RIT

Enterprise Risk Management

Risk Assessment and Response Guide

Contents

Overview 3

I. Establish and Understand the Context 5

II. Risk Identification and Description 7

III. Risk Analysis and Prioritization 9

IV. Risk Response 11

V. Report Findings and Response 13

VI. Monitor Risk Plans 13

Appendix A - Key Terms and Definitions 14

Appendix B - Potential Risk Areas for Higher Education 17

Appendix C – Risk Assessment Categories and Impact and Likelihood Scales 20

Table 1: Risk Categories 20

Table 2: Risk Measurement Scale: Impact 21

Table 3: Risk Measurement Scale: Likelihood 22

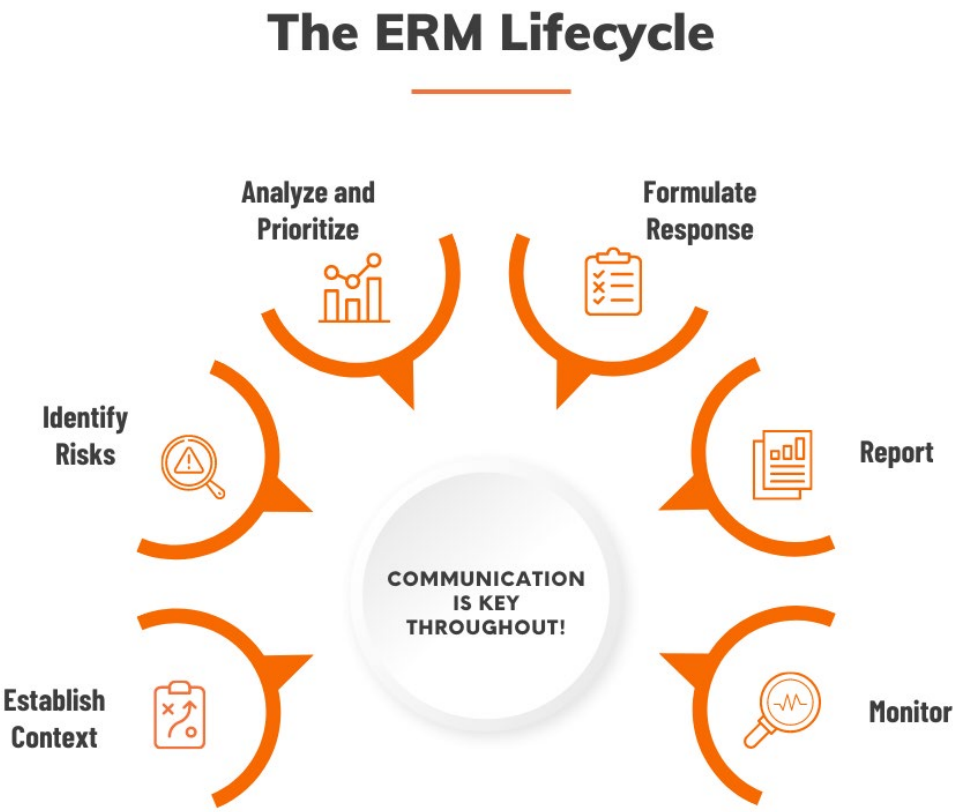
Table 4: Risk Prioritization Matrix 23

Overview

University Risk Philosophy

The University takes a broad view of “risk” as any event that could affect the University’s competitive position or ability to achieve its mission, vision, and strategic objectives. The University acknowledges that risk is present in virtually all its endeavors, and that successful risk-taking will often be necessary to achieve its goals. RIT does not seek to eliminate *all* risk; rather it seeks to be risk-aware and to effectively manage the uncertainty inherent in its environment. RIT seeks to identify, understand, assess, and respond to the risks facing the university, taking into account their impact on the RIT community and RIT’s standing, reputation, financial position, and performance.

Enterprise Risk Management (ERM) is a structured business process designed to identify, evaluate, and respond to risks that could affect the university’s ability to achieve its strategic goals and objectives. ERM is proactive in nature and designed to assist organizations in identifying potential risks before the risks become an active issues. An active ERM Program protects organizations like RIT from the potentially costly and negative legal, operational, and strategic impact of risks left unaddressed.



