NDMA

NATIONAL DATA
MANAGEMENT AUTHORITY

Information Security Risk Management Standard

Prepared By:

National Data Management Authority
March 2023

Document Status Sheet

	Signature	Date
Policy Coordinator (Cybersecurity)	**Muriana McPherson**	**31-03-2023**
General Manager (NDMA)	**Christopher Deen**	**31-03-2023**

Document History and Version Control

Date	Version	Description	Authorised By	Approved By
31-03-2023	**1.0**		**General Manager, NDMA**	**National ICT Advisor**

Summary

1. These Standard addresses information security risk management.
2. It was adapted from NIST Cybersecurity Framework Policy Template Guide.
3. This is a living document which will be updated annually or as required.
4. Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

1.0 Purpose

Risk management is a critical component of any information security programme. It helps ensure that any risk to confidentiality, integrity, and availability is identified, analysed, and maintained at acceptable levels. Risk assessments allow management to prioritise and focus on areas that pose the greatest impact to critical and sensitive information assets. This provides the foundation for informed decision-making regarding information security.

Routine assessments are required to identify risk and ensure appropriate controls. Risk assessments allow alignment of information security with business objectives and regulatory requirements. Identifying information security risk and considering control requirements from the onset is essential, and far less costly than retrofitting or addressing the impact of a security incident.

This standard provides a risk management framework to evaluate current security posture, identify gaps, and determine appropriate actions.

2.0 Authority

The Permanent Secretary, Administrative Head, Head of Human Resources or their designated representative of the Public Sector Organisation is responsible for the implementation of this standard. For further information regarding the foregoing, please contact the Policy Coordinator - National Data Management Authority (NDMA).

3.0 Scope

This standard encompasses all systems, automated and manual, for which the Government of Guyana has administrative responsibility, including systems managed or hosted by third parties on behalf of the Government. It addresses all information, regardless of the form or format, which is created or used in support of business activities. It is the user’s responsibility to read and understand this standard and to conduct their activities in accordance with its terms.

4.0 Standard

Information security risk management considers vulnerabilities, threat sources, and security controls that are planned or in place. These inputs are used to determine the resulting level of risk posed to information, systems, processes, and individuals that support business functions.

While risk management and related assessment activities can take many forms (e.g., formal risk assessment, audits, security reviews, configuration analysis, vulnerability scanning and testing), all are aimed at the same goal - identifying and acting on risk to improve overall security posture.

It should be noted that an organisation can never completely eliminate risk but can take steps to manage risk.

As per the Information Security Policy, any system or process that supports business functions must be appropriately managed for risk and undergo risk assessments as part of its life cycle.

4.1 Risk Management Process

The risk management process is iterative and should be followed throughout a system's or process's life cycle.

4.1.1 Frame Risk

The first step in managing risks is to:

4.1.1.1.develop a strategy for conducting your risk assessment which considers assumptions, constraints, priorities, dependencies, tradeoffs, and resources that will be used.

4.1.1.2.determine the risk tolerance, or the level of risk that is acceptable. For information security risk decisions that may affect multiple organisations, the lowest level of risk tolerance for those organistions must prevail. It is important that organisations recognize how fundamental this decision is to the risk management process. Risk tolerance is an executive-level decision and information technology (IT) staff should not be determining the risk tolerance for an organisation.

4.1.2 Assess Risk

Assessing risk starts with identifying and classifying assets within scope. Risk is assessed by determining the threats and vulnerabilities to these assets, identifying the potential impact of each vulnerability being exploited, and determining the likelihood of occurrence. A list of potential threats and vulnerabilities needs to be developed and may come from preexisting resources.

It is important to note that the risk assessment process is comprehensive by intention, to assure due diligence, compliance, and proper documentation of security related controls and considerations. Designing security into systems requires an investment of time and resources. The extent of the risk assessment should be commensurate with the classification (information sensitivity and system criticality) of the system/process and the risks this system/process introduces into the overall environment.

Types of Information security risk assessments include, but are not limited to:

4.1.2.1.Enterprise Risk Assessments – Assesses risks to core agency assets, operational processes, and functions.

