Example Health System

Security Threat and Risk Assessment (TRA)

<Title of assessment/target assessed>

<Date>

<Branch>

<Division>

**Table of Contents**

[Introduction 3](#_Toc97905131)

[1 Target Definition 4](#_Toc97905132)

[1.1 Prepared For 4](#_Toc97905133)

[1.2 Key Stakeholders 4](#_Toc97905134)

[1.3 Scope 4](#_Toc97905135)

[1.4 Background 4](#_Toc97905136)

[1.5 References 4](#_Toc97905137)

[1.6 Information Classification 5](#_Toc97905138)

[2 Vulnerabilities & Threats Identification 6](#_Toc97905139)

[2.1 Identification of Known Vulnerabilities 6](#_Toc97905140)

[2.2 Threats Identification and Definition 7](#_Toc97905141)

[3 Threats & Risks Assessment and Treatment 9](#_Toc97905142)

[4 Conclusion 12](#_Toc97905143)

[5 Reviews and Approvals 13](#_Toc97905144)

[5.1 Information Controller Signature 13](#_Toc97905145)

[5.2 CISO Signature 13](#_Toc97905146)

[Appendix A: Statement of Sensitivity 14](#_Toc97905147)

[Information Classification 14](#_Toc97905148)

[Confidentiality 15](#_Toc97905149)

[Integrity 16](#_Toc97905150)

[Availability 16](#_Toc97905151)

[Information Classification Declaration 17](#_Toc97905152)

**History Version**

| **Date** | **Author** | **Version** | **Description of Change** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

# Introduction

This Security Threats and Risks Assessment (TRA) is primarily used to identify and assess risks relating to a service or solution (target of the assessment), develop and define treatment of identified risks, and ensure that identified risks become part of the appropriate Government Risk Register, ensuring that risks are monitored and managed while the related service or solution is used to the benefit of the citizens of our region.

The TRA should be used in advance of deciding whether a service or solution should be implemented based on assessed risks to the population and potential treatment of the risks by the project team.

Steps used to perform the assessment:

1. Identification and definition of the target
2. Vulnerabilities & Threats Identification
   1. Identification of known vulnerabilities
   2. Identification of Threats
3. Threats & Risks Assessment and Treatment
   1. Assessment of Risk Exposures based on probability and potential impacts of a threat
   2. Determine action for each threat (accept/ reduce/ avoid/ transfer)
   3. Define actual treatment plan based on actions for each threat
4. Conclusion: What are the next steps, or final recommendations

# Target Definition

This section should cover:

* The motivation for conducting the assessment
* Who requested the TRA
* Stakeholders for the system being considered
* What is being assessed at a high level – in other words – what is the “target”, what does this “target” do and where is it located, and what is the status of the target (is it implemented? Pilot? Proof of Concept? In process of being implemented?)
* What is the scope of the assessment? Are there only certain subsystems or types of devices being assessed? Which particular use-cases are being assessed? Any impacts due to scope?
* Who are the end users of the system? Internal versus external populations?
* Diagrams are often helpful if possible to help describe the environment the TRA is being performed on.

## Prepared For

State who requested the TRA

## Key Stakeholders

List key stakeholders impacted by the target

## Scope

Provide overview of scope – what you will be assessing exactly? i.e. is this a documentation review only? Will there be additional penetration testing/vulnerability scanning conducted?

## Background

Provide a context regarding the target and the need for the TRA

## References

List References such as project documents, legislation, policies, design documents, etc.; if more than five refs, please add an appendix at the end and move it there

## Information Classification

Please complete the Statement of Sensitivity (SoS) self-assessment in Appendix A to assist completing this section for the application or system. In addition, summarize the data classification information below.

Please use this space to provide any comments on the sensitivity of the information assets associated with the system:

|  |
| --- |
|  |

Information Classification:

**Class A**: A breach or loss of information could reasonably be expected to cause extremely serious personal or enterprise injury, including significant financial loss, loss of life or public safety, social hardship, major political or economic impact.

