RISK ASSESSMENT ORIENTATION

ENTERPRISE RISK MANAGEMENT – PURPOSE

The purpose of an Enterprise-Wide Risk Assessment is to:

- Identify risks to the achievement of goals and objectives
- Measure the significance of each identified risk
- Determine the most appropriate business response to each risk
- Evaluate and report on how well the chosen responses are carried out

ENTERPRISE RISK MANAGEMENT – VALUE

- Anticipate risks earlier and more explicitly, opening more options for managing the risks
- Identify and pursue existing new opportunities
- Respond to deviations in performance more quickly and consistently
- Develop and report a more comprehensive and consistent portfolio of risk
- Improve collaboration, trust, and information-sharing

BENEFIT TO USF

ERM integrates with strategy and performance.

This allows USF to implement a focused, systematic approach to addressing risk and identifying opportunities involving our:

STRATEGIC PLAN

PERFORMANCE-BASED FUNDING

PREEMINENCE METRICS

U.S. NEWS AND WORLD REPORT RANKINGS

RISK COMMITTEE AREAS REPRESENTED

- Academic Affairs
- Administrative Services
- Advancement
- Athletics
- Business & Finance
- Information Technology
- University Police
- Human Resources
- General Counsel
- Communications and Marketing
- Research & Innovation
- Student Affairs & Student Success
- Government Relations
- USF Health
- USF Sarasota-Manatee Campus
- USF St. Petersburg Campus
- USF Executive Services
- Internal Audit
- Compliance & Ethics

ERM PROCESS

IDENTIFY AND ASSESS RISKS
REPORT RISKS
MITIGATE AND TREAT RISKS

RISK TYPES

Compliance Risks	Risks impacting compliance with legal, regulatory, contractual, policy, accreditation, NCAA, and other requirements
Financial Risks	Risks impacting resources, financial structure, ability to meet future financial needs, and financial reporting
Operational Risks	Risks impacting continuity of activities, safety and security, IT operations, physical infrastructure, process efficiency, and program effectiveness
Reputational Risks	Risks impacting our public image, brand, external opinions, prominence, and standing of our University
Strategic Risks	Risks impacting our constituent relationships, ability to generate funds, and goal achievement

Based on the ACUA (Association of College and University Auditors) Risk Dictionary

COMPLIANCE RISKS

Risks impacting compliance with legal, regulatory, contractual, policy, accreditation, NCAA, and other requirements

Compliance with Laws and Regulations Risk	Risks associated with violating laws and regulations which may result adverse consequences *e.g., Non-compliance with the law, receiving fines, penalties, and litigation*
Conflict of Interest Risk	Risks associated with unresolved conflicts between an employee's private interests and the public interests of our institution *e.g., Nepotism, unequal compensation, hiring an unqualified relative, etc.*
Data Privacy Risk	Risks associated with inadequately protecting data controlled or owned by our institution in accordance with the law and best practices *e.g., sharing patient or student data in a manner which violates federal law, such as HIPAA or FERPA, respectively*

FINANCIAL RISKS

Risks impacting resources, financial structure, ability to meet future financial needs, and financial reporting

Billing Accuracy Risk	Risks associated with inaccurate billing or failing to bill for services rendered by our institution *e.g., Tuition or Medicare/Medicaid Clinical Care billing and student receivables*
Financial Reporting Risk	Risks associated with incomplete, inaccurate, or untimely communication of financial information *e.g., Production and distribution of financial reports, failing to adhere to Governmental Accounting Standards Board (GASB)*
Fraud, Theft, and Embezzlement Risk	Risks associated with financial losses stemming from students, employees, vendors, or other third parties, doing business with our institution, engaging in fraud, theft, or embezzlement *e.g., Falsifying credentials, violating time and effort reporting requirements, stealing (misappropriating) assets, or fabricating/falsifying records*

OPERATIONAL RISKS

Risks impacting continuity of activities, safety and security, IT operations, physical infrastructure, process efficiency, and program effectiveness

