REPUBLIC
OF GHANA

CYBER SECURITY AUTHORITY
CSA

RISK ASSESSMENT FRAMEWORK FOR THE PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE

A Secure and Resilient Digital Ghana

Published by the Cyber Security Authority (CSA)

Risk Assessment Framework for the Protection of Critical Information Infrastructure (CII)

Table of Content

Foreword

Ghana's digital landscape is undergoing a dynamic transformation, driven by the Ministry of Communications, Digital Technology and Innovations, through the advancements in technology and the increasing reliance on online services. The emergence of digital technology not only drives economic growth and social inclusion but also presents the element of cyber risks.

The global cybersecurity landscape has in recent times witnessed a surge in cyberattacks, with Ghana experiencing a significant increase in cyber threats. In an era of sophisticated cyberattacks, countries are moving towards establishing, implementing, and adopting cybersecurity frameworks and standards to ensure the protection of their Critical Information Infrastructure (CII), which are information assets vital to the nation's security, economic and social well-being of citizens.

The Ministry of Communication, Digital Technology and Innovations acknowledges this growing concern and has undertaken various initiatives to bolster Ghana's digital resilience. These include, the passage of the Cybersecurity Act, 2020 (Act 1038), establishment of the Cyber Security Authority (CSA), and the launch of the Directive for the Protection of Critical Information Infrastructure (CII).

The increasing sophistication and frequency of cyberattacks necessitate a proactive approach to risk management. The Risk Assessment Framework (RAF) is a pivotal step towards achieving a secure and resilient digital ecosystem. By equipping stakeholders with a structured approach to identify and evaluate risk, the RAF will empower CII Owners to safeguard their critical information assets and information, building a secure and resilient digital Ghana.
As a policy direction and in accordance with Act 1038, the Cyber Security Authority (CSA) shall publish relevant guidelines for the continuous identification, registration, and management of cybersecurity risks posed to Ghana's CIIs. A cyber-resilient CII ecosystem is an enabler for digital innovations, trust, and confidence building in the use of digital services, with a huge potential to contribute to the growth of our GDP by improving revenue generation and economic development.

The successful adoption of the RAF requires continuous and collaborative actions and heightened cybersecurity awareness between the CSA and CII Owners.

Mr. Samuel Nartey George (MP)
Minister for Communication, Digital Technology and Innovations
Republic of Ghana

Preface

In an increasingly interconnected world, Ghana, faces a growing challenge from cyber threats. The digital landscape not only offer significant opportunities for progress and development but also presents risks that malicious actors can exploit.

Managing risk effectively is essential for achieving the objectives of the CIIs, ensuring compliance with legislation, regulations, directives.

According to the World Economic Forum's Global Risks Report 2024, cyber-related risks are ranked 5th most significant global risk, accounting for 39% of the current risk landscape due to rapid digitisation. In recent years, Ghana has experienced a significant increase in cybersecurity incidents impacting critical sectors, including Banking and Finance, Government, and Energy. This alarming trend poses severe threats to Ghana's national security, social, and economic well-being of citizens. To address these challenges, this Risk Assessment Framework (RAF) has been developed to provide a consistent and structured approach for identifying, and analyzing cyber risks to CII. It will serve as a guide to implement robust cybersecurity measures promptly to protect our critical information infrastructure and ensure a secure digital ecosystem.

This Risk Assessment Framework (RAF) provides a flexible structure that can be tailored and adopted by CII Owners in their unique risk landscape, while ensuring compliance with relevant standards, regulations and best practices. The RAF equips CII Owners to navigate the uncertainties of the future and make informed decisions amidst potential challenges.

The CSA is committed to supporting Critical Information Infrastructure (CII) Owners in safeguarding their systems. The adoption of the Risk Assessment Framework (RAF) is essential for addressing current and emerging threats. This framework offers practical guidance on risk assessment, helping CII Owners identify vulnerabilities, implement effective countermeasures, and enhance overall security. We strongly urge all CII Owners to incorporate the RAF into their operations, as doing so is crucial for ensuring a secure and resilient digital ecosystem for Ghana.