**Class B**: A breach or loss of information could reasonably be expected to cause serious personal or enterprise injury, loss of competitive advantage, loss of confidence in the government, financial loss, legal action, damage to partnerships, relationships and reputation.

**Class C**: A breach or loss of information could reasonably be expected to cause personal or enterprise injury including limited levels of financial losses and impacts on services, performance levels, and reputation.

**Public**: A breach or loss of information will not result in injury to individuals, governments, or private sector institutions.

|  |  |  |  |
| --- | --- | --- | --- |
| **SoS Questions** | **Confidentiality** | **Integrity** | **Availability** |
| Information Class [Protected A, B, C or Public?] | [Critical|High|Medium|Low] |  |  |
| Integrity Class [Low, Medium, High, or Very High?] |  | [Low|Medium|High|Very High] |  |
| What is the RTO? |  |  |  |
| What is the RPO? |  |  |  |

Recovery Time Objective (RTO) often refers to the quantity of time that an application, system and/or process, can be down for without causing significant damage to the business as well as the time spent restoring the application and its data.

Recovery Point Objective (RPO) generally refers to the amount of data that can be lost within a period most relevant to a business, before significant harm occurs, from the point of a critical event to the most preceding backup.

# Vulnerabilities & Threats Identification

## Identification of Known Vulnerabilities

*Vulnerabilities are the known potential weaknesses or short-comings of a solution that are known and could be exploited by an attack.*

Provide a brief introduction regarding the method used to identify vulnerabilities, such as reference material where the information was found, interviewee list, vulnerability scan, etc. Provide a high level overview of the vulnerabilities of the target.

Vulnerabilities do not necessarily have to be technical vulnerabilities; it could be short-comings of a solution, i.e. a lack of documented process, limited logging, insufficient monitoring, no encryption, no backup/disaster recovery solution, etc.

For technical vulnerabilities, refer to OWASP[[1]](#footnote-1) as a reference or others. DO NOT list technical vulnerabilities below if it is NOT proven to be a weakness of the system; if it is a potential threat then it should be listed in the Threats section.

Here are some areas where lack of controls could introduce a potential weakness or vulnerability:  
*Confidentiality, integrity, availability, authentication, authorization, auditability, patching, physical security, proactive vulnerability assessment*, *security plan, incident management, operational support, data classification*, data residency, etc.

| **ID** | **Vulnerability Description** | **Vulnerability Rating** |
| --- | --- | --- |
| V1 | <e.g. **The solution or service is in the cloud** and little information is provided about protections in place> | <e.g. High> |
| V2 | <e.g.: **The solution uses a custom authentication mechanism** and does not integrate with industry standard tools> | <e.g. High> |
| V3 |  |  |
| V4 |  |  |

LEGEND FOR VULNERABILITY RATING:

|  |  |
| --- | --- |
| Very High | Exploitation of this vulnerability is almost certain (>90%) in 12 months. |
| High | Exploitation of this vulnerability is likely (>60% and <90%) in 12 months. |
| Medium | Exploitation of this vulnerability is possible (>40% and <60%) in 12 months. |
| Low | Exploitation of this vulnerability is unlikely (>10% and <40%) in 12 months. |
| Very Low | Exploitation of this vulnerability is extremely rare (<10%) in 12 months. |

## Threats Identification and Definition

*Threats are the potential exploits of vulnerabilities that could be performed during an attack, and the potential negative impacts resulting from these exploits.*

Provide a brief intro to explain at a high level how threats were identified. For each threat identified, clearly and briefly describe in a short paragraph the threat itself, then “**bold**” what will be used as a short description for the threat. It is preferred that the threats link back to the vulnerabilities in the previous section. Also identify the potential threat actor(s), and describe the impact to the business or their potential reaction /response to the threat actually occurring. For threat models, it may be useful to refer to models such as MS STRIDE[[2]](#footnote-2) or others.