4.1.2.2.Physical Infrastructure Assets and Systems Risk Assessments – Identifies and assesses vulnerabilities and risks to core physical infrastructure assets and systems.

4.1.2.3.Project Security Risk Assessments (New Risks) – Identifies and assesses new risks to existing components introduced by new technology or service offerings.

4.1.2.4.Change Request Risk Assessments – Assesses risk of change to ensure security is not compromised by the proposed change.

4.1.3 Respond to Risk

Once the risk has been assessed, the organisation must determine and implement the appropriate course of action. Options include:

4.1.3.1. Risk Acceptance – This is a documented decision not to act on a given risk at a given time and place. It is not negligence or "inaction" and can be appropriate if the risk falls within the risk tolerance level. For example, organisations may choose to accept the risk of an earthquake, based on a low likelihood of extensive damage and the high cost of controls.

4.1.3.2. Risk Avoidance – These are specific actions taken to eliminate the activities or technologies that are the basis for the risk. This is appropriate when the identified risk exceeds the risk tolerance, even after controls have been applied (i.e., residual risk). For example, if a connection between two networks includes unacceptable risks and the countermeasures are not practical, the organisation may decide not to make the connection.

4.1.3.3. Risk Mitigation/Reduction – These are specific actions taken to eliminate or reduce risk to an acceptable level. This is the most common approach and is appropriate where controls can reduce the identified risk. For example, to reduce the risk of network intrusion, an organisation may choose to deploy a firewall.

4.1.3.4. Risk Transfer/Sharing – These are specific actions taken to shift responsibility for the risk, in whole or in part, to a third party. This may be appropriate when it is more cost effective to transfer the risk, or when a third party is better suited to manage the risk. For example, an organisation may transfer risk through legal disclaimers or by outsourcing to a vendor.

4.1.4 Monitor Risk

The organisation must monitor the effectiveness of its risk response measures, by verifying that the controls put in place are implemented correctly and operating as intended. This must occur annually, at a minimum. In addition, the organisation must have a process to alert it of significant changes in the factors it uses to assess its risk (e.g., assets, threats, controls, regulations, policies, risk tolerance). These changes may indicate a new assessment is needed.

5.0 Compliance

This standard shall take effect upon publication. Compliance is expected with all organisational policies and standards. Failure to comply with the standard may, at the full discretion of the Permanent Secretary, Administrative Head, or Head of Human Resources of the Public Sector Organisation, may result in the suspension of any or all privileges and further action may be taken by the Ministry of Public Service.

6.0 Exceptions

Requests for exceptions to this standard shall be reviewed by the Permanent Secretary, Administrative Head, Head of Human Resources of the Public Sector Organisation, or the Policy Coordinator, NDMA. Departments requesting exceptions shall provide written requests to the relevant personnel. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a timeframe for achieving the minimum compliance level with the policies set forth herein.

7.0 Maintenance

The Policy Coordinator, NDMA shall be responsible for the maintenance of this standard.

8.0 Definitions of Key Terms

Term	Definition
Information Security Risk[1]	The risk to organisational operations (including mission, functions, image, reputation), organisational assets, individuals, other organizations, and the Nation due to the potential for unauthorised access, use, disclosure, disruption, modification, or destruction of information and/or information systems.
Risk[2]	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Risk Assessment[3]	The process of identifying risks to organisational operations (including mission, functions, image, reputation), organisational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.
Security Control[4]	A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.
Threat[5]	Any circumstance or event with the potential to adversely impact organisational operations (including mission, functions, image, or

[1] *Retrieved from:* NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/information_security_risk

[2] *Retrieved from:* NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/risk

[3] *Retrieved from:* NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/risk_assessment

[4] *Retrieved from:* NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/security_control

[5] *Retrieved from:* NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/threat

	reputation), organisational assets, or individuals through an information system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.
User[6]	Individual or (system) process authorised to access an information system.
Vulnerability[7]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

9.0 Contact Information

Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

[6] *Retrieved from:* NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/user

[7] *Retrieved from:* NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/vulnerability