Step 1 Establish and Understand the Context

- Understand organizational objectives and both external and internal environmental factors
- Define scope of risk assessment

Step 2 Risk Identification & Description

- Find, recognize, and describe risks
- Assign an owner to each risk

Step 3 Risk Analysis & Prioritization

- Score risks by analyzing the impact and likelihood of occurrence for each risk
- Evaluate and prioritize immediacy of the risks

Step 4 Formulate Risk Response

- Develop a Risk Response Plan to address the risk, consulting with subject matter experts, as necessary

Step 5 Report Findings & Response

- Inform and discuss risks and risk management with appropriate stakeholders, including Board of Trustees (BOT)

Step 6 Monitor Risk Plans

- Routinely check the status of each risk and revise response plans as needed

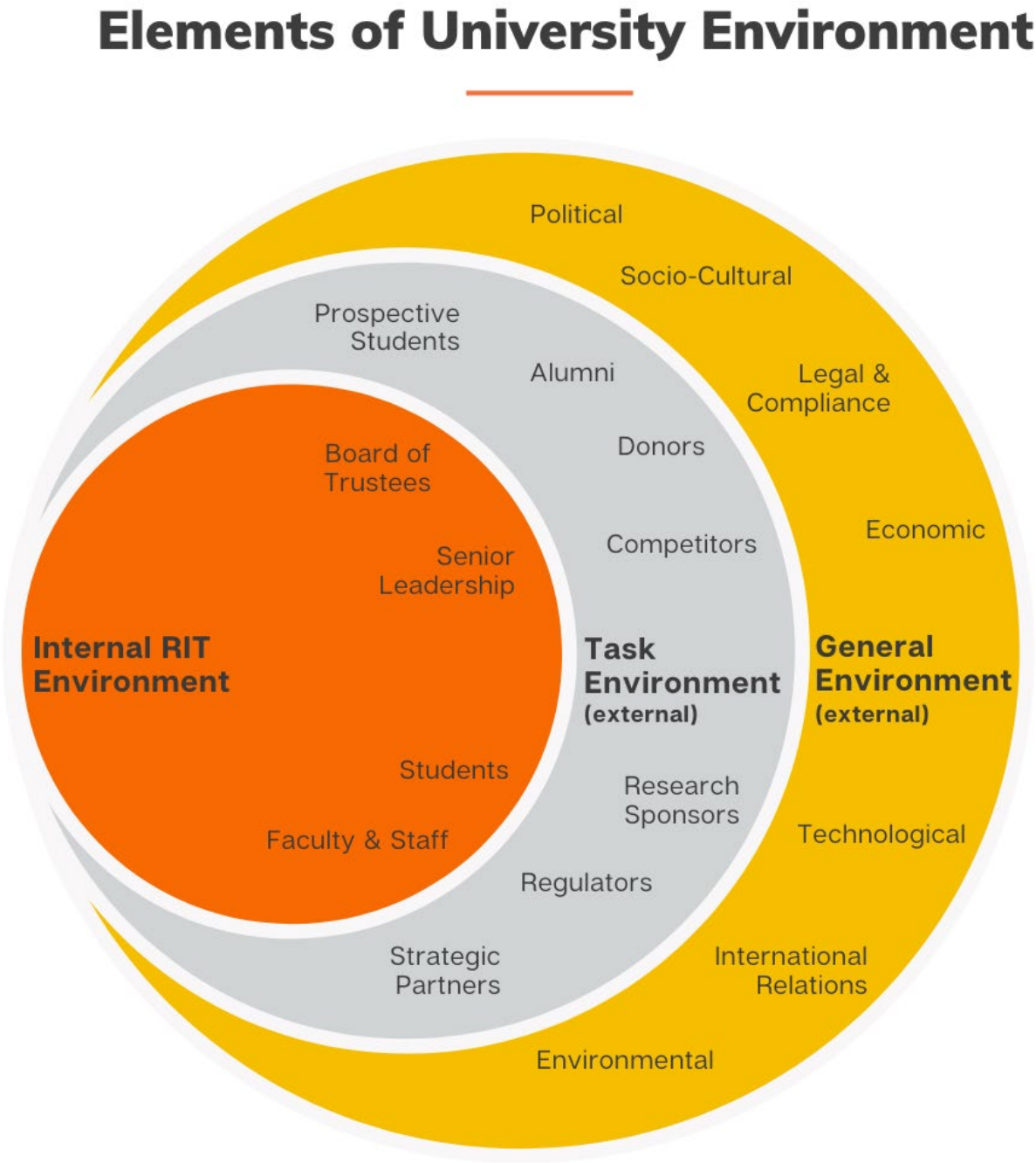
In addition to the ERM Program, this Risk Assessment and Response Guide can be utilized for interim Risk Assessments conducted within your area, college, or department. Risk Assessments should be conducted whenever there is a change in the University environment for your area with the potential to impact RIT's strategic goals, objectives, and mission.