| **ID** | **Threat Description**  (link back to vulnerabilities where possible) | **Threat Actor** | **Potential Impacts** |
| --- | --- | --- | --- |
| T1 | <e.g. **Unauthorized access to system data** causing loss of confidentiality, integrity or availability of data (V1, V2)> | <e.g. Malicious attacker> | <e.g. The data within this system is critical to the program and extremely confidential in nature. Data becoming public, being modified or becoming unavailable would cause significant harm to the service and could impact the operator’s reputation.> |
| T2 | <e.g. **Accidental data breach** by sharing a file through an email link, therefore losing access controls to the file and allowing the recipient to share the file through the same link (V1).> | <e.g. Authorized user> | <e.g. The data within this system is critical and extremely confidential in nature. Data becoming public, being modified or becoming unavailable would cause significant harm to the service and could impact the operator’s reputation.> |
| T3 |  |  |  |
| T4 |  |  |  |

# Threats & Risks Assessment and Treatment

*The Risk is essentially the organizational exposure generated by the probability and potential impact of a threat materializing itself. It is assessed by multiplying the* ***probability (P)*** *factor with the* ***impact (I)*** *factor to obtain the overall* ***exposure (E=PxI)*** *factor, which is used to assign a priority to the various identified threats.*

*Treatment refers to the response to identified risks. Will the key stakeholders* ***Accept*** *the risk and do nothing to mitigate them? Will they* ***Reduce*** *the risk – that is – develop a mitigation plan or implement a measure to reduce the probability and/or the impact of the risk? Will they* ***Avoid*** *the risk by discontinuing activities that are generating the risk? Will they* ***Transfer*** *the risk by outsourcing work relating to potential impacts or passing it on to partners?*

Each threat listed above should be listed in the following table – cut and paste – and assessed as to probability (P) and impacts (I). Exposure (E) is determined as a product of P and I. Provide a brief introduction to this assessment section.

Actions should be taken based on the Probability and potential Impacts of each threat (Accept/ Reduce/ Avoid/ Transfer), and Treatment/Response are likely to involve dealing with identified vulnerabilities (plugging the holes essentially). The Risk Owner may be different for each risk; therefore, it’s best to identify the area or name of the risk owner for each risk identified below.

| **ID** | **Threat Description** | **P** | **I** | **E**  (PxI) | **Action**  **(Accept, Reduce, Avoid, Transfer)** | **Treatment/Response** | **Risk Owner** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| T1 | <e.g. **Unauthorized access to system data** causing loss of confidentiality, integrity or availability of data (V1, V2)> | 3 | 4 | 12 | <e.g. Reduce> | <e.g. The implementation project will reduce the risks associated to unauthorized access, in particular due identified vulnerabilities by implementing “Tool X” as an interface that will integrate the solution’s authentication mechanism thereby creating an artificial single sign on environment.> | <e.g. Area / Name> |
| T2 | <e.g. **Accidental data breach** by sharing a file through an email link, therefore losing access controls to the file and allowing the recipient to share the file through the same link (V1).> | 5 | 4 | 20 | <e.g. Accept> | <e.g. The business recognizes the risks, however, the ability to share documents using emailed links is one of the key functions they are looking for.> | <e.g. Area / Name> |
| T3 |  |  |  |  |  |  |  |
| T4 |  |  |  |  |  |  |  |

LEGEND FOR PROBABILITY (P):

|  |  |  |
| --- | --- | --- |
| 5 | Very High | Almost Certain: Event is expected to occur with a probability of 90% or higher in 12 months. |
| 4 | High | Likely: 60 to less than 90% chance of occurrence in 12 months |
| 3 | Medium | Possible: 40 to less than 60% chance of occurrence in 12 months |
| 2 | Low | Unlikely: 10 to less than 40% chance of occurrence in 12 months |
| 1 | Very Low | Rare: Less than 10% chance of occurrence in 12 months. |