Divine Selase Agbeti
Ag. Director-General
Cyber Security Authority (CSA)

1 Background

Technology is the main driver of industrialisation and the daily livelihoods of Ghanaians. Aspects of Ghanaian's daily lives, from communication to healthcare and transportation are supported by Information Technology (IT). Organisations rely heavily on IT systems to deliver products and services to customers. Services such as energy distribution, communications and healthcare are essential for Ghana to function efficiently. These services are also increasingly supported by Operational Technology (OT) which deliver automation, remote control and monitoring and control of physical systems.

Ghana has designated 13 sectors of the country as Critical Information Infrastructure (CII) Sectors, namely, National Security and Intelligence, Information and Communication Technology (ICT), Banking and Finance, Energy, Health, Transport, Government, Emergency Services, Water, Food and Agriculture, Manufacturing, Mining and Education. The critical systems of these sectors are constantly being targeted by attackers which poses risks to Ghana's national security or the economic and social well-being of citizens.

Risk is a measure of the degree to which an entity is threatened by a potential situation or event. This is determined by the resulting impact of the event and the possibility of the event occuring. Risks to organisations have multiple sources such as, but not limited to organisational processes, supply chain, competitors, nation states and insiders . To ensure the continuous delivery of services to Ghanaians, the risks need to be managed. Risk Management is the process of identifying, analysing, prioiritising, managing/mitigating, monitoring and reducing risks to information systems. The Risk Managament Process comprises establishing the risk context, assessing the risk, responding or treating the risk and the continuous monitoring of the risk.

Risk Assessment forms an integral part of the Risk Management Process. The Risk Assessment processes identifies, analyses and evaluates the risk to CII. The process is a critical component of any comprehensive strategy for safeguarding critical systems, improving the well-being of citizens, and promoting sustainable development. Understanding, assessing and managing risk is crucial for building resilience in an increasingly complex and interdependent world. This Risk Assessment Framework (RAF) describes the underlying principles, objectives, and key elements for conducting risk assessments.

2 About the CSA

The Cyber Security Authority (CSA) is a national agency under the Ministry of Communication, Digital Technology and Innovations (MOCDTI), established by the Cybersecurity Act, 2020 (Act 1038), to regulate cybersecurity activities in the country; to promote the development of cybersecurity in the country, and provide for related matters. The CSA is responsible for Awareness Creation & Capacity Building, Cybersecurity Incident Coordination & Response, Critical Information Infrastructure Protection (CIIP), Child Online Protection (COP) and International Cooperation, among others. The CSA is responsible for the development and implementation of Ghana's National Cybersecurity Policy & Strategy.

3 Objective

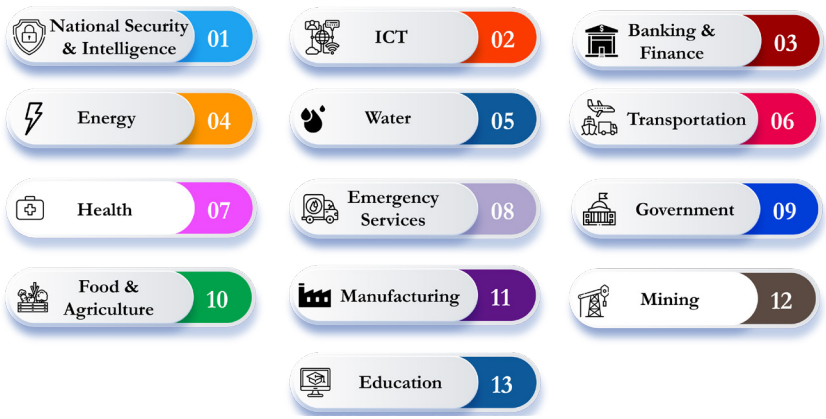
The objective of this Framework is to:

a. provide a structure for conducting risk assessments of Critical Information Infrastructure (CII) as required in Section 5.2 (j) of the Directive for the Protection of CII.

b. provide the structure and key information required for the Risk Assessment Report that shall be submitted to the Cyber Security Authority, quarterly, per Section 5.2 (j) of the Directive for the Protection of CII.