Purchasing Risk	Risks associated with the procurement processes for obtaining services, products, or resources *e.g., Needs analysis, vendor selection, supplier diversity, supply chain management, contract management*
Logical Access, Cybersecurity, and Vulnerability Management Risk	Risks associated failing to protect the confidentiality, integrity, and availability of IT assets of our institution from potential threats *e.g., Outside party stealing a user's credentials in order to access the university's systems and perform malicious activities, downloading software that compromises a device making it vulnerable*
Personnel Issues or Workplace Violence Risk	Risks associated with personnel issues or workplace violence *e.g., Favoritism, conflicts, harassment, bullying, nepotism, threats of physical violence or concomitance of violence against fellow workers, etc.*

REPUTATIONAL RISKS

Risks impacting our public image, brand, external opinions, prominence, and standing of our University

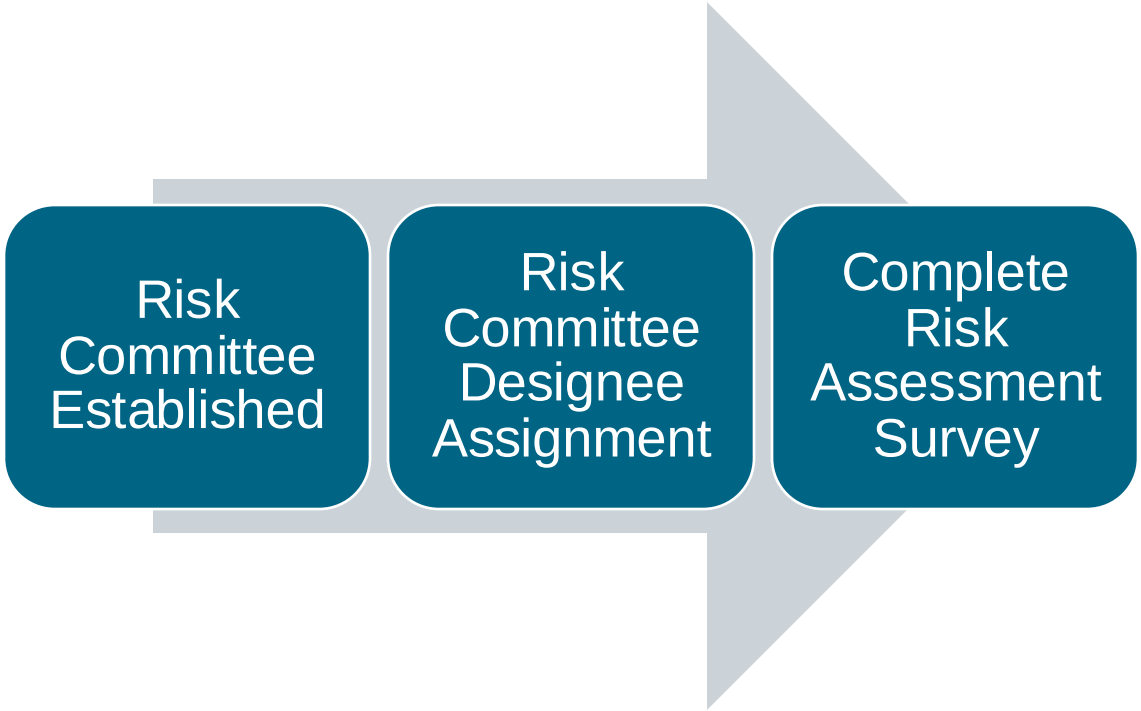
Communication Risk	Risks associated with ensuring that a consistent message is shared and understood among all constituents and there is clear and consistent coordination as needed
Emerging Issues Risk	Risks associated with potential issues in their earliest stages of development *e.g., Foreign influence in research, international travel bans, pandemics, hurricanes, etc.*
Public Image Risk	Risks associated with threats to or endangerment of the institution's good name or standing which can arise from the actions of our institution, employees, or third-parties (vendors, affiliates, and guests)

STRATEGIC RISKS

Risks impacting our constituent relationships, ability to generate funds, and goal achievement

Governance Risk	Risks associated with ineffective processes and structures to identify, assess, manage, and communicate risks to the achievement of the organization's objectives *e.g., Ineffective governance structure fails to ensure committees at both the Board and Senior Management levels have been created with formalized mandates, authority, and representation to proactively identify and respond to organizational risks*
New Programs and Delivery Models Risk	Risks associated with an inability to meet community needs by effectively adapting to new academic and service offerings or programs, including program content and how they are delivered *e.g., Remote education delivery, hybrid learning models, changes to clinical models*
Variability in Customer Volume and Funding Availability Risk	Risks associated with significant changes that may lead to insufficient revenue and/or funding that challenges underlying assumptions of strategic forecasts or may cause a material variance from the forecasts *e.g., Customers include students, patients, and other relevant stakeholders that provide revenues to the institution. Funding availability risk pertains to funding from federal, state, and local entities as well as private companies*

