Threat and Vulnerability Assessment Tool

Version 4.0

This is a sample of the final product and these pages are for your review and are protected by Janco's copyright.

https://www.e-janco.com
TABLE OF CONTENTS

Threat & Vulnerability Assessment Process ................................................................. 3

Purpose ....................................................................................................................... 4

Components of a Threat & Vulnerability Assessment .............................................. 4

  Administrative Safeguards .................................................................................... 4

  Logical Safeguards ............................................................................................. 4

  Physical Safeguards ............................................................................................ 5

Threat Analysis ......................................................................................................... 5

Threat and Risk Assessment Matrix ......................................................................... 6

Threat & Vulnerability Assessment Work Plan ...................................................... 7

Threat and Vulnerability Assessment Form ........................................................... 9

What’s New ............................................................................................................... 13

This is a sample of the final product and these pages are for your review and are protected by Janco’s copyright.

https://www.e-janco.com
Risk management is a process to identify, assess, manage and control potential events to provide reasonable assurance regarding the achievement of business objectives. The risk management process has five key objectives:

1. Identify and prioritize risk arising from business strategies and activities
2. Determine the level of risk acceptable to the university (risk appetite)
3. Design and implement risk mitigation activities designed to reduce risk
4. Perform on-going monitoring activities to re-assess risk and the effectiveness of controls
5. Analysis of vulnerabilities faces
6. Review and summarization of risks and acceptability of the risks with proposed solutions

The risk management process should not be treated primarily as a technical function carried out by IT staff but rather as an essential management function of the enterprise. The principal goal of the Threat and Vulnerability Assessment Process is to protect enterprise assets and the enterprise’s ability to carry out its mission in the face of potential threats to these assets.

Successful threat and vulnerability assessments require the full support of senior management and be conducted by teams that include both functional managers and information technology administrators.

As business operations, workflow, or technologies change, periodic reviews must be conducted to analyze these changes, to account for new threats and vulnerabilities created by these changes, and to determine the effectiveness of existing controls.
PURPOSE

The purpose of the IT Security Risk Management Program is to:

- Comply with the enterprise’s security policy, as well as other mandated regulations/requirements, to develop, implement, and maintain a security plan with appropriate and auditable security controls;
- Provide a governance framework for understanding potential risks to enterprise assets based on the security plan;
- Provide guidelines for evaluating and documenting the management, operational and technical security environment of enterprise assets; and
- Provide management with direction, planning, and guidance in the area of information security.

COMPONENTS OF A THREAT & VULNERABILITY ASSESSMENT

ADMINISTRATIVE SAFEGUARDS

- Classification of data handled and identification of controls to protect those assets;
- Documentation of procedures, standards, and recommended practices to ensure that applicable policies and controls are implemented appropriately for a given business process;
- Identification of personnel who are authorized to access systems;
- Assurance that appropriate authorization controls are implemented;
- Security awareness training and education for all personnel; and
- Background checks prior to the selection and hiring of new personnel into critical positions.

LOGICAL SAFEGUARDS

- Ensure access to only authorized users and session termination when finished;
- Enforce secure password management;
- Manage tracking of development, maintenance, and changes to application software and information systems;
- Manage access to the network; and
- Ensure event logging.
## THREAT AND RISK ASSESSMENT MATRIX

<table>
<thead>
<tr>
<th>Score</th>
<th>High = 5</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>Low = 1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organizational Uncertainty</strong></td>
<td>The business unit has no plan. Management is uncertain about responsibility there is no business sponsor</td>
<td>The business unit has no specific and has designated, but not committed, resources to the initiative</td>
<td>The business unit has a plan but has not committed resources</td>
<td>The business unit has no specific plan but has committed resources</td>
<td>The business unit has a plan and has committed resources</td>
</tr>
<tr>
<td><strong>Technical Uncertainty</strong></td>
<td>No knowledge or experience</td>
<td>Emerging area</td>
<td>Some experience</td>
<td>Understood in a different area</td>
<td>Understood</td>
</tr>
<tr>
<td><strong>Skills Required</strong></td>
<td>Extensive new skills for both staff &amp; management</td>
<td>Extensive new skills for staff; some new skills for management</td>
<td>Some new skills required for both staff &amp; management</td>
<td>Some new skills for staff; none for management</td>
<td>No new skills for staff &amp; management</td>
</tr>
<tr>
<td><strong>Hardware Dependencies</strong></td>
<td>Hardware is immature; just emerging from vendor labs</td>
<td>Hardware exists but is not yet used within the organization</td>
<td>Hardware exists and has been tested, but is not yet operational</td>
<td>In use in a different application</td>
<td>In use in similar applications</td>
</tr>
<tr>
<td><strong>Software Dependencies</strong></td>
<td>Non-standard software with complex interfaces</td>
<td>Programs available commercially, but highly complex</td>
<td>Programs can be developed in-house with moderate complexity</td>
<td>Programs can be developed in-house with minimal complexity</td>
<td>Programs exist &amp; need minimal modification</td>
</tr>
<tr>
<td><strong>Application Software</strong></td>
<td>No package or solution exists. Complex design and development is required</td>
<td>Programs available commercially, but highly complex</td>
<td>Programs available commercially, but highly complex</td>
<td>Programs available commercially, but highly complex</td>
<td>Programs available commercially, but highly complex</td>
</tr>
</tbody>
</table>

### Total Technical Uncertainty Score

### Infrastructure Uncertainty

| Score | Major changes to the existing infrastructure are needed | Significant changes to the existing infrastructure are needed | Moderate changes to the existing infrastructure are needed | Small changes are required to the existing infrastructure. Investment is needed | The solution will use existing infrastructure and services no investment is required |

### Total Risk Score
## Threat and Vulnerability Assessment
### Physical and Electronic Sites

#### Risk Ranking

<table>
<thead>
<tr>
<th>Vulnerability (Probability of Threat)</th>
<th>Will Occur over 90%</th>
<th>Extreme 90%&lt; &gt;75%</th>
<th>High 75%&lt; &gt;25%</th>
<th>Moderate 25%&lt; &gt;10%</th>
<th>Low Under 10%</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Catastrophic</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Very High</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Noticeable to ENTERPRISE</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Minor</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>None</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Interpretation of scores

- **6 to 8** These risks are extreme. Countermeasure actions to mitigate these risks should be implemented immediately.
- **5** These risks are very high. Countermeasure actions to mitigate these risks should be implemented as soon as possible.
- **3 to 4** These risks are moderate. Countermeasure actions to mitigate these risks should be implemented in the near term.
- **1 to 2** These risks are low. Countermeasure actions to mitigate these risks should be implemented as convenient as they will enhance security overall.
- **None** These currently pose no risk but should continue to be monitored.
WHAT'S NEW

VERSION 4.0
- Updated to reflect the latest security and mandated requirements of US Federal, US States, EU, and ISO
- Specific work plan steps identified

VERSION 3.3
- Update the introduction to include a purpose section
- Updated electronic forms

VERSION 3.2
- Converted Risk Assessment Matrix to EXCEL Electronic Form

VERSION 3.1
- Added Risk Assessment Matrix with scoring definition

VERSION 3.0
- Section Added Components of a Threat & Vulnerability Assessment
- Section Added Threat & Vulnerability Assessment Work Plan
- Threat and Vulnerability Assessment tool provided in PDF, WORD 2007, and EXCEL 2007 formats

This is a sample of the final product and these pages are for your review and are protected by Janco’s copyright. https://www.e-janco.com