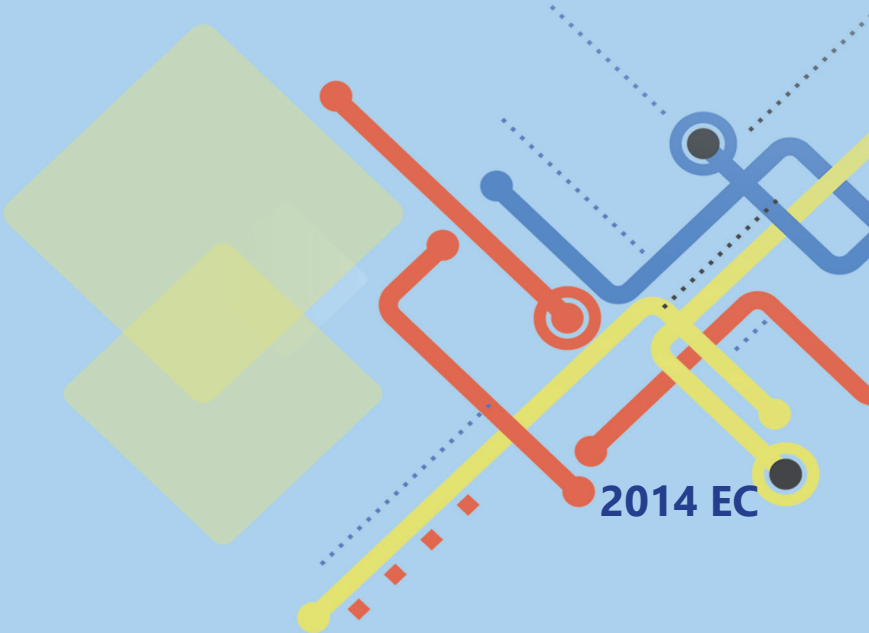
Information Network Security Agency (INSA)

# CYBER SECURITY RISK ASSESSMENT FRAMEWORK

## Version 1.0



2014 EC

Information Network Security Agency (INSA)

# CYBER SECURITY RISK ASSESSMENT FRAMEWORK

## Version 1.0

**2014 EC**

## Forward

Cyberspace is more than just the information and communications technology. It is a domain similar to the domains of land, air, sea, and space, but with its own distinct characteristics and challenges. The cyber domain is characterized by digital storage, modification, and exchange of information through interconnected systems and supported by critical information technology infrastructures. The nation's economy, the administration of government, and the provision of essential services now rely on the integrity of cyberspace and on the infrastructure, systems, and information that support it. A loss of trust in that integrity would jeopardize the benefits of this technological revolution. As all aspects of organizations/nations have become more dependent on a secure cyberspace, new vulnerabilities have been revealed and new threats continue to emerge.

To address these challenges at the national level, a comprehensive cyber security risk assessment should be conducted by identifying several key challenges on organizational governance, processes, humans and technology resulting directly from emerging risk areas.

Recognizing this and understanding the critical role of cyber security risk assessment, the **Information Network Security Agency (INSA)** has developed the National Cyber security Risk Assessment Framework The purpose of the framework is to enable organizations on how to conduct cyber security risk assessments at strategic, tactical and operational level.

Draft national policies, laws, standards, and strategies that enable to ensure the information and computer-based key infrastructures security and oversight their enforcement upon approval is one of the power and duties are given to the Information Network Security Agency (INSA).

Therefore, this framework is issued by Information Network Security Agency (INSA) pursuant to Article 13 of Information Network Security Agency Re-establishment proclamation Execution council of ministers Regulation No.320/2014

## Acronyms

| Abbreviation | Description |
|---|---|
| **SGOC** | Strength, Gap, Opportunity and Challenge |
| **PESTLE** | Political, Economic, Social, Technological, Legal and Environmental |
| **ISO** | International Organization for Standardization |
| **BMIS** | Business Model for Information security |
| **ISMS** | Information Security Management System |

# Contents

# 1. Introduction

Risk assessment involves identifying and analyzing risks in order to take adequate measures to reduce risk to an acceptable level. Risk assessment is one part of risk management, and it is an on-going process of discovering, correcting and preventing security problems. It also plays significant role in mitigation and reducing vulnerabilities.

This risk assessment framework can be used to assess the cyber security risks at strategic, tactical and operational levels, by focusing on people, technologies, process and organizational governance. The framework can enable to effectively assess cyber security risks and develop cyber security risk profiles for national, Sectorial and organizations that have impacts on their all over business operations.