IDENTIFY AND ASSESS RISK



ERM SURVEY TOOL

ERM SURVEY TOOL

- You will be sent a link to complete the Qualtrics survey with password to access
- Can be completed on mobile device, tablet, or computer
- Printable Survey
- Risk Dictionary
- ERM Webpage

PRINTABLE SURVEY

Compliance Risks: *Risks impacting compliance with legal, regulatory, contractual, policy, accreditation, NCAA, and other requirements.*

Type of Risk	Does it apply? Yes or no?	Please describe how it does or does not apply to your risk area.	Impact Rating	Velocity Rating	Likelihood Rating	Preparedness Rating
Breach of Contract Risk: Risks associated with failure to meet contractual requirements leading to adverse consequences.	**Yes**	**This applies to…**	**Moderate**	**Moderate**	**Major**	**Somewhat Prepared**
Compliance with Laws and Regulations Risk: Risks associated with violating laws and regulations which may result adverse consequences.	Choose an item.	Click or tap here to enter text.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
Conflict of Commitment Risk: Risks associated with activities interfering with an employee's full and faithful performance of their professional or institutional responsibilities or obligations which are not mitigated.	Choose an item.	Click or tap here to enter text.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
Conflicts of Interest Risk: Risks associated with unresolved conflicts between an employee's private interests and the public interests of our institution.	Choose an item.	Click or tap here to enter text.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
Data Privacy Risk: Risks associated with inadequately protecting data controlled or owned by our institution in accordance with the law and best practices.	Choose an item.	Click or tap here to enter text.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
Employment Practices Risk: Risks associated with violating employment law and human resources standards.	Choose an item.	Click or tap here to enter text.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
Research Contract and Grant Violations Risk: Risks associated with violating grant-related requirements and research funding agreements.	Choose an item.	Click or tap here to enter text.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
Other:	Choose an item.	Click or tap here to enter text.	Choose an item.	Choose an item.	Choose an item.	Choose an item.

