

Only a single impact rating, which is usually the highest rated impact statement based on the various potential impact categories (i.e., privacy, financial, regulatory) can be assigned to the risk although multiple impact statements might be assigned to a risk.

2. Likelihood Assessment

The inherent risk rating needs to be defined by assessing the likelihood of the risk eventuating without additional controls being implemented. This will help enable the effectiveness of any new controls that further reduce the likelihood of a risk event occurring to be assessed.

If an incident has occurred earlier, the frequency of occurrence should be used to help determine the likelihood of the risk eventuating.

3. Risk Rating

The risk rating is evaluated using a risk matrix. Risk Framework (Appendix A) includes a risk matrix that can be used to generate the overall Risk Rating from the assessed inherent likelihood and impact ratings.

Inherent risk is defined as the risk rating without any additional controls being implemented. Risk is dynamic and hence even risks that have a risk rating of rare should be documented, to ensure they can be monitored and re-assessed on a regular basis to ensure that the likelihood and/or impact do not change as the internal and external environment changes around them.

4. Controls Identification and Assessment

Information systems generally have controls in place to reduce the likelihood and/or impact of some of the risks that have been identified. Controls help reduce the risk by reducing the likelihood and/or impact of an event occurring. Assessment of the effect the control has on the overall risk helps in determining the residual risk rating. Controls can be broadly categorised as:

- **Deterrent Controls** - these discourage a potential attacker (e.g., login banner on a network device, Kensington lock, CCTV camera)
- **Preventative Controls** - minimise the likelihood of an incident happening (e.g., restricting server room access to authorised personnel)
- **Detective Controls** – intended to identify when an incident has occurred (e.g., firewall security logs, intrusion detection system alerts)

- **Corrective Controls -** fix information system components after an incident has occurred (e.g., data backups, data replication, business continuity plans)

During the risk assessment, a control may be identified as being ineffective, not sufficient, or simply not relevant to the risk it is supposed to be mitigating. In such cases an analysis is performed to determine whether the control should be replaced with another more suitable control or be supplemented with additional controls.

2.4 Risk Evaluation

The purpose of the risk evaluation phase is to support decisions and assist the government or agency in deciding which risks are to be prioritised for treatment and which may be able to be accepted (in that it does not require a treatment plan to be put in place). This is why once the risk analysis has been completed, the risks are evaluated against the government or agency's defined risk tolerance level (risk appetite) to determine whether additional actions are warranted.

Risks that are assessed as 'Low' on the risk matrix are **generally** considered to present an acceptable level of risk and do not require further evaluation. However, risks being dynamic and constantly fluctuating, should be added to the risk register to be monitored and assessed on a regular basis. Risks evaluated as being 'Moderate' and above would **generally** be evaluated and prioritised.

The risk evaluation outcome should be documented, communicated and validated across multiple levels of the agency or government for agreement. Any decisions or priorities established at this stage should take into account internal and external contexts, impacts and consequences of both actual and perceived risks.

2.5 Risk Treatment

'Risk treatment' is the process whereby the risk is modified by changing the consequences or likelihood of a risk occurring. Risk treatments will generally create new controls or amend controls that already exist.

When treating risks, it is important to consider a range of factors, such as the approach to risk treatment that will be taken, those responsible for treatment, costs and benefits associated with treatment, the likelihood of success, and how risk treatments will be measured.

Risk treatment activities enable the risk to be re-assessed and awarded a 'residual risk' rating, recognising the reduction in risk that has been achieved through the additional controls applied.