# 2. Objective

## 2.1. General Objective

The general objective of this framework is establishing effective process and method in order to assess national, sectorial and organizational cyber security risks.

## 2.2. Specific Objectives

- Enables to adequately identify and analyze cyber security risks.
- Enables to produce cyber security risk registers which will help to mitigate and follow up the status of the risks.
- Helps to identify adequate and cost effective cyber security controls to protect

# 3. Characteristics of the Risk Assessment Framework

The framework has the following characteristics which will help to make the execution of risk assessment more effective.

A. **Comprehensive:** this framework encompasses strategic, tactical and operational levels risk assessment. It also considers national, sectorial and organizational risk assessments.

B. **Simple and Effective:** this framework is designed in a way that will be simple to implement and effective on assessing cyber security risks.

C. **Contextualization:** this framework is contextualized considering the overall situation of our country. It also empowers sectors and organizations to adapt the framework based on their context.

D. **Generic:** This framework is applicable for various sectors and organizations with different size, type and context.

## 4. Perspectives of Risk Assessment

The risk assessment framework perspectives focus on organizational governance, human (people), process and technology. This will help to make the risk assessment holistic and effective.

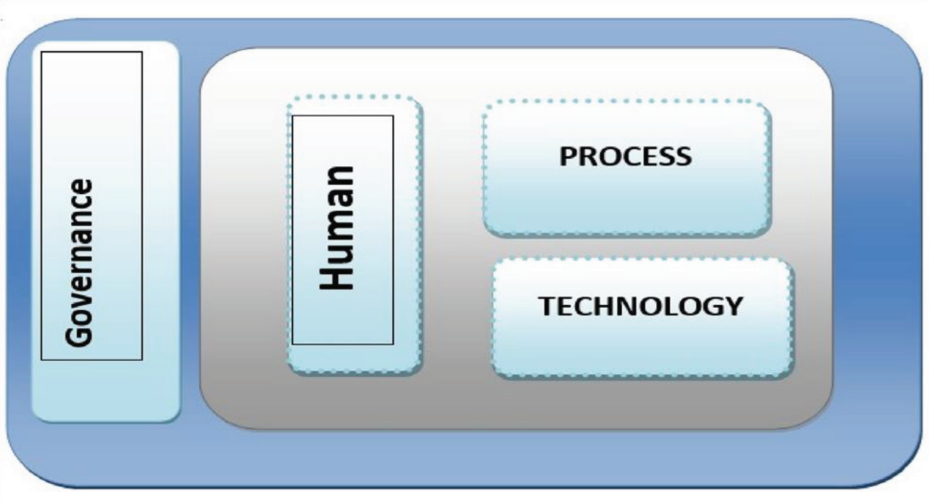



Fig 1: Cyber security risk assessment perspectives

A. **Governance:** governance focuses on identifying the status regarding the strategic and managerial aspects of cyber security. Some of the issues that should be assessed includes the following.

- Availability of adequate cyber security governance and management frameworks such as strategy, policies and procedures.
- Embedding information security in the structures and processes.
- Establishment of information security department or other responsible body.
- Adequate management of information security risks.

B. **Human:** this element focuses on the human resources and the security issues that surround them. It addresses the security capability of the human resource at each level of the organization. The capability ranges from security awareness to security expertise. It also considers the security issues that should be considered while managing the human resource. Some of the issues that should be assessed include the following.

- Cyber security awareness and culture of management members, employees and other third parties.
- Availability of cyber security professionals and managers, and their level of expertise.
- Cyber security consideration from recruitment to termination process of human resource management.

C. **Process:** process includes developed and implemented cyber security processes that will help to practice cyber security as part of the day to day activities and strategic initiatives. Some of the issues that should be assessed include the following.

- The development of cyber security processes in alignment with the context of the organization or sector.
- The implementation of the developed processes and their effectiveness.
- Technology: the technology element involves the secure implementation of the information technologies of the organization or sector, and the availability of adequate cyber security technologies. Some of the issues that should be assessed include the following.
- The secure implementation of existing information technologies.
- The availability of adequate cyber security technologies.
- The measures to keep the technology and security controls up-to-date and invulnerable.

## 5. Cyber security risk assessment framework

The following figure shows the cyber security risk assessment framework which helps to make national, sectorial and organizational risk assessment. Each component of the framework will be explained in the following sections.