RISK DICTIONARY

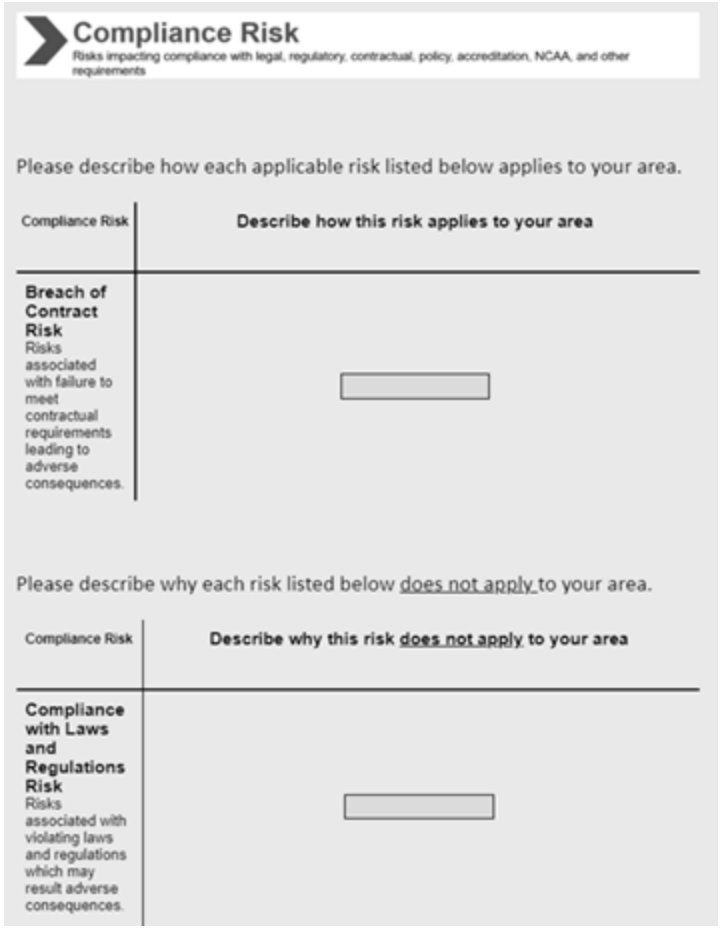
Level 1 Risk	Level 2 Risks	Description	Examples
Compliance Risk	Breach of Contract Risk	Risks associated with failure to meet contractual requirements leading to adverse consequences.	
Compliance Risk	Compliance with Laws and Regulations Risk	Risks associated with violating laws and regulations which may result adverse consequences.	Examples include, but are not limited to, non-compliance with the law as well as receiving fines, penalties, and litigation.
Compliance Risk	Conflict of Commitment Risk	Risks associated with activities interfering with an employee's full and faithful performance of their professional or institutional responsibilities or obligations which are not mitigated.	Examples include, but are not limited to, employees working so many hours at their second job that they cannot fully and faithfully perform the job they were hired to do for our institution. Similarly, employees working for our direct competitors, thereby undermining our position in the marketplace.
Compliance Risk	Conflicts of Interest Risk	Risks associated with unresolved conflicts between an employee's private interests and the public interests of our institution.	Examples include, but are not limited to, nepotism, unequal compensation, hiring an unqualified relative, accepting payment from another company for information about your employer, or employees hiring a student or employee for their private company when they supervise the student or employee as part of their employment with our institution.
Compliance Risk	Data Privacy Risk	Risks associated with inadequately protecting data controlled or owned by our institution in accordance with the law and best practices.	Examples include, but are not limited to, failing to exercise due diligence and oversight when disclosing data to third parties or sharing patient or student data in a manner which violates federal law, such as HIPAA or FERPA, respectively.
Compliance Risk	Employment Practices Risk	Risks associated with violating employment law and human resources standards.	Examples include, but are not limited to, litigation stemming from unlawfully hiring, promoting, disciplining, or terminating employees; or discriminating against or sexually harassing employees.
Compliance Risk	Research Contract and Grant Violations Risk	Risks associated with violating grant-related requirements and research funding agreements.	

STEP 1: IDENTIFICATION OF RISKS

Check all applicable risks or type in your own

STEP 2: APPLICABILITY

Then, for each type of risk (whether checked or unchecked), you will be asked to describe how each risk applies to your area and why the other risks do not apply to your area.



Compliance Risk

Risks impacting compliance with legal, regulatory, contractual, policy, accreditation, NCAA, and other requirements

Please describe how each applicable risk listed below applies to your area.

Compliance Risk	Describe how this risk applies to your area
Breach of Contract Risk Risks associated with failure to meet contractual requirements leading to adverse consequences.	

Please describe why each risk listed below does not apply to your area.

Compliance Risk	Describe why this risk does not apply to your area
Compliance with Laws and Regulations Risk Risks associated with violating laws and regulations which may result adverse consequences.	

STEP 3: SCORING

You will only score the risks that you identified as applicable to your area.

Impact

- Scale to rate the potential consequences of risks impacting various areas within the organization. ***There is a custom impact scale for each of the five risk types.***

Velocity

- Scale to rate how quickly a risk can impact our organization

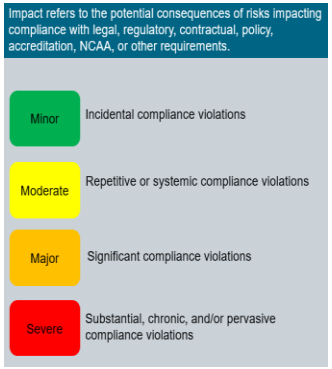
Likelihood

- The probability a risk may occur given the effectiveness of your existing controls, as known to you.

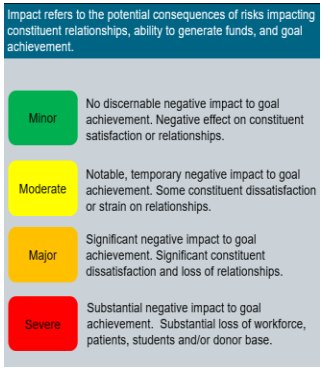
Preparedness

- The University's readiness to address a risk based on the existence and effectiveness of prevention/detection controls.