LEGEND FOR IMPACT (I):

|  |  |  |
| --- | --- | --- |
| 5 | Critical | Catastrophic: A disaster with the potential to lead to long term damage or permanent outage |
| 4 | High | Major: Major event that with proper management can be endured |
| 3 | Medium | Moderate: Significant event that can be managed under normal circumstances |
| 2 | Low | Minor: An event that can be absorbed |
| 1 | Very Low | Insignificant: The event will have almost no impact if realized |

LEGEND FOR EXPOSURE (E): Priority indicator

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 5 | 5 | 10 | 15 | 20 | 25 |
| 4 | 4 | 8 | 12 | 16 | 20 |
| 3 | 3 | 6 | 9 | 12 | 15 |
| 2 | 2 | 4 | 6 | 8 | 10 |
| 1 | 1 | 2 | 3 | 4 | 5 |
| **P / I** | 1 | 2 | 3 | 4 | 5 |

# Conclusion

Summarize findings as well as proposed next steps and final recommendations. This could include “NOT” implementing the service or the solution for instance, or implementing it along with identified treatment plans.

# Reviews and Approvals

## Information Controller Signature

The responsible Information Controller or delegate (Service/Risk Owner) has reviewed the risks and recommendations, and signs below as acceptance of risks (along /w recommended treatment plans).

Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## CISO Signature

The Chief Information Security Officer (CISO) of the appropriate organizational body has reviewed the risks and recommendations and confirms that due diligence was used in the completion of this assessment. Please note, the CISO does not sign off risks.

Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Appendix A: Statement of Sensitivity

The three key properties of information security are confidentiality, integrity, and availability. The Information Classification is based on the assessments of these three key properties of the information. This Statement of Sensitivity is intended to assist the Information Owner in assessing the confidentiality, integrity, and availability requirements of an information system and in identifying the Information Classification.

**Confidentiality** – Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. The confidentiality level assessed for information assets informs the level of protection necessary to prevent disclosure of information to unauthorized parties.

**Integrity** – Integrity is the property of information accuracy and completeness and refers to the level of protection necessary to prevent information assets from being modified by unauthorized parties.

The information integrity level assessed for information assets informs the level of protection necessary to ensure that information is authentic and protected from alteration by unauthorized parties.

**Availability** – Availability is the property of information being accessible and usable upon demand by an authorized entity. The availability level assessed for information assets informs the level of protection necessary to ensure that authorized entities are able to access the information when needed. Information security controls ensure that information assets are available to authorized parties whenever they need to access them.

## Information Classification

Information can be classified based on it’s sensitivity and/or value.

**Class A**: A breach or loss of information could reasonably be expected to cause extremely serious personal or enterprise injury, including significant financial loss, loss of life or public safety, social hardship, major political or economic impact.

**Class B**: A breach or loss of information could reasonably be expected to cause serious personal or enterprise injury, loss of competitive advantage, loss of confidence in the government, financial loss, legal action, damage to partnerships, relationships and reputation.

**Class C**: A breach or loss of information could reasonably be expected to cause personal or enterprise injury including limited levels of financial losses and impacts on services, performance levels, and reputation.

**Public**: A breach or loss of information will not result in injury to individuals, governments, or private sector institutions.

## Confidentiality

Answer each of the questions in the tables that follow. The questions apply to information that is processed, transmitted, managed, and/or stored. To assist with the determination of confidentiality, conduct an injury test by asking, “Who or what will be harmed if the information is disclosed to unauthorized parties?” Remember that aggregate data can be more sensitive than an individual record or a smaller subset of records.

CRITICAL (extremely serious injury)

Does the data contain… Yes No

1. information that, if compromised, would jeopardize an individual’s safety? ☐ ☐

2. information about police informants or witness protection? ☐ ☐

3. confidential documents? ☐ ☐

4. proposed legislation or regulations under development? ☐ ☐

5. information that, if compromised, could cause damages in excess of $10,000,000? ☐ ☐

6. other examples of CRITICAL Confidentiality information? (describe below) ☐ ☐

HIGH (serious injury)

Does the data contain… Yes No

7. information that, if compromised, could cause invasion of privacy or identity theft? ☐ ☐