4 Applicability

This Framework shall apply to all designated Critical Information Infrastructure (CII).

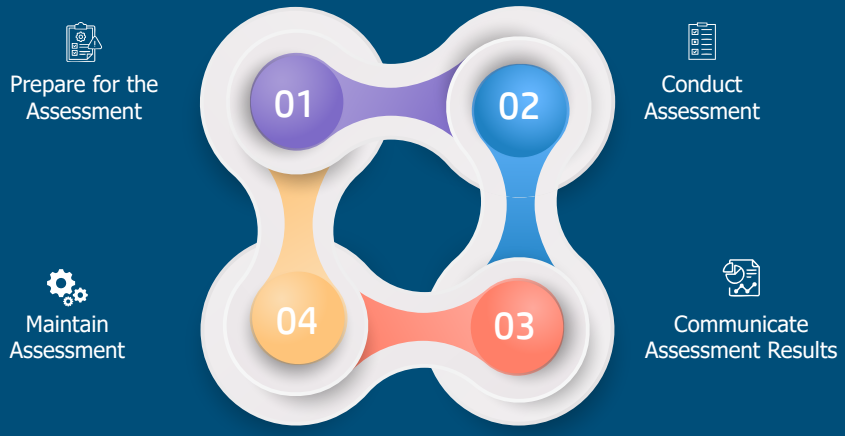


5 Risk Assessment

To conduct a thorough Risk Assessment for critical systems, a methodology needs to be adopted. The methodology for risk assessment encompasses the risk assessment process, the risk model adopted, the assessment approach and the analysis approach. The methodology is defined based on the risk management strategy adopted by the organisation.

This Risk Assessment Process aims to provide a guide for CII Owners to:

a. Prepare for a risk assessment.
b. Conduct a risk assessment.
c. Communicate the risk assessment results.
d. Monitor and review.



5.1 Prepare for Risk Assessment

The Preparation Process of the Risk Assessment establishes the context for the risk assessment and includes the following procedures:

- A thorough Understanding of the Organisation
- Identifying the organisations IT processes
- Identifying the organisational information assets
- Identifying the purpose of the risk assessment
- Identifying the scope of the risk assessment
- Identifying the assumptions and constraints associated with the risk assessment.
- Identifying the sources of information to be used as inputs to the risk assessment.
- Identifying the risk model, assessment and analytic approaches to be employed.

5.1.1 Understanding the Organisation

A comprehensive cybersecurity risk assessment requires first establishing organizational context and meticulously scoping the technology environment. This foundational step involves differentiating between Information Technology (IT), Application Technology, and Operational Technology (OT) systems, as each domain possesses unique threat landscapes, risk tolerances, and security requirements.

5.1.2 IT Processes

Inherent risk emerges from the business processes and activities essential to achieving strategic objectives. A foundational step in cybersecurity risk assessment is to identify and document all IT-supported processes. This mapping enables a systematic analysis to identify inherent risks within each process and to prescribe the appropriate mitigating security controls.

5.1.3 Information Asset Identification

To effectively evaluate the risk to an organisation, an up-to-date information asset inventory is required. The inventory identifies and categorises the information asset based on its criticality to business processes and should include, but not limited to dependencies on external service providers and outsourcing arrangements

5.1.4 Purpose of the Risk Assessment

Identify the purpose of the risk assessment; the information the risk assessment is intended to produce and the decisions the risk assessment is intended to support. The purpose of the risk assessment should be stated in requisite detail to ensure that the assessment produces the appropriate information.

5.1.5 Scope of the Risk Assessment

The scope determines what will be considered in the assessment and is determined by the organisation's risk management strategy and the request for the assessment.

5.1.6 Assumptions and Constraints

Identify the specific assumptions and constraints under which the risk assessment is performed. Document the assumptions and limitations.

