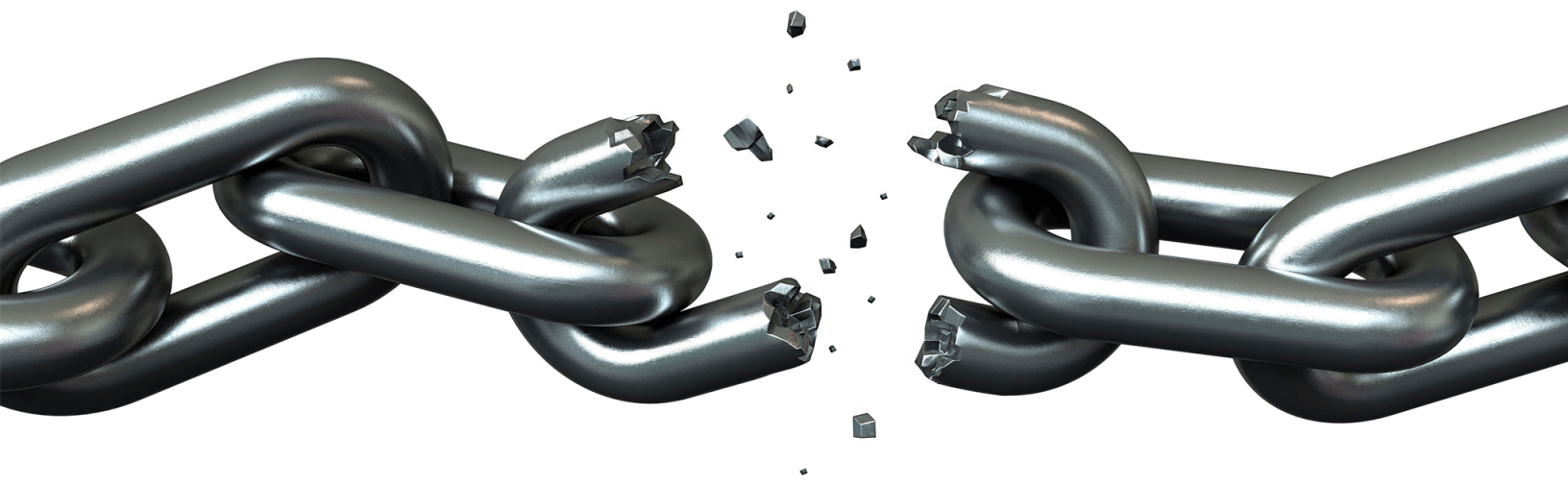
Threat and Vulnerability Assessment Tool

2024



Janco Associates, Inc.

TABLE OF CONTENTS

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 ongoing monitoring activities to re-assess risk and the effectiveness of controls
- Communicate periodic risk management process reports to management

To complete a compressive assessment there are six components in the planning and execution:

1. Define the scope of the process (Internal and external resource identification)
2. Data gathering via questionnaires, interviews, and analysis of existing data
3. Review of existing policies and procedures
4. Identification of potential threats
5. Analysis of
6. Review and ns

The risk managemen t by IT staff but rather as an essentia and Vulnerability Assessr arry out its mission in the face o

Successful threat and vulnerability assessments require the full support of senior management and are 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, account for new threats and vulnerabilities created by these changes, and determine the effectiveness of existing controls.

THREAT ANALYSIS

Threats are anything that could contribute to accessing, altering, tampering with processes, destruction of assets (both physical and digital), business interruptions, and reduction in the value of the reputation or assets of the enterprise:

Controllable Human	Non-Human
Ha Ma Ra Th Fir Ac Po Backup Staff IT Pros Support services staff Terminated/disgruntled employees	rnal) Electrical Air (Dust and contamination) Temperature control

Threats that are identified need to be evaluated with the operational enterprise environment and the effect the threat, if it occurs will have on the enterprise, its employees, and/or operations.

The presentation of findings is greatly enhanced when treats are quantified and graded in such a way that the probability and costs associated with each treatment are put in perspective. To that end, the table that follows is key to their process.

Janco Associates

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 are required for both staff & management	Some new skills for staff; none for management	No new skills for staff & management	
Hardware Dependencies	Ha... imm... emergi...				...e in similar ...plications	
Software Dependencies	No... softwar... ir...				...ard software; ...programming ...required	
Application Software	No package or solution exists. Complex design and development are required	Programs are available commercially, but highly complex. Complex design and development	Programs available commercially with extensive modifications OR Programs can be developed in-house with moderate complexity	Programs available commercially with 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						

SAMPLE GRAPHIC

Below is a sample graphic that can be generated with the attached Excel Spreadsheets.

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					
Minor					
None					

THREAT & VULNERABILITY ASSESSMENT WORK PLAN

RISK MANAGEMENT PROCESS

Overview

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:

-
-
-
- ss of controls
-

The risk n n carried out by IT staff but as an essential management function of the enterprise. The principal goal of the Information Technology Risk Management Program is to protect IT assets and the company's ability to carry out its mission in the face of potential threats to its IT assets

Purpose

The purpose of the IT Risk Management Program is to:

- Comply with the Board of Director's risk policy, as well as other state and federal regulations, to develop, implement, and maintain a security plan with appropriate and auditable controls;
- Provide a governance framework for understanding potential risks to IT assets based on the threat assessment plan;
- Provide guidelines for evaluating and documenting the management, operational, and technical environment of IT assets; and
- Provide management with direction, planning, and guidance in the area of information threat assessments.

APPENDIX

Attached as separate items are the following:

Forms

- Threat and Vulnerability Assessment Form
- Risk Assessment Matrix Form
- Risk Assessment Spreadsheet
- Threat and Vulnerability Excel Spreadsheet

Job Descriptions

- Chief Security Officer (CSO)
- Manager Compliance
- Manager Security and Workstations
- Manager SOX Compliance

WHAT'S NEW

2024

- Add Job Description for
  - Chief Security Officer
- Updated all the included forms, job descriptions, and spreadsheets

2023

- Add Job Descriptions for
  - Manager Compliance
  - Manager Security and Workstations
  - Manager SOX Compliance
- Updated all the included forms and spreadsheets

2022

- Added materials to the Work Plan that addresses issues with WFH, shutdowns, and pandemic
- Updated all the included forms and spreadsheets

2021

- Updated all the included forms and spreadsheets
- Updated to Ransomware implications

2020

- Updated all the included forms and spreadsheets
- Updated to consider CCPA and GDPR implications
- Reformatted tool per client suggestions