The Office of Compliance and Ethics (OCE) is a resource for all stakeholders in the ERM process. We are available to answer questions, facilitate risk assessment workshops, and conduct other educational/training sessions. Please reach out to complianceandethics@rit.edu for assistance.

Additional guidance is also available on the OCE Enterprise Risk Management website.

I. Establish and Understand the Context

The purpose of establishing context for Risk Assessment is to set the stage for risk identification. Identifying and understanding the external and internal factors that could impact RIT's ability to achieve its mission, vision, goals, and objectives, is a prerequisite to recognizing risks. Context also helps us understand where risk comes from and its potential impact.



A. Considerations: Internal Factors

- ☑ What are RIT's strategic plans, goals, and objectives?
- ☑ What is the message from leadership about achieving plans, goals, and objectives? Are roles and accountability clearly defined?
- ☑ What are the strategic goals of your college, school, division, department, or business unit?
- ☑ What major initiatives is your area currently engaged in or planning?
- ☑ Since the previous risk assessment survey, have there been changes to processes, people, programs, or technology in your area or in RIT leadership?
- ☑ What current activities, functions, or services does your area provide to others at RIT, and which are critical to continuity of business?
- ☑ What are the current strengths, weaknesses, opportunities, and threats for RIT and your area?

B. Considerations: External Factors

- ☑ What are the current and potential future legal and regulatory requirements impacting your area? Are major regulatory changes coming?
- ☑ What are external stakeholder perceptions and expectations of RIT? Consider recent feedback from alumni, donors, third-party business partners, the local community, and others. How do external stakeholders view RIT?
- ☑ What are the political, economic, social/cultural, technological, or environmental factors currently impacting RIT and your area?

C. Context Summary

Context helps us understand where our risks come from and the potential impact of each risk on RIT's strategic goals and objectives. Before starting your risk assessment, consider the internal and external factors that establish the context of the risk. Document your responses so you can refer back to them as you continue with the risk assessment.

II. Risk Identification and Description

Once you've established the context, the next step is to identify all of the actual and potential risks to RIT, draft a clear and concise risk statement, and then assign a primary risk owner to each risk.

A. Identify Risks

The purpose of risk identification is to generate a list of key risks based on events that might create, enhance, prevent, degrade, accelerate, or delay the achievement of RIT's strategic objectives. When identifying risks within the scope of the established context:

- ☑ Engage a diverse team of individuals in your area for the discussion.
- ☑ Review common risk areas for universities and identify all potential and applicable risks that are both within and outside of your control. *See,* Appendix B for Potential Risk Areas for Higher Education.
- ☑ Determine whether the risk is primarily financial, operational, strategic, reputational, or compliance/legal. *See,* Appendix C for Risk Categories and their definitions.
- ☑ Consider related risks and cascading or cumulative impact. For example, if the risk identified is declining student enrollment due to international politics and a negative perception of higher education in the United States consider how the risk will impact areas outside of enrollment management.