5.1.7 Information Sources

Identify the relevant sources of information on threats, vulnerabilities, and impact to be used in the risk assessment to ensure the production of applicable results.

5.1.8 Risk Model, Assessment and Analytic Approach

Identify and document the risk models to be used for the assessment - The risk model defines the risk factors (threat, vulnerability, impact, likelihood) to be assessed and the linkages among the factors.

Identify the approach for the risk assessment - The approaches are quantitative, qualitative, or semi-quantitative.

- Quantitative assessments involve the use of a set of methods, principles, or rules to assess risk, typically using numerical data. Cost-benefit analysis of alternative risk responses or action plans is more effectively supported by quantitative assessments.
- Qualitative assessments typically employ a set of methods, principles, or rules for assessing risk based on non-numerical categories or levels, including very high, high, moderate, low, or very low. Decision makers can be informed about risk outcomes through this assessment.
- Semi-quantitative assessments are often conducted using a set of principles, methods and rules that assess risk using categories or representative numbers. The benefits of both quantitative and qualitative assessment can be achieved through this type of assessment.

Analytic approaches also need to be identified-The analytic approaches are threat-oriented, impact-oriented, or vulnerability-oriented.

5.2 Conduct Risk Assessment

The Risk Assessment process produces a list of information security risks that can be prioritised by risk level to inform risk response decisions. To achieve this goal, organizations analyse threats, vulnerabilities, impacts, and likelihood.

Conducting a risk assessment involve the following procedures:

- Identifying relevant threat sources and events.
- Identifying vulnerabilities.
- Determining the likelihood/probability of specific threat events being triggered by the identified sources and the likelihood of successful threat event.
- Determining the extent of impact of the vulnerability exploitation by threat sources on CII.
- Determining the information security risks as a product of the likelihood of exploitation of vulnerabilities and the impact of such exploitation.
- Identifying the risk ownership, and assigning a responsible individual

5.2.1 Identify Threat Sources and Events

The threat events are characterised by the threat sources that could initiate the events or attacks.

5.2.2 Identify Vulnerabilities

Identify and map vulnerabilities of critical systems to threat sources that have been identified and threat events that can be initiated.

5.2.3 Determine Likelihood

Determine the likelihood that:

- threat events can result in adverse impacts with the considerations that threat events will occur,
- threat events when occurred will have a devastating impact on critical information assets or
- the possibility of the threat event occurring that would have a devastating impact.

With the determination of Likelihood of a threat event, a scale is employed in the evaluation. Depending on the organisation's risk management strategy, a Likert (Very Unlikely to Very Likely) scale can be used in the evaluation of the likelihood.

5.2.4 Determine Impact

Considerations for evaluating impact are the characteristics of the threat sources that could initiate the events that the vulnerabilities identified; and the susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.
Negative impact can be evaluated in terms of the potential effect on confidentiality, integrity and availability to a critical information asset. A Likert (Negligible to Severe) scale can be used in the evaluation of the impact.

5.2.5 Determine Risk Ownership

Clearly identify the institutional role responsible for risk ownership. The designated role must be accountable for monitoring the risk, ensuring that control measures are effectively implemented, reporting on the risk status, and reassessing the risk as conditions change

5.3 Communicate and share Risk Assessment Information

Communicating the results of the risk assessment is key to ensuring that decision makers have the right information to guide risk-based commitments. Communicating and sharing information consists of the following specific tasks:

- Communicate the results of the risk assessment.
- Share related risk to support other risk management activities.

5.3.1 Communicate Risk Assessment Results

Requirement for, and defined channels of communication of risk assessment results to decision makers are to be established and agreed by the organisation. Forms of communication include risk assessment reports (a structure of risk assessment report provided in Appendix A), executive briefings, dashboards among others. The risk results are illustrated in a risk register (Appendix B) and a risk matrix as shown in Figure 2 below. The matrix visualises the likelihood of a risk and the impact of the risk and prioritises risk decisions based on the rating on the matrix.