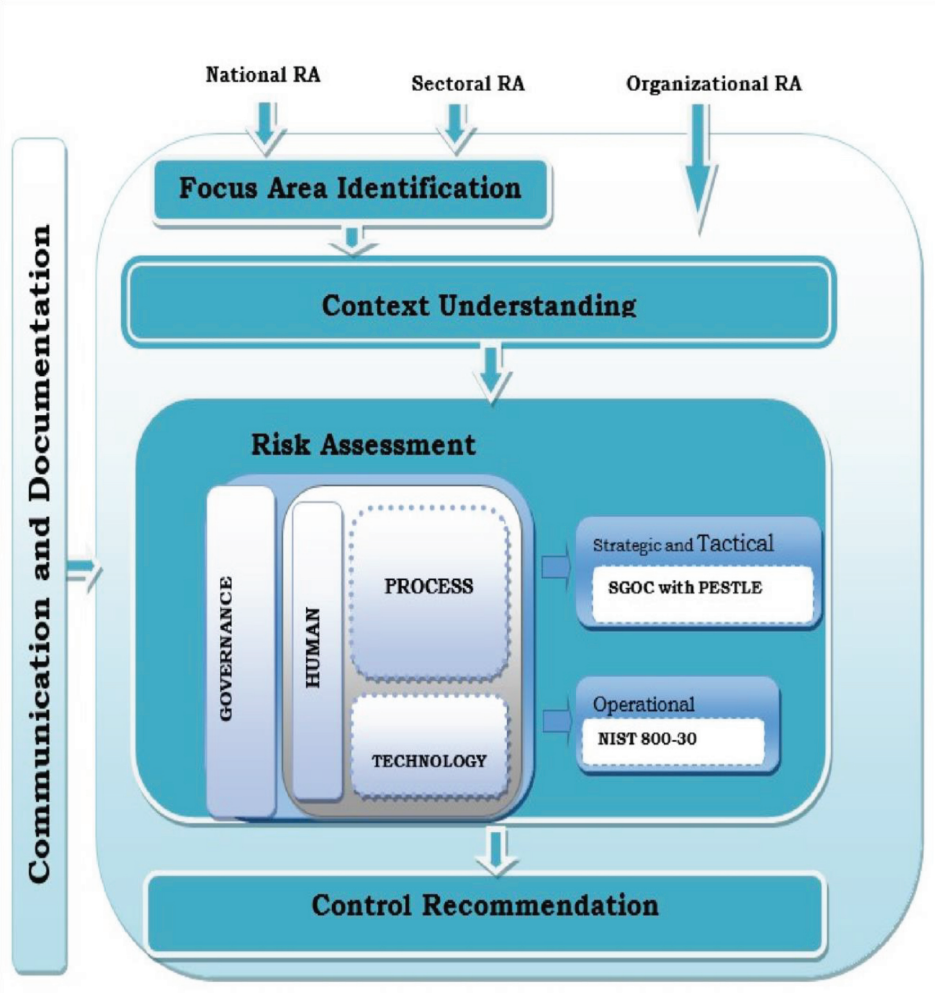



Fig.2: Cyber security risk assessment framework

## 5.1. Focus Area Identification

Focus area identification is the first step in national and sectorial risk assessment. The purpose of this step is to select the assessment area of the national and sectorial cyber security risk assessment. Assessing risk arising from the selected focus area should show how cyber security risks can damage the national and sectorial level interest in terms of political, social, economic and environmental factors.

To effectively identify focus areas of risk assessment, the responsible body for the assessment should have a selection criteria based on the objective of the risk assessment. The criteria should consider overall aspects including /but not limited to/ political, social, and economic aspects.

## 5.2. Context Understanding

The purpose of defining the context for risk assessment is to set the stage for risk assessment. Context understanding involves understanding the mission, vision, business process, structure and other internal aspects of the organization as well as external factors and third parties which can affect the security of the organization.

Establishing the context defines the scope for the risk assessment process and sets the criteria against which the risks will be assessed. The scope should be determined within the context of the firm's organizational objectives. Risks are uncertainties that affect the achievement of business objectives, so risks cannot fully be identified if these objectives and strategies are unclear.

### A. Context understanding issues

The following issues should be considered in context understanding:

**Understanding the organization and its context**: The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system (ISMS). Understanding the needs and expectations of interested parties: Interested parties and stakeholders that are relevant to the information security management system should be identified and their needs and expectations /requirements/ related to information security should be analyzed.

**Determining the scope of the information security management system:** The organization shall determine the boundaries and applicability of the information security management system to establish its scope.

B. **Context understanding techniques**

The context of an organization or sector can be understood by different techniques. Some of the techniques are:

- Reviewing documents related with the organization and its business processes
- Reading the organization establishment proclamation or related documents
- Visiting the organization website and other websites which genuinely describe about the organization.
- Discussing with relevant bodies of the organization (interview).
- Disseminating questionnaires for relevant bodies of the organization.

