**Disclaimer:**

This Organisation Impact Analysis template is provided for general informational purposes only. It is not a substitute for professional advice, and users should adapt it to their specific needs and circumstances. While this template is based on best practices, L2 Cyber Security Solutions make no warranties or guarantees regarding its effectiveness or suitability for any particular situation. Users are responsible for ensuring the accuracy and completeness of the analysis for their organisation. This template does not constitute legal advice, and users should consult with legal counsel for their specific legal needs. Organisation resilience best practices evolve, and users are encouraged to stay updated on industry standards. It is crucial to regularly test and revise this analysis to ensure its effectiveness.

**[Your Organisation Logo]**

**[Organisation Name]**

Organisation Impact Analysis (OIA)

Version: 1.0

Date: **[Date]**

Contents

[1. Introduction 3](#_Toc160441136)

[2. Organisation Process Identification 3](#_Toc160441137)

[3. Impact Assessment 3](#_Toc160441138)

[3.1 Financial Impact 3](#_Toc160441139)

[3.2 Operational Impact 3](#_Toc160441140)

[3.3 Reputational Impact 3](#_Toc160441141)

[4. Recovery Objectives 4](#_Toc160441142)

[5. Risk Assessment 4](#_Toc160441143)

[5.1 Threats and Vulnerabilities 4](#_Toc160441144)

[5.2 Likelihood and Impact 4](#_Toc160441145)

[6. Priority and Recommendations 5](#_Toc160441146)

[6.1 Priority Levels 5](#_Toc160441147)

[6.2 Recommended Mitigation and Recovery Strategies 5](#_Toc160441148)

[7. Appendices 5](#_Toc160441149)

# 1. Introduction

The Organisation Impact Analysis (OIA) assesses the potential impact of disruptions to operational processes and helps prioritise recovery efforts.

# 2. Organisation Process Identification

Identify and describe the critical operational processes within your organisation. Use a table to organise this information.

| **Process Name** | **Description** | **Process Owner** | **Dependencies** |
| --- | --- | --- | --- |
| Organisation Process 1 | Description 1 | Owner 1 | Dependencies 1 |
| Organisation Process 2 | Description 2 | Owner 2 | Dependencies 2 |
| ... | ... | ... | ... |

# 3. Impact Assessment

Assess the potential impact of disruptions on your critical operational processes in terms of financial, operational, and reputational factors.

## 3.1 Financial Impact

Describe the potential financial consequences of disruptions to each critical process. Use a table to summarise this data.

| **Process Name** | **Financial Impact** |
| --- | --- |
| Organisation Process 1 | Impact Description 1 |
| Organisation Process 2 | Impact Description 2 |
| ... | ... |

## 3.2 Operational Impact

Describe the potential operational consequences of disruptions to each critical process. Use a table for clarity.

| **Process Name** | **Operational Impact** |
| --- | --- |
| Organisation Process 1 | Impact Description 1 |
| Organisation Process 2 | Impact Description 2 |
| ... | ... |

## 3.3 Reputational Impact

Assess the potential impact on your organisation's reputation due to disruptions. Use a table to summarise this information.

| **Process Name** | **Reputational Impact** |
| --- | --- |
| Organisation Process 1 | Impact Description 1 |
| Organisation Process 2 | Impact Description 2 |
| ... | ... |

# 4. Recovery Objectives

Define the desired Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each critical Organisation process.

* **RTO** is the goal your organisation sets for the maximum length of time it should take to restore normal operations following an outage or data loss.
* **RPO** is the goal for the maximum amount of data the organisation can tolerate losing. This parameter is measured in time from the moment a failure occurs to the most recent backup.

| **Process Name** | **RTO** | **RPO** |
| --- | --- | --- |
| Organisation Process 1 | RTO 1 | RPO 1 |
| Organisation Process 2 | RTO 2 | RPO 2 |
| ... | ... | ... |

# 5. Risk Assessment

Evaluate the threats and vulnerabilities associated with each critical process. Use tables or matrices to present risk assessment data.

## 5.1 Threats and Vulnerabilities

List potential threats and vulnerabilities relevant to each process.

| **Process Name** | **Threats and Vulnerabilities** |
| --- | --- |
| Organisation Process 1 | Threats and Vulnerabilities 1 |
| Organisation Process 2 | Threats and Vulnerabilities 2 |
| ... | ... |

## 5.2 Likelihood and Impact

Assess the likelihood and potential impact of each threat and vulnerability. Use a matrix or tables to document this data.

| **Process Name** | **Threat/Vulnerability** | **Likelihood** | **Impact** |
| --- | --- | --- | --- |
| Organisation Process 1 | Threat/Vulnerability 1 | Likelihood 1 | Impact 1 |
| Organisation Process 2 | Threat/Vulnerability 2 | Likelihood 2 | Impact 2 |
| ... | ... | ... | ... |

# 6. Priority and Recommendations

Based on the impact assessment, recovery objectives, and risk assessment, prioritise critical processes and provide recommendations for mitigation and recovery strategies.

## 6.1 Priority Levels

Assign priority levels to each critical process based on its impact, recovery objectives, and risk assessment.

| **Process Name** | **Priority Level** |
| --- | --- |
| Organisation Process 1 | High |
| Organisation Process 2 | Medium |
| ... | ... |

## 6.2 Recommended Mitigation and Recovery Strategies

List recommended strategies for mitigating risks and achieving the defined recovery objectives.

| **Process Name** | **Mitigation and Recovery Strategies** |
| --- | --- |
| Organisation Process 1 | Strategies for Organisation Process 1 |
| Organisation Process 2 | Strategies for Organisation Process 2 |
| ... | ... |

# 7. Appendices

Include any additional information, such as a key employee dependency, detailed impact assessment data, risk assessment details, Risk Register and a glossary of terms.

This template provides a structured framework for conducting an Organisation Impact Analysis (OIA) and documenting its findings. You can customise and expand upon it to meet the specific needs of your organisation.