Impact

Likelihood	Neglibible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

Figure 2 Risk Matrix

5.3.2 Share Risk-Related Information

Share the risk information that is generated during the assessment with appropriate personnel within the organisation. Information sharing is done through reports and briefings as well as documented sources of information.

5.4 Risk Monitoring and Review

Risk reviews and monitoring should take place at all stages of the risk assessment process, and its outcomes should be a planned part of the enterprise risk management process, with defined responsibilities.

Risk monitoring and review includes planning, gathering, and analysing information, recording results, and providing feedback. The results of risk monitoring and review should be integrated into all the organisation's performance management, measurement, and reporting activities.

6 Application of Risk Assessments

Risk assessments can be conducted at the organisational level, business process level, and information systems level.

6.1 Risk Assessments at the Organisational Level

At the organisational level, risk assessments support the organisation's risk management strategies, policies, direction, and processes. Risk assessments performed at the organisational level focus on organisational operations, information assets, and people (human capital), with a comprehensive assessment across business tasks. Organisation-wide risk assessments can be based solely on assumptions, constraints, risk tolerances, priorities, and trade-offs. For decentralized organisations or organisations with different business missions/functions and/or operating environments, expert analysis may be required to standardise risk assessment results across task/business process level.

Risk assessment at the organisational level can focus on:

a. The specific types of threats targeting organisations that may differ from other organisations and how those threats affect policy decisions.
b. Systemic weaknesses or deficiencies discovered in organisational information systems that could be exploited by adversaries.
c. The potential negative impact on organisations due to loss or compromise of organisational information, whether intentional or unintentional.
d. The use of new information technologies such as artificial intelligence, quantum, mobile and cloud computing and the potential impact on the ability of organisations to carry out their missions/business when using these technologies.

Results of organizational-level risk assessments are communicated to organisational units at the mission/business and information systems (technology) levels.

6.2 Risk Assessment at the Mission/Business Process Level

At the mission/business process level, risk assessments support the determination of its protection and resiliency requirements.

Mission/business process level risk informs and guides decisions on how, and when to use information systems for specific mission/business processes or for alternative mission/business processing in the face of compromised information systems.

The risk assessments focus on mission/business segments, which typically include multiple information systems, with varying degrees of criticality and/or sensitivity about core organisational missions/business functions. Risk assessments at the mission/business process level can also focus on information security architecture as a critical component of enterprise architecture. Risk assessment results produced at the mission/business process level are communicated to and shared with organisational entities at the information system level to help inform and guide the implementation of security controls to the information systems and environments in which these systems operate.

6.3 Risk Assessment at the Information System (Technology) Level

The mission/business process level context and the system development life cycle of the information system determine the purpose and define the scope of risk assessment activities at the information system (technology) level.

Risk assessments examine anticipated weaknesses that could compromise the confidentiality, integrity, and availability of critical systems in the context of the expected operating environments. The assessments inform risk response, enabling information system owners/programmes managers, to make the decisions about the necessary security controls based on the security appetite, categorization and the environment of operation.

Risk assessments are also conducted at later phases in the system development life cycle, updating risk assessment results from earlier phases. The risk assessment results include an assessment of the overall risk to the organisation and the information contained in the critical systems by operating the systems as evaluated. Risk assessment results at the information system (technology) level are communicated to organisational entities at the organisational and mission/business process levels.