## 5.3. Risk Assessment

Risk assessment consists of strategic, tactical and operational level assessments. The strategic and tactical assessment can be conducted in combined way as discussed in the following section. The operational level assessment should be conducted separately since it requires a different approach. However, the operational level assessment should be aligned with the strategic and tactical assessment.

### 5.3.1. Strategic and tactical risk assessment

Strategic and tactical levels risk assessment enables to identify the cyber security governance and management status. It can be conducted using SGOC with PESTLE in it. This helps to identify the Strengths, Gaps, Opportunities and Challenges of the organizations or sector regarding cyber security, and analyze the impact on the Political, Economic, and Social, Technological, Environmental and legal aspect /PESTLE/.

1. **Risk identification and analysis using SGOC and PESTLE**

The strategic and tactical risks can be identified using SGOC identification. It also include identifying the threats and threat actors using PESTLE. The SGOC identification should address all the perspectives mentioned in section 4 and should focus on strategic and managerial aspects.

Data collection techniques, such as interview, questioner, document review and observation can be used to identify the current cyber security status of the organization or sector. The selected techniques should enables to address the SGOC identification in all perspectives and identification of threat and threat actors based on PESTLE aspects.

SGOC and PESTLE will also be applied to analyze the findings. The SGOC with PESTLE in it analysis will show the strategic and tactical current cyber security status and threats both from internal and external. It also shows the impact of the current status (mainly gaps) on the overall PESTLE aspects of the organization or sector. The analysis also shows the probability of the threats exploiting the gaps identified. As a result the overall risk level can be explained using the impact and the probability.

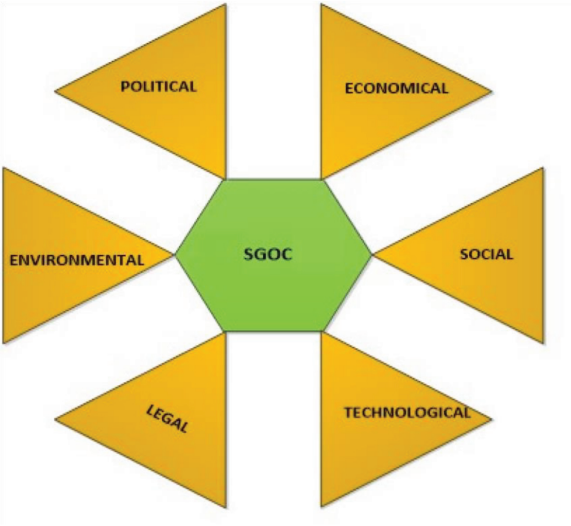



Fig.3 SGOC with PESTLE in it

## A. SGOC

The general notion of **SGOC** is described as follows.

**Strength:** Internal factors that are favorable to achieve cyber security objectives by establishing security controls which are used to secure the organization or sector to reduce political, economic, social, technological, legal and environmental impacts.

**Gap:** Internal factors that are unfavorable to achieve cyber security objectives. Gaps are lack of cyber security controls which may result security breach and cause adverse political, economic, social, technological, legal and environmental impacts.

**Opportunity:** External factors that are favorable to achieve cyber security objectives. Opportunities can occur for a variety of reasons and may result from sectorial, national or global changes that will bring favorable condition to assure cyber security.

**Challenge:** External factors that are unfavorable to achieve the cyber security objectives. It involves external threats or other factors that have negative impact on the cyber security of the organization, sector or nation.

## B. PESTLE

The main issues that should be consider while applying PESTLE are described below. The issues are not exhaustive and the organization or sector may include other issues as applicable.

**Political**

- Cyber threats and threat actors that originate from political intentions.
- The negative political impacts of cyber-attack that may happen due to the gaps.
- The positive political impacts of the security posture that may happen due to the strengths.

**Economical**

- Cyber threats and threat actors that emanate from groups/individuals which need economic benefits/advantages,
- The negative economic impacts of cyber-attack that may happen due to the gaps.
- The positive economic impacts of the security posture that may happen due to the strengths.

**Social**

- Cyber threats and threat actors that may target the services of the organization to adversely affect the society.
- The negative social impacts of cyber-attack that may happen due to the gaps.

- The positive social impacts of the security posture that may happen due to the strengths.

**Technological**

- Cyber threats and threat actors that may target to damage the technology of the organization.
- The negative technological impacts of cyber-attack that may happen due to the gaps.
- The positive technological impacts of the security posture that may happen due to the strengths.