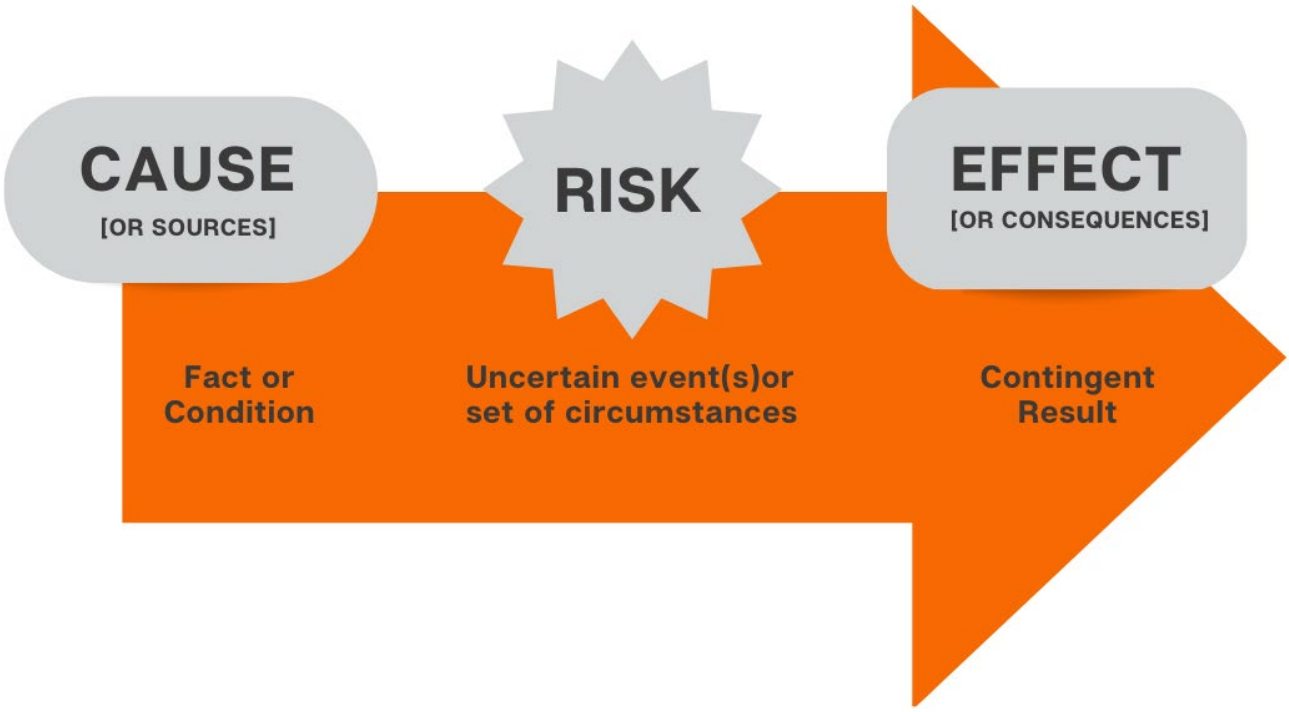
Note that risk is about the effect of uncertainty and therefore concerns the future. Risks are distinct from existing issues, problems or business conditions, where the likelihood of occurrence is not an issue.

B. Write Risk Statement(s)

Once you have identified each of the key risks, you will need to draft a Risk Statement for each risk identified.

A clear, concise, well-defined Risk Statement:

- ☑ Raises awareness and educates staff and faculty on important strategic priorities
- ☑ Facilitates understanding of potential events and impact on strategic priorities
- ☑ Provides context for related action plans and activities
- ☑ Allows RIT to better utilize risk information to support decision making at all levels
- ☑ Uses plain, simple language that can be understood at all levels across the university



An effective Risk Statement answers:

- ☑ What could happen? (the risk, event, or uncertain circumstances)
- ☑ Why could it happen? (the source or cause)
- ☑ Why should RIT care? (the effect or consequences)

Below are three examples of effective "SOURCE" "RISK" and "EFFECT" risk statements:

1. The current hardware is not fast enough to support testing so [SOURCE] we may not be able to test performance until we start production [RISK], which may delay hiring new employees" [EFFECT].

