# Threat and Vulnerability Identification Template

Use this template to identify key assets, associated threats, potential vulnerabilities, and initial ideas for mitigation. This exercise helps build foundational skills in cybersecurity risk assessment.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Asset Name | Asset Description | Associated Threats | Potential Vulnerabilities | Mitigation Notes |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Risk Criteria

The below explains what each item in the Risk Assessment means.

| Criteria | Description |
| --- | --- |
| **Risk Description** | Detailed explanation of the scenario, what could go wrong, and why it matters. |
| **Assets at Risk** | The information, system, or service impacted (e.g. customer data, VDI environment). |
| **Threat** | Who or what could cause the risk (e.g., insider, cybercriminal, accident, malware). The action or event (e.g., data exfiltration, privilege misuse, physical theft). |
| **Vulnerability** | Weakness – the gap or condition that enables the threat (e.g., extended idle session, clipboard sharing). |
| **Existing Controls** | Current safeguards in place (e.g., MFA, logging, endpoint DLP). |
| **Inherent Risk Rating** | Risk level before any mitigations are applied. |
| **Residual Risk Rating** | Risk level after current controls are considered. |
| **Likelihood** | The probability of occurrence (e.g., Rare, Possible, Likely). |
| **Consequence** | Severity – level of damage if realised (e.g., Minor, Moderate, Major, Extreme). |
| **Rating** | The outcome of the risk likelihood and consequence evaluation. |
| **Mitigations** | Treatment Plan – actions to reduce, transfer, avoid, or accept the risk. |
| **Risk Owner** | Person or role accountable for managing the risk (e.g., the person who uses the software) |

**Risk Assessment**

Complete this assessment for at least 3 risks.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Risk Details | | | | | |
| **Risk ID** |  | | **Date Identified** | |  |
| **Risk Title** |  | | **Review Date** | |  |
| **Risk Identification** | | | | | |
| **Risk Description** |  | | | | |
| **Assets at Risk** |  | | | | |
| **Threat** |  | | | | |
| **Vulnerability** |  | | | | |
| **Existing Controls** |  | | | | |
| **Inherent Risk Analysis** | | | | | |
| **Likelihood** | | **Consequence** | | **Inherent Risk Rating** | |
|  | |  | |  | |
| **Residual Risk Analysis** | | | | | |
| **Likelihood** | | **Consequence** | | **Residual Risk Rating** | |
|  | |  | |  | |
| **Risk Treatment** | | | | | |
| **Mitigations** |  | | | | |
| **Risk Monitoring and Review** | | | | | |
| **Risk Owner** |  | | | | |

|  |  |
| --- | --- |
| **To** | Person Person Person |
| **Cc** | Person |
| **Bcc** | Person |
| **Subject** |  |
|  | |

Cybersecurity Risk Prioritisation Matrix

**Understanding the Likelihood Rating**

The table below provides the categories and ratings for likelihood:

| Likelihood Ratings | Description | Criteria |
| --- | --- | --- |
| **Rare (1)** | Exceptional circumstances only | May occur only in very unusual situations |
| **Unlikely (2)** | Possible, but not expected | Could happen but not typical; requires specific conditions (e.g. targeted phishing bypassing all filters). |
| **Possible (3)** | Might occur at some point | Has occurred in similar organisations; realistic but not frequent (e.g. ransomware attempt on enterprise endpoint). |
| **Likely (4)** | Will probably occur in most circumstances | Expected to happen periodically (e.g. phishing emails, credential stuffing attempts). |
| **Almost Certain (5)** | Expected to occur frequently | Has occurred multiple times, highly predictable (e.g. malware probes, daily scanning activity). |

**Understanding the Consequence Ratings Table**

The table below provides the categories and ratings for impacts:

|  |  |  |
| --- | --- | --- |
| Consequence Rating | Description | Criteria |
| **Insignificant (1)** | Negligible impact | No compromise of sensitive data, no disruption, minimal financial or reputational impact. |
| **Minor (2)** | Small impact | Limited operational disruption; minimal data exposure (non-sensitive data); easily contained. |
| **Moderate (3)** | Noticeable impact | Partial service disruption; limited sensitive data exposure; moderate cost or compliance breach. |
| **Major (4)** | Severe impact | Significant outage of critical systems; large-scale sensitive data breach; regulatory non-compliance with penalties. |
| **Extreme (5)** | Catastrophic impact | Extended enterprise-wide outage; compromise of PROTECTED/SECRET data; severe financial/reputational damage; possible criminal or regulatory prosecution. |

**The 5x5 Risk Matrix**

Use this 5x5 risk matrix to evaluate and prioritise cybersecurity risks. For each identified risk, assess its likelihood (1 = Rare, 5 = Almost Certain) and impact (1 = Insignificant, 5 = Critical). Plot the risk in the matrix and use the result to guide mitigation priorities.

**Risk Levels**

| Likelihood ↓  Impact → | Insignificant (1) | Minor (2) | Moderate (3) | Major (4) | Extreme (5) |
| --- | --- | --- | --- | --- | --- |
| 5 – Almost Certain | **MEDIUM** | **HIGH** | **HIGH** | **EXTREME** | **EXTREME** |
| 4 – Likely | **MEDIUM** | **MEDIUM** | **HIGH** | **HIGH** | **EXTREME** |
| 3 – Possible | **LOW** | **MEDIUM** | **MEDIUM** | **HIGH** | **HIGH** |
| 2 – Unlikely | **LOW** | **LOW** | **MEDIUM** | **MEDIUM** | **HIGH** |
| 1 – Rare | **LOW** | **LOW** | **LOW** | **MEDIUM** | **MEDIUM** |

* **Low** – Acceptable; manage by routine controls and monitoring.
* **Medium** – Requires management attention; additional controls may be needed.
* **High** – Significant; must be treated with priority, monitored closely, and escalated to senior management.
* **Extreme** – Unacceptable; immediate executive-level attention and remediation required.

**Tips for Completing the Matrix**

- Start by identifying the risk scenario (e.g., data breach, system outage).

- Assign a likelihood score based on how often this type of risk occurs.

- Assign an impact score based on potential damage to operations, reputation, or finances.

- Use the matrix to prioritise: risks in the top-right corner (high likelihood and impact) need urgent attention.