8. personal health information? ☐ ☐

9. government/ministerial briefing notes? ☐ ☐

10. trade secrets or intellectual property? ☐ ☐

11. information related to exploration and production of mineral/energy resources? ☐ ☐

12. information that if compromised, would cause damage of $100,000 to $10,000,000? ☐ ☐

13. other examples of HIGH Confidentiality information? (describe below) ☐ ☐

MEDIUM (low injury)

Does the data contain… Yes No

14. a small amount of personal information? ☐ ☐

15. economic statistics, analysis, and/or forecasts? ☐ ☐

16. general administrative files? ☐ ☐

17. information that, if compromised, would cause damages of $1000 to $100,000? ☐ ☐

18. other examples of MEDIUM Confidentiality information? (describe below) ☐ ☐

LOW (no injury)

Does the data contain… Yes No

19. information intended to be accessed by the public on government websites? ☐ ☐

20. job advertisements? ☐ ☐

21. public reports and policy statements? ☐ ☐

22. job duties and pay scales? ☐ ☐

23. public health news and advisories? ☐ ☐

24. other examples of LOW Confidentiality information? (describe below) ☐ ☐

## Integrity

CRITICAL Integrity

Does the data contain… Yes No

1. information that, if compromised, would impact critical infrastructure? ☐ ☐

2. information that, if compromised, may impact the food/water supply causing death? ☐ ☐

3. information on extremely large financial transactions? ☐ ☐

4. other examples of CRITICAL Integrity information? (describe below) ☐ ☐

HIGH Integrity

Does the data contain… Yes No

5. information that, if compromised, may impact the food/water supply? ☐ ☐

6. information related to non-emergency health care? ☐ ☐

7. information on financial transactions and payments? ☐ ☐

8. ownership and disposition of minerals, lands, and oil and gas rights? ☐ ☐

9. other examples of HIGH Integrity information? (describe below) ☐ ☐

MEDIUM/LOW Integrity

Does the data contain… Yes No

10. information with requirements not in the categories above? (describe below) ☐ ☐

## Availability

CRITICAL Availability

Would loss of the data or information system… Yes No

1. result in an extended loss of an essential government service? ☐ ☐

2. cause a loss of crisis communications in an emergency? ☐ ☐

3. cause a loss of emergency health services? ☐ ☐

4. disrupt financial systems resulting in losses exceeding $10,000,000? ☐ ☐

5. cause loss of a critical service identified in a Service Level Agreement? ☐ ☐

6. other examples of CRITICAL Availability? (describe below) ☐ ☐

HIGH Availability

Would loss of the data or information system… Yes No

7. cause unavailability of payments of benefits or income support citizens? ☐ ☐

8. cause unavailability of financial and reporting systems? ☐ ☐

9. cause unavailability of senior management information systems? ☐ ☐

10. disrupt financial systems resulting in losses between $100,000 and $10,000,000? ☐ ☐

11. cause loss of a medium availability service identified in a Service Level Agreement? ☐ ☐

12. other examples of HIGH Availability? (describe below) ☐ ☐

MEDIUM/LOW Availability

13. Is the data availability not covered in the categories above? (describe below) ☐ ☐

## Information Classification Declaration

Using results from the Confidentiality, Integrity, and Availability tables above, the Information Owner now declares the appropriate Information Classification of the data contained within or processed by the system. Select the appropriate class below:

|  |  |
| --- | --- |
| **Information Classification** | |
| **Class A** | A breach or loss of information could reasonably be expected to cause extremely serious personal or enterprise injury. |
| **Class B** | A breach or loss of information could reasonably be expected to cause serious personal or enterprise injury. |
| **Class C** | A breach or loss of information could reasonably be expected to cause low injury to individuals or enterprises. |
| **Public** | A breach or loss of information will not result in injury to individuals, governments, or private sector institutions. |

1. OWASP: https://www.owasp.org/index.php/Category:Vulnerability [↑](#footnote-ref-1)
2. MS STRIDE: https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx [↑](#footnote-ref-2)