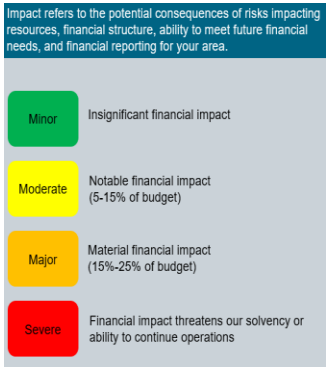
CUSTOMIZED IMPACT SCORING FOR EACH RISK TYPE



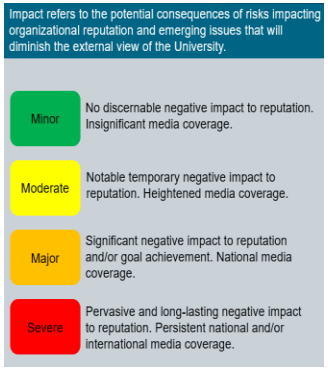
Compliance



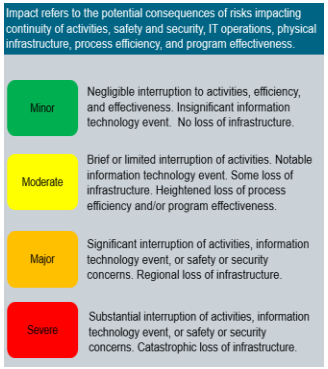
Financial



Operational

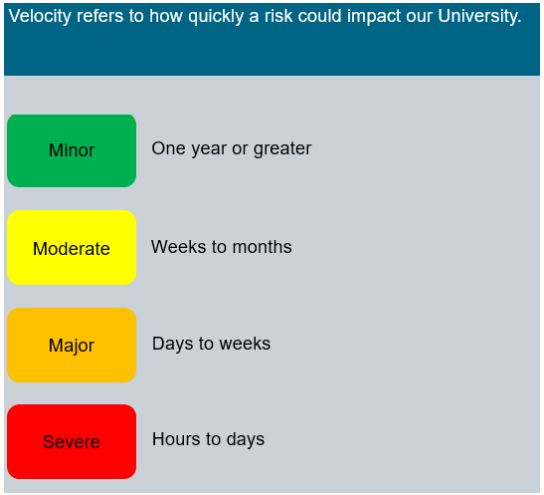


Reputational

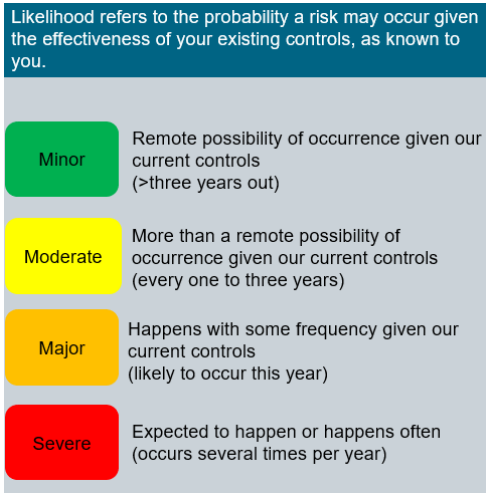


Strategic

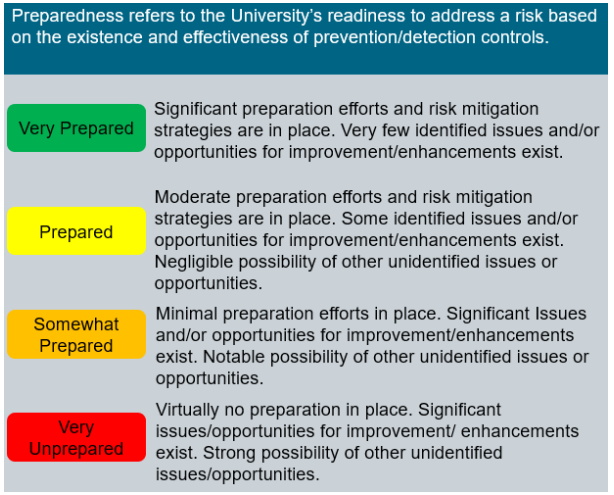