The following are the primary approaches that can be selected in order to manage risks:

Avoid	**To avoid risk involves stopping, postponing, or cancelling the activity that would give risk to, and allow, this risk to eventuate.**
Treat	This approach requires putting in place or amending controls to reduce a risk or risks likelihood or consequence to an acceptable level.
Transfer/ Share	Transfer or share the impact of the risk eventuating with a third or external party. This is most often done through insurance or outsourcing risk. It should be noted that transferring or sharing a risk does not always eliminate entirely the responsibility or accountability you may have with regards to that risk.
Accept	Making the informed decision to accept the risk at its current level. This is generally chosen when a risk is assessed as falling within the defined risk tolerance, or if it is impractical to avoid, treat or transfer the risk (e.g. the cost of treatment outweighs the risk impact/consequence posed by the risk itself). While no further actions are taken to treat a risk, ongoing monitoring is still required.

Once a treatment approach (or approaches) is chosen, a risk treatment plan should be developed. Treatment plans be documented in a central repository (such as a risk register) and should incorporate and detail:

- The chosen treatment option;
- The owner and personnel accountable for monitoring and reporting on progress of the treatment plan and its efficacy; and
- Identify a date for which the risk should be resolved and/or reassessed by.

Consideration for a risk treatment plan should be given to how they will be monitored and implemented, and take into account resource and budget availabilities, and communication requirements.

2.6 Monitoring and Review

Reviews of risk is necessary to ensure that any changes to a risk are captured and identified. Regular monitoring of identified risks will ensure that (for example) any changes to risk (both positive or negative) are identified and acted on or new risks are identified and treated, mitigating their potential consequence. This will require risk tools (such as a risk register) to be assessed on a regular basis.

Ongoing monitoring and review ensure that identified action plans are relevant and updated, and the overall risk management process is monitored for improvements and to ensure an effective implementation.

This is also important because risks do not remain static, and while a risk may be at a level which currently sits within the risk appetite – it may not remain here and the current controls in place may not remain adequate.

Monitoring and review is an integral component of the risk management process more broadly. Without this, ensuring the maintenance of an effective and efficient risk management process will not be able to be sustained.

A review of the risk management cycle should be conducted regularly, with the aim of this being to develop and embed risk management as part of the Government's everyday activities, culture and norms.

Continuous improvement and review of the risk management framework at the GoS should include:

- Regular assessment of the risk management process at the government across all agencies to identify opportunities for improvement;
- Collection of the ongoing risk management output data and metrics to gather improvement, communication and training requirements;
- Regular reviews of risk management frameworks and standards used globally to align with best practices being implemented; and
- Ongoing training programs covering all risk management aspects, ensuring that all personnel with risk management activities are equipped with the knowledge and skills base required.

The results obtained from monitoring and reviewing risks will allow the government and its agencies to learn from lessons and experiences, review treatment plans and outcomes, and feed these observations back into the broader process to maximise efficacy. These results and lessons must also be communicated throughout the agency and with relevant stakeholders to ensure the whole government is able to reap the benefits and lessons learned.

Appendix A - Risk Framework
Risk Matrix

A risk matrix is a tool that establishes the risk rating by assessing a given risk's likelihood (on the left column) against its consequence and impact should the risk eventuate (identified along the top of the table).

The purpose of using the risk matrix is to identify the rating of a risk and enable the organisation to prioritise its approach to risk mitigation, focusing on those most urgent to the Samoan Government or Ministry's operations.

	Insignificant	Minor	Moderate	High	Extreme
Almost Certain	H	H	H	E	E
Likely	M	M	H	H	E
Possible	L	M	M	H	H
Unlikely	L	L	M	M	H
Rare	L	L	L	M	M

Likelihood Ratings

Likelihood is the possibility of the risk occurring.

Likelihood	Description	Frequency
Almost certain	Is expected to occur in most circumstances and is almost inevitable	10+ times a year
Likely	Is expected to, and should occur in some circumstances. It would not be a surprise event	Up to 10 times a year
Possible	Might occur in some circumstances.	Once in 1 - 3 years
Unlikely	Could occur at some time, but is not expected to occur	Once every 3 - 5 years
Rare	May occur but only in exception circumstances	Once every 5+ years

Consequence Ratings

This is a scale that can provide guidance to those conducting risk assessments around the consequence and level of impact to the Government or Ministry that may present itself should an identified risk eventuate.

