

Threat and Vulnerability Assessment Tool

Version 4.0



JANCO ASSOCIATES, INC.

**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>

THREAT & VULNERABILITY ASSESSMENT PROCESS

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:

- ✚ Identify and prioritize risk arising from business strategies and activities
- ✚ Determine the level of risk acceptable to the university (risk appetite)
- ✚ Design and implement risk mitigation activities designed to reduce risk
- ✚ Perform on-going monitoring activities to re-assess risk and the effectiveness of controls

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>

- management
 - the planning and execution:
 - ce identification)
 - f existing data
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;
- ✦ Security practices to ensure that applicable business process;
- ✦ Security systems;
- ✦ Security implemented;
- ✦ Security and
- ✦ Security personnel into critical positions.

**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>

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 Vulnerability Assessment Tool


THREAT AND RISK ASSESSMENT MATRIX

	High = 5	4	3	2	Low = 1	Score
Organizational Uncertainty	The business unit has no plan. Management is uncertain about responsibility there is no business sponsor	The business unit has no specific and has designated, but not committed, resources to the initiative	The business unit has a plan but has not committed resources	The business unit has no specific plan but has committed resources	The business unit has a plan and has committed resources	
Technical Uncertainty	No knowledge or experience	Emerging area	Some experience	Understood in a different area	Understood	
Skills Required	Extensive new skills for both staff & management	Extensive new skills for staff; some new skills for management	Some new skills required for both staff & management	Some new skills for staff; none for management	No new skills for staff & management	
Hardware Dependencies	Hardware is immature; just emerging from vendor labs	Hardware exists but is not yet used within the organization	Hardware exists and has been tested, but is not	In use in a different application	In use in similar applications	
Software Dependencies	Non-standard software with interface				Standard software; no programming is required	
<div style="border: 2px solid black; padding: 10px; background-color: white;"> <p>This is a sample of the final product and these pages are for your review and are protected by Janco's copyright.</p> <p>https://www.e-janco.com</p> </div>						
Application Software	No package or solution exists. Complex design and development is required	Programs available commercially, but highly complex. Complex design and development	extensive modifications OR Programs can be developed in-house with moderate complexity	minimal modifications OR Programs can be developed in-house with minimal complexity	Programs exist & need minimal modification	
Total Technical Uncertainty Score						
Infrastructure Uncertainty	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 FORM

Page 1



Threat and Vulnerability Assessment Physical and Electronic Sites - Page 1

Prepared by Date

Location Type Company Residence Multi-Tenant Public Access

Address

Main Phone Facility Manager

Assets at facility Head count at Facility Primary Functions Performed

Power Grid Distribution Point

Telephone CO Location

Backup Power Yes No Length of Support Hrs

**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>

Category III - Medium Financial Impact Any Cat III in Facility Yes No

Category IV - Low Financial Impact Any Cat IV in Facility Yes No

Public Access <input type="radio"/> Yes <input type="radio"/> No	Security Badges <input type="radio"/> Yes <input type="radio"/> No
Reception Desk <input type="radio"/> Yes <input type="radio"/> No	Card Key <input type="radio"/> Yes <input type="radio"/> No
Guards <input type="radio"/> Yes <input type="radio"/> No	Fenced <input type="radio"/> Yes <input type="radio"/> No
Armed <input type="radio"/> Yes <input type="radio"/> No	Guard Gate <input type="radio"/> Yes <input type="radio"/> No
Guest Escorted <input type="radio"/> Yes <input type="radio"/> No	Gate Manned <input type="radio"/> Yes <input type="radio"/> No
Cameras <input type="radio"/> Yes <input type="radio"/> No	24/7 Security <input type="radio"/> Yes <input type="radio"/> No
RT Monitoring <input type="radio"/> Yes <input type="radio"/> No	After Hours Contact <input style="width: 100px;" type="text"/>

Threat and Vulnerability Assessment Physical and Electronic Sites

Risk Ranking

Impact of Loss	Vulnerability (Probability of Threat)				
	Will Occur over 90%	Extreme 90% < >75%	High 75% < >25%	Moderate 25% < >10%	Low Under 10%
Catastrophic					
Very High					
Noticeable to ENTERPRISE					
Minor					
None					

Impact of Loss	Risk Point Value				
	Will Occur over 90%	Extreme 90% < >75%	High 75% < >25%	Moderate 25% < >10%	Low Under 10%
Catastrophic	8	7	6	5	4
Very High	7	6	5	4	3
Noticeable to ENTERPRISE	6	5	4	3	2
Minor	5	4	3	2	1
None	4	3	2	1	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>

8	
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.
0	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>