**Legal**

- Legal requirements which will influence the information security, both external and internal sides.
- The negative legal impacts of cyber-attack that may happen due to the gaps.

**Environmental**

- Cyber threats and threat actors that may target the activities and/or infrastructures of the organization to adversely affect the environment,
- The negative environmental impacts of cyber-attack that may happen due to the gaps.
- The positive environmental impacts of the security posture that may happen due to the strengths.

#### 5.3.2. Operational level risk assessment

The operational level risk assessment involves identifying risks on the day to day operation of the organization and the risks related with particular assets of the organization. This assessment can be conducted using "NIST Special Publication 800:30, 2002. Risk management guide for information technology systems". The strategic and tactical risk assessment findings should be cascaded to the operational risk assessment and the findings in the two assessments should align with each other.

## 5.4. Communication and Documentation

**A. Communication**

Communication has a fundamental importance in the management of risks. It allows stakeholders to participate in, or be effectively represented in, decisions about assessing and managing risks. It also plays a vital part in putting decisions into practice - whether helping stakeholders to understand each phase of the assessment, informing them and advising them about risks they can control themselves, or dissuading them from antisocial and risky behavior.

Risk communication is an activity to achieve agreement on how to manage risks by exchanging and/or sharing information about risk between the decision-makers and other stakeholders. The information includes, but is not limited to the existence, nature, form, likelihood, severity, treatment, and acceptability of risks. (Refer annex C)

Risk communication should be carried out in order to achieve the following:

- To collect risk information
- To share the results from the risk assessment and present the risk treatment plan
- To avoid or reduce both occurrence and consequence of information security breaches due to the lack of mutual understanding among decision makers and stakeholders
- To support decision-making
- To obtain new information security knowledge
- To co-ordinate with other parties and plan responses to reduce consequences of any incident
- To give decision makers and stakeholders a sense of responsibility about risks • To improve awareness

**B. Documentation**

For each stage of the assessment process, adequate records must be kept that are sufficient to satisfy an independent audit. Documentation should be clearly labeled with classification level, revision date and number, effective dates, and document owner. Appropriate documentation that is readily available regarding risk assessment as well as other relevant risk related matters is required to effectively manage risk.

Annex B shows documentation guidance.

## 5.5. Control Recommendation

Control recommendation involves suggesting adequate control implementation for the risks identified in the strategic, tactical and operational risk assessments in order to reduce risk to an acceptable level. The control recommendation and implementation are mainly part of the next stage of risk assessment, i.e. risk treatment

# Annexes

## Annex A:

**Strategic and tactical risk assessment template**

The strategic and tactical risks assessment result can be compiled with the following template.

| Threats | Gaps | Impact | | | | | | Likelihood | Risk level |
|---|---|---|---|---|---|---|---|---|---|
| | | Political | Economic | Social | Technological | Legal | Environmental | | |
| | | | | | | | | | |

## Annex B: Documentation guidance

The following documents should be prepared as a final output of the risk assessment process. These documents are the minimum required documents there could be more documents produced in the risk assessment process.

**1. Risk Assessment Report**

Risk assessment report should be prepared and delivered to audiences with the expected quality, format and time.

The strategic and tactical risk assessment report should contain at the following contents. The operational risk assessment report can be prepared using the format used in the NIST SP 800-30.

1. Executive summary
2. Purpose
3. Scope
4. Audience
5. Applied methods

6. Context understanding
7. Assessment findings
8. Analysis
9. Conclusion
10. Recommendation
11. Appendices

**2. Risk Register**

A risk register should be prepared and maintained up to date through continuous monitoring of the current status of the risks identified.

**Performance Evaluation**

A responsible body should measure the risk assessment result and the documents by applying different performance measurement methods, and take corrective actions if the assessment document fails to adequately address the expected results. Some of the metrics to measure the performance includes, but not limited to:

- **Quality:** follow proper assessment methods and getting genuine information.
- **Content:** addressing all the required areas and perspectives of the organization.
- **Relevance:** fulfill the objective of the risk assessment.

## 6. References

1. INSA, 2016. Critical mass cyber security requirement standard V1.0
2. ISACA, 2014. CISM_review manual
3. NIST SP 800:30, 2002. Risk management guide for information technology systems
4. ISO/IEC 27005:2011, Information technology — security techniques — information security management systems

+251-11-371-71-14
Fax: +251-11-3-20-40-37
P.O.BOX: 124498
contact@insa.gov.et
www.facebook.com/INSA.ETHIOPIA
www.insa.gov.et
Addis Ababa
Ethiopia