SCORING APPLICABLE FOR EACH RISK TYPE



Velocity

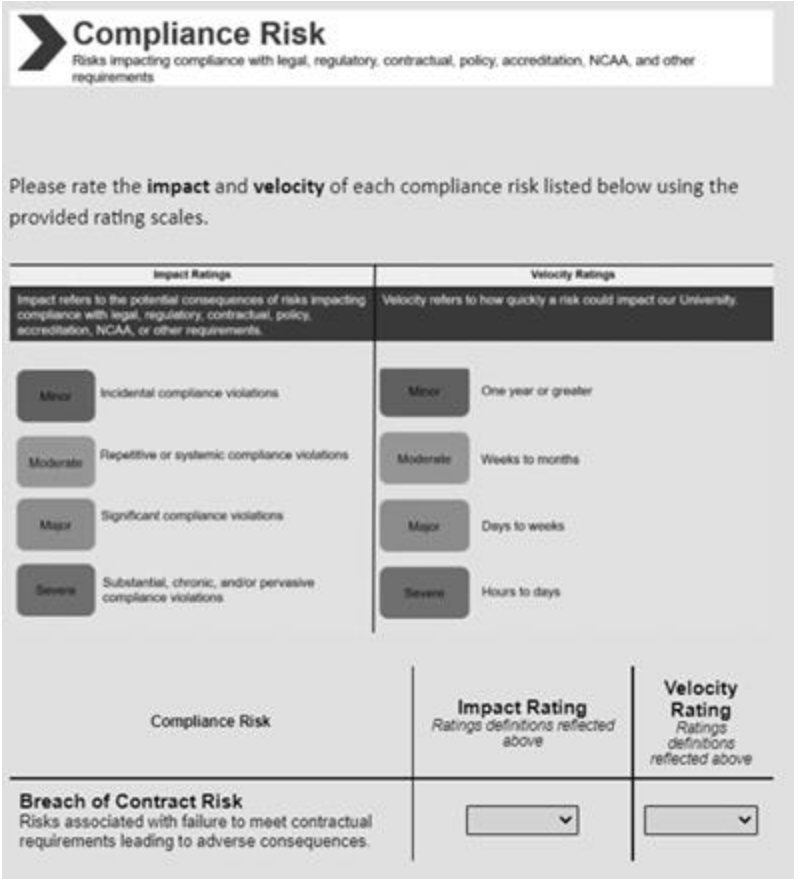


Likelihood



Preparedness

EXAMPLE FROM ONLINE SURVEY



Compliance Risk

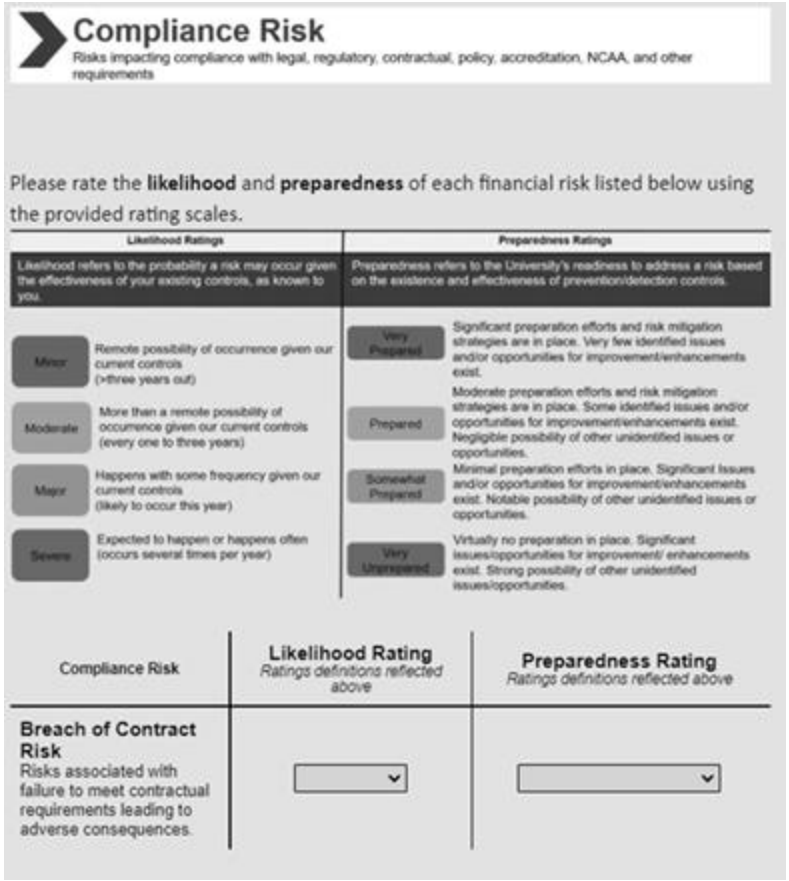
Risks impacting compliance with legal, regulatory, contractual, policy, accreditation, NCAA, and other requirements

