Threat Risk Assessment Template

Ministry of Central Services
Information Technology Division
Information Security Branch

Last revised: October 2018
Last reviewed: October 2018
Next review: October 2019

Table of Contents

Revision History

Date (dd/mm/yyyy)	**Version**	**Comments**	**Reviewers Name**
03/05/2015	0.1	Template Created	Fuad Iddrisu
02/10/2018	0.2	Minor revisions to threat and vulnerability tables.	Darren Sproat

1. Executive Summary

A risk assessment is the foundation of a comprehensive information systems security program. It is the process of identifying, analyzing, and reporting the risks associated with an IT system's potential vulnerabilities and threats.

Good business practices require all "major systems/applications" to undergo formal risk assessment reviews as part of their certification process. Risk assessments must be performed for each major system/application or when there is a major change in the system's technical environment.

Use this section to provide a summary of what you were asked to review/assess and the specific risk concerns.

2. Scope

What is the extent/magnitude of the assessment?

3. Summary of Findings

List the observations from the assessment based on prioritized risk.

4. Background

Describe the history and nature of the problem.

5. Risk Identification

5.1. Business Impact Assessment

This section should answer questions such as what is the asset classification. Use the Statement of sensitivity questionnaire to classify the asset. Once the classification is understood, ask the questions below to understand the business impact of a compromise on CIA, in order to understand the overall business impact.

- *What is the impact of a compromise on confidentiality?*
- *What is the impact of a compromise on integrity?*
- *What is the impact of a compromise on availability?*
- *What is the overall business impact?*

5.1.1. Network Diagram

Insert/draw a network diagram or topology

5.2. Threat and Vulnerability Assessment

5.2.1. Threat Assessment

This section should identify threats that could affect the asset in scope of the assessment. Note that a threat is any action that could disrupt the ability of an asset to fulfill its purpose in a secure manner. Use GOS threat catalogue for threat identification.

Threat #	Threat Descriptions	Threat Likelihood
T1		
T2		
T3		

5.2.2. Vulnerability Assessment

Vulnerabilities are flaws or weaknesses in system security procedures, design, Implementation or internal controls that could be exercised (accidentally triggered or intentionally exploited) resulting in a security breach or a violation of the systems security policy. In this section, consider the current state of existing safeguards, and if the infrastructure components are still vulnerable to the possible threats, describe the vulnerability (i.e. how can a threat/threat agent get at the asset being protected?)

Vulnerability #	Vulnerability Descriptions
V1	
V2	
V3	

5.3. Security Control Selection

5.3.1. Assess and Evaluate Risk

In this section, potential impacts and the likelihood of occurrence are projected, with consideration of existing controls /safeguards that could reduce the impact /likelihood. Use a risk rating of Critical, High, Medium, low and insignificant to describe the magnitude of risk.

Threat Type	Threat Description	Threat Likelihood	Impact Rating	Risk Exposure Rating
T1				
T2				
T3				

5.3.2. Recommendations

In consideration of the potential vulnerability and risk, what additional safeguards are recommended to lower the risk to an acceptable level? Describe the proposed measures.

Appendix A: Risk, Likelihood, and Impact Ratings

Risk Rating

Rating	Descriptor	Description
5	**Critical**	Immediate action is required
4	**High**	Consider action and have a contingency plan
3	**Medium**	Consider action
2	**Low**	Keep under periodic review
1	**Insignificant**	Trivial impact

Likelihood Rating

Rating	Threat Likelihood	Description
5	**Almost Certain**	Greater than 75% probability of occurrence. Almost certain it will happen or is already happening
4	**Likely**	Between 50% and 75% probability of occurrence. Very likely. Will occur in most circumstances (next 12 months)
3	**Possible**	Between 25% and 50% probability of occurrence. Probability of occurring 1-5 years
2	**Unlikely**	Less than 25% probability of occurrence. Unlikely, may occur at some point (5-10 years)
1	**Rare**	Never happen, may occur in exceptional circumstances. No material probability of occurrence, possible but would be very surprising

Impact Rating

Rating	Impact	Description
5	**Catastrophic**	Loss of ability to sustain ongoing operations
4	**Major**	Significantly reduced ability to achieve business strategies and objectives
3	**Moderate**	Risks that should be watched; Currently well-managed and should have limited effect on the achievement of business strategy and objectives
2	**Minor**	No material impact on the achievement of business strategy and objectives
1	**Insignificant**	Trivial impact

Risk Exposure Matrix

Risk Exposure Matrix		IMPACT				
		Insignificant	Minor	Moderate	Major	Catastrophic
LIKELIHOOD	Almost Certain	Low	Medium	High	Critical	Critical
	Likely	Low	Medium	High	Critical	Critical
	Possible	Insignificant	Low	Medium	High	High
	Unlikely	Insignificant	Low	Low	Medium	Medium
	Rare	Insignificant	Insignificant	Insignificant	Low	Low