2. The team does not have a design for the gateway software so [SOURCE] the architecture may not work [RISK], which may result in increased costs [EFFECT].

3. Failure to track the work conducted on a grant [SOURCE] may result in inaccurate effort reporting [RISK], subjecting the university to substantial financial and reputational damage [EFFECT].

C. Identify and Assign Responsible Official/Risk Owner

Each risk identified should have a primary Responsible Official or Risk Owner (RO). The RO is the individual at RIT with accountability and authority to manage the risk. An RO is usually a Vice President, Dean, and is ultimately responsible for ensuring the risk is addressed appropriately and effectively.

In addition to RO(s), one or more Responsible Persons (RP) may be documented for each risk. An RP is generally an Associate Vice President, a Director, Department Chair, and/or Manager with oversight and authority to manage the day-to-day actions associated with the identified risk.

III. Risk Analysis and Prioritization

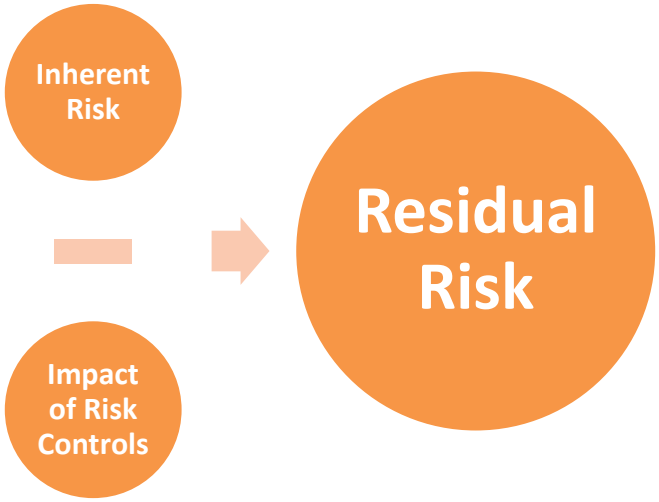
The purpose of a Risk Analysis is to develop an understanding of the risk in order to inform your decisions and determine the appropriate response.

During this stage of the process, you will assess the potential Impact and Likelihood of each identified risk, as well as the immediacy of each risk, so you can prioritize any required responses.

A. Understand Inherent Risk vs. Residual Risk

Inherent Risk is the innate level of risk of an event on strategic objectives if there are no controls in place and not actions are taken to alter the risk's impact and/or likelihood.

Residual Risk is the level of risk that remains after the development and implementation of the controls and activities by the organization to reduce the risk's impact and/or likelihood.



B. Perform Risk Analysis

When performing a Risk Analysis, consider all potential negative consequences for RIT, including whether the risk identified is interdependent with other risks or has a cascading or cumulative consequences for other areas or risks.

1. Determine Inherent Risk

- ☑ Identify the Risk Category for each identified risk
- ☑ Consider the inherent risk and worst-case Impact of each risk
- ☑ Consider the inherent Likelihood of each risk occurring
- ☑ Multiply the scores for Impact and Likelihood to produce the initial, Inherent Risk Score for each risk

2. Determine Residual Risk

- ☑ Consider efficacy of current controls and treatment strategies used to reduce or modify the worst-case Impact of each risk
- ☑ Consider efficacy of current controls and treatment strategies used to reduce or modify the Likelihood of each risk occurring
- ☑ Multiply the scores for Impact and Likelihood to produce the Residual Risk Score for each risk

3. Prioritize Risks

- ☑ If performing a Risk Assessment within the scope of ERM, Residual Risk Scores of 12 or higher will be elevated to the University Risk and Compliance Committee (URCC).

- ☑ If performing a Risk Assessment outside the scope of ERM, review the Residual Risk Score for each risk assessed in your area to determine the urgency of addressing the risk. *See,* Table 4. Risk Prioritization Matrix.

IV. Risk Response

Each risk identified and analyzed requires a formulated Risk Response Plan, based on the calculated Risk Score (Impact x Likelihood) and priority