7 Definitions

- **Risk** is a measure of the extent to which an entity is threatened by a potential circumstance or event and is typically a function of:
  a. The adverse impacts that would arise if the circumstance or event occurred.
  b. Likelihood of occurrence (probability).
- **Information security risks** are risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts on an organisation's operation, information assets, stakeholders, employees, and the nation.
- **Risk assessment** is the process of identifying, estimating, and prioritising information security risks. Assessing risk requires the careful analysis of threat and vulnerability information to determine the extent to which circumstances or events could adversely impact an organisation and the likelihood that such circumstances or events will occur.
- **Risk assessment methodology** typically includes:
  a. A risk assessment process.
  b. An explicit risk model, defining key terms and assessable risk factors and the relationships among the factors.
  c. An assessment approach (Quantitative, Qualitative, or Semi-qualitative) specifies the range of values the risk factors can assume during the assessment and how to combinations of risk factors are identified/analysed so that the values of those factors can be functionally combined to evaluate risk.
  d. An analysis approach (threat-oriented, information asset/impact-oriented, or vulnerability-oriented) describes how combinations of risk factors are identified/analysed to ensure adequate coverage of the problem space at a consistent level of detail.
- **Threat** is any circumstance or event with the potential to adversely impact organisational operations and information assets, individuals, stakeholders, or the nation through an information system via unauthorised access, destruction, disclosure, modification of information, or denial of service.
- **Threat events** are caused by threat sources, characterised as the intent and method targeted at the exploitation of a vulnerability, or a situation and method that may accidentally exploit a vulnerability. When threat events are identified with great specificity, threat scenarios can be modelled, developed, and analysed.
- Organisations can specify threat events as single events, actors or circumstances, or sets /sequences of related actions, activities, or circumstances. Risks materialise because of a series of threat events, each of which takes advantage of one or more vulnerabilities.
- **A threat source** is the intent and method targeted at the exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability.

- **Risk models** refer to the risk factors to be assessed and the relationships among those factors. Risk models differ in the degree of detail and complexity with which threat events are identified.
- **Risk factors** are characteristics used in risk models as inputs to determine levels of risk in risk assessments. It is used extensively in risk communications to highlight what strongly affects the levels of risk in particular situations, circumstances, or contexts. Risk factors include threat, vulnerability, impact, likelihood, and predisposing condition. It is important for organisations to predefine definitions prior to conducting risk assessments because the assessments rely upon well-defined attributes of threats, vulnerabilities, impact, and other risk factors to effectively determine risk.
- **A vulnerability** is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. Some vulnerabilities emerge over time as organisational missions or business functions evolve, new technologies proliferate, environments of operation change, and new threats emerge. The tendency for security controls to potentially degrade in effectiveness over time reinforces the need to maintain risk assessments during the entire system development life cycle and the importance of continuous monitoring programmes to obtain ongoing situational awareness of the organisational security posture. Vulnerabilities can be found in organisational governance structures, including the lack of effective risk management strategies, poor intra-agency communication, inconsistent decisions, or misalignment of enterprise architecture to support mission/business activities. Vulnerabilities can also be found in external relationships (supply chains, information technologies, and telecommunications providers), mission/business processes, and enterprise/information security architectures. The severity of a vulnerability is an assessment of the relative importance of mitigating/remediating the vulnerability. The severity can be determined by the extent of the potential adverse impact if such a vulnerability is exploited by a threat source. Thus, the severity of vulnerabilities, in general, is context dependent.
- **The likelihood** of occurrence is a weighted risk factor based on an analysis of the probability that a given threat can exploit a given vulnerability/set of vulnerabilities. Organisations typically employ a three-step process to determine the overall likelihood of threat events.
    a. The organisation assesses the likelihood that threat events will be initiated or occur.
    b. The organisation assesses the likelihood that the threat events, once initiated or occurring, will result in adverse impacts or harm to organisational operations and information assets, individuals, other organisations, or the nation.
    c. The organisation assesses the overall likelihood as a combination of likelihood of the initiation/occurrence and likelihood of resulting in adverse impact.

- **The level of impact** from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. The organisation should establish the process used to conduct impact determinations, assumptions related to impact determinations, sources, and methods for obtaining impact information, and the rationale for conclusions reached regarding impact determinations. Organisations may explicitly define how established priorities and values guide the identification of high-value information assets and the potential adverse impacts on organisational stakeholders.
- **Organisational information assets** represent any resource or set of resources that the organisation values, including intangible information assets such as image or reputation.

8 Reference

- Centre for Internet Security (CIS) Risk Assessment Method (RAM)
- ISO 31000 Risk Management – Guidelines
- National Institute of Standards and Technology (NIST) – Guide for Conducting Risk Assessments.