	Consequence				
	Insignificant	**Minor**	**Moderate**	**High**	**Extreme**
Availability	Availability of system may be down for minutes	Availability of systems is lost for a number of hours	Availability of systems is lost for up to a week	Availability of systems is down for months	System availability is lost entirely and cannot be recovered
Resources	No staff, or one or two members are required to assist resolution, and this is able to be done in a few days	Few staff & tools required to assist Little time required to remediate. Likely to take weeks to recover impacts.	Some key personnel involved in mitigating risk, may take months to recover	Groups of Government stakeholders will be pulled from operations. Up to a year to recover	Loss of executives, CEO and years to recover.
Cost	Result in loss of >1% of the impacted Ministry(s) budget	Result in loss of >2% of the impacted Ministry(s) budget	Result in loss of >3% of the impacted Ministry(s) budget	Result in loss of >4% of the impacted Ministry(s) budget	Result in loss of >5% of the impacted Ministry(s) budget
Compromise of Information	No important information is compromised	Important information is compromised, but can be managed	Some Sensitive, personal, private or other key information is compromised	Significant sensitive, personal, private or other key information is compromised	Top secret government information, proprietary secrets & citizen or member PII is disclosed and unable to be recovered
Reputation	Reputation is not impacted or can be repaired without too much effort	Reputation of Government is impacted slightly	Reputation of Government is impacted with civilians and other nations	Reputation is impacted significantly and takes significant effort to repair	Reputational impacts are irrecoverable and cannot be repaired

Risk Acceptance Criteria

The below criteria represent the relevant stakeholders who must be consulted prior to a risk treatment being implemented when the risk is identified as a given rating (e.g. High).

Risk Acceptance	Criteria
Extreme	Immediate treatment is required, and this must be approved by CEO
High	ACEO OR CEO approval for treatment is required and treatment actions MUST be planned for implementation soon.
Medium	Principal OR ACEO should be informed of this risk and approve the risk treatment controls
Low	Able to be managed by routine procedures, no additional controls required nor approval for this

Appendix B – Supporting documentation (example)

Risk Register

Risk registers are living, breathing documents that are constantly reviewed and updated. The below is an example of what a risk register within the Government of Samoa that may be maintained by a Ministry or entity should capture at a minimum.

Risk ID	Risk Scenario	Asset affected	Asset Owner	Inherent risk			Current controls	Residual Risk			Risk Treatment Approach	Proposed Controls	Risk Owner	Treatment Due
				Likelihood	Consequence	Risk Rating		Likelihood	Consequence	Risk Rating				
01														
02														
03														

Appendix C – Glossary

Term	Definition
Acceptable risk	The level of potential losses that a society or community considers acceptable given existing social, economic, political, cultural, technical and environmental conditions
Asset	An asset is a component or part of a total system to which is of value to the company and hence requires protection based on its value.
Asset owners	The asset owners are personnel responsible for ensuring assets are suitably secure whilst being developed, produced, maintained, and used.
Incident	Any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service
Inherent Risk	The probability of loss arising out of circumstances or existing in an environment, in the absence of any action to control or modify the circumstances
Residual Risk	Exposure to loss remaining after other known risks have been countered, factored in, or eliminated
Risk	A situation involving exposure to a potential danger.
Security Risk Assessment	The Term “security risk assessment” refers to the methodology or process used to find security risks. Security risks are risks that impact the Confidentiality, Availability, and Integrity of the business as a whole.
Stakeholders	The stakeholders are personnel that can affect - or be affected by – an asset including a perception that they themselves will be affected by it
System owners	The person(s) responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system
Threat	A possible danger that might exploit a vulnerability to breach security
Vulnerability	The term "vulnerability" refers to the security flaws in a system that allow an attack to be successful

Version Management

Version	Date	Comments and Remarks
1.0		