Please rate the **impact** and **velocity** of each compliance risk listed below using the provided rating scales.

Impact Ratings	Velocity Ratings
Impact refers to the potential consequences of risks impacting compliance with legal, regulatory, contractual, policy, accreditation, NCAA, or other requirements.	Velocity refers to how quickly a risk could impact our University.
Minor — Incidental compliance violations	Minor — One year or greater
Moderate — Repetitive or systemic compliance violations	Moderate — Weeks to months
Major — Significant compliance violations	Major — Days to weeks
Severe — Substantial, chronic, and/or pervasive compliance violations	Severe — Hours to days

Compliance Risk	Impact Rating *Ratings definitions reflected above*	Velocity Rating *Ratings definitions reflected above*
Breach of Contract Risk Risks associated with failure to meet contractual requirements leading to adverse consequences.		

EXAMPLE FROM ONLINE SURVEY



Compliance Risk

Risks impacting compliance with legal, regulatory, contractual, policy, accreditation, NCAA, and other requirements

Please rate the **likelihood** and **preparedness** of each financial risk listed below using the provided rating scales.

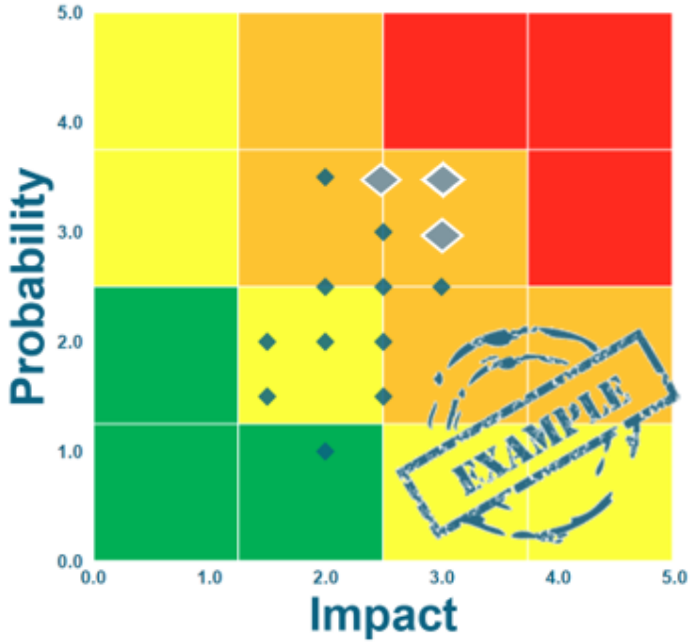
Likelihood Ratings	
Likelihood refers to the probability a risk may occur given the effectiveness of your existing controls, as known to you.	
Minor	Remote possibility of occurrence given our current controls (>three years out)
Moderate	More than a remote possibility of occurrence given our current controls (every one to three years)
Major	Happens with some frequency given our current controls (likely to occur this year)
Severe	Expected to happen or happens often (occurs several times per year)

Preparedness Ratings	
Preparedness refers to the University's readiness to address a risk based on the existence and effectiveness of prevention/detection controls.	
Very Prepared	Significant preparation efforts and risk mitigation strategies are in place. Very few identified issues and/or opportunities for improvement/enhancements exist.
Prepared	Moderate preparation efforts and risk mitigation strategies are in place. Some identified issues and/or opportunities for improvement/enhancements exist. Negligible possibility of other unidentified issues or opportunities.
Somewhat Prepared	Minimal preparation efforts in place. Significant issues and/or opportunities for improvement/enhancements exist. Notable possibility of other unidentified issues or opportunities.
Very Unprepared	Virtually no preparation in place. Significant issues/opportunities for improvement/ enhancements exist. Strong possibility of other unidentified issues/opportunities.

Compliance Risk	**Likelihood Rating** *Ratings definitions reflected above*	**Preparedness Rating** *Ratings definitions reflected above*
Breach of Contract Risk Risks associated with failure to meet contractual requirements leading to adverse consequences.		

IDENTIFY AND ASSESS RISK

RISK FOOTPRINT DISTRIBUTED



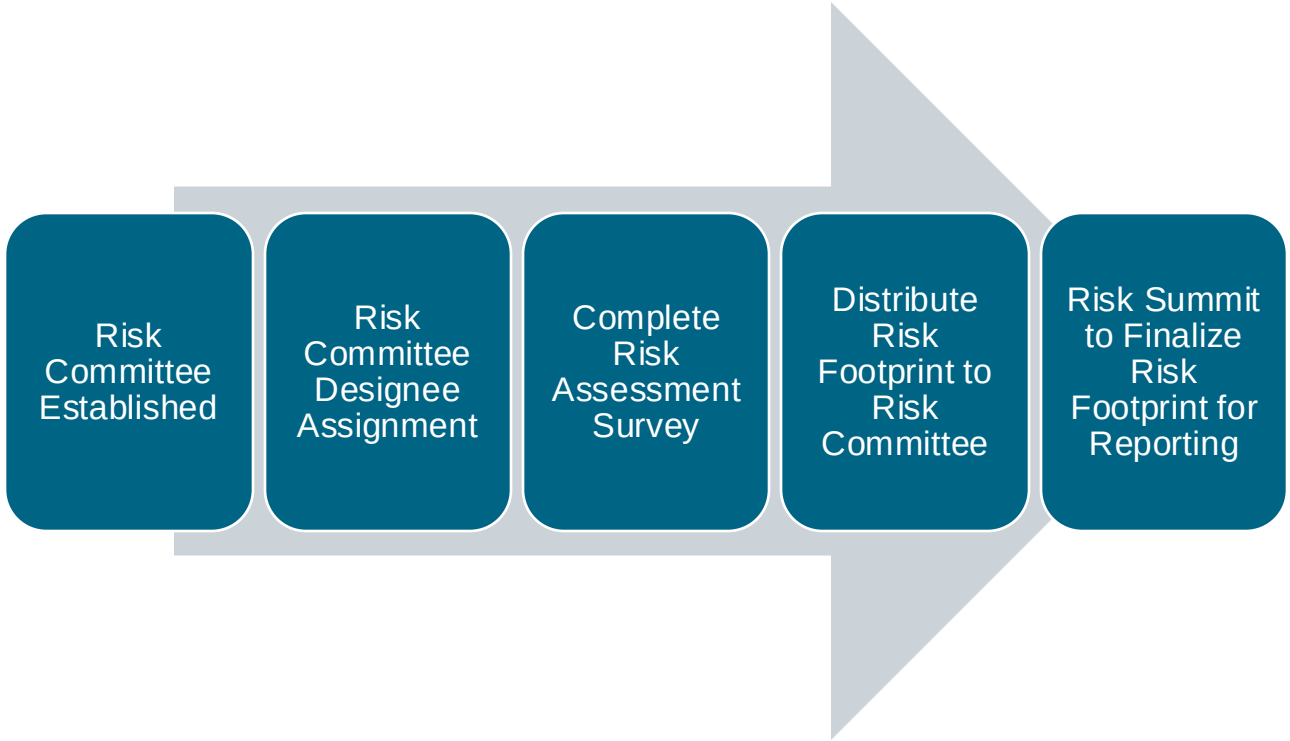
Blue dots represent the identified risks.

Impact (*x-axis*) calculated as average of Impact and Preparedness ratings.

Probability (*y-axis*) calculated as average of likelihood and velocity ratings.

Note: If there are multiple survey entries identifying the same risk, then plotted point is the averaged data.

IDENTIFY AND ASSESS RISK



ERM PROCESS

IDENTIFY AND ASSESS RISKS
REPORT RISKS
MITIGATE AND TREAT RISKS