Appendix A – Risk Assessment Report

This appendix provides a structure and key information required for the development and communication of the results of a risk assessment.

Cover Page

Cybersecurity Risk Assessment Report
Prepared For : [CII Owner Name]
Date:
Prepared By: [Your Team]

Executive Summary

- Summarise the purpose of the risk assessment.
- Describe the scope of the risk assessment (Which systems/processes/business functions)
- State whether it is an initial or subsequent risk assessment. If subsequent risk assessment, state the reason/circumstances that prompted the update and refer to the previous risk assessment report.
- Describe the overall risk posture (based on the scale used – e.g. High, Major, Critical, 20)
- List the top risks and their risk level.
- List the priority actions

Body of the Report

- Describe the purpose of the risk assessment.
- Identify the assumptions and constraints.
- Describe the risk tolerance inputs to the risk assessment.
- Descrive the methodology employed which includes the risk model and analytical approach.
- Provide a rationale for any risk related decisions during the assessment process
- Describe the uncertainties within the process and how they influence decisions.
- Describe the organisation mission/business function/information system that was evaluated (how the business process supports the business function, what mission the information system supports, the information flow and dependencies among systems or business functions)
- Summarise the risk assessment results in an easy-to-understand form for decision making.
- Identify the validity timeframe for the risk assessment.
- List the risks from the threats identified.
- Provide recommendations and highlight the priority actions.

Appendices

- List references and sources of information.
- Detailed Risk Register and any supporting evidence

Appendix B – Risk Register

This appendix provides the elements and information required for the development of a risk register.

- Risk ID – A unique identifier for the risk
- Source – the source of the discovered risk
- Vulnerability – The weakness creating the risk
- Threat – The threat exploiting the vulnerability.
- Affected Asset – What asset is affected by the risk
- Current Mitigating Controls – Compensating controls currently in place to reduce the risk
- Risk Likelihood – The likelihood of risk occurrence
- Risk Impact – The potential impact of the risk
- Quantitative Risk – A numerical value assigned to the risk exposure based on the likelihood and impact
- Qualitative Risk – A qualitative description of the risk exposure based on the likelihood and impact (dependent on scale used)
- Risk Treatment Decision – Best treatment of risk based on costs, resource requirements and other factors
- Risk Treatment Plan – Plan to reat the risk based on the Risk Treatement Decision
- Residual Risk Likelihood – Residual Likelihood after the risk treatment has been implemented
- Residual Risk Impact - Residual impact after the risk treatment has been implemented
- Residual Quantitative Risk – A numerical value assigned to the residual risk exposure based on the likelihood and impact
- Residual Qualitative Risk – A qualitative description of the residual risk exposure based on the likelihood and impact
- Risk Owner – Who is responsible
- Supporting Roles – Who will be supporting the owner in treating risk and what are their responsibilities
- Due Date – When the risk treatment is due
- Status – Status of the remediation of the risk

RISK ID	SOURCE	VULNERABILITY	THREAT	AFFECTED ASSET(s)	CURRENT MITIGATING CONTROLS	RISK LIKELIHOOD	RISK IMPACT	QUALITATIVE RISK	QUANTITATIVE RISK	RISK TREATMENT DECISION	RISK TREATMENT PLAN	RESIDUAL RISK LIKELIHOOD	RESIDUAL RISK IMPACT	RESIDUAL QUALITATIVE RISK	RESIDUAL QUANTITATIVE RISK	OWNER	SUPPORTING ROLES	DUE DATE	STATUS

Figure B.1 Sample Risk Register


Designated CII Sectors
National Security & Intelligence
Information & Communication Technology (ICT)
Banking and Finance
Energy
Water
Transport
Health
Emergency Services
NATIONAL AMBULANCE SERVICE
Government
Food and Agriculture
Manufacturing
Mining
Education

FREEDOM AND JUSTICE

A Secure and Resilient Digital Ghana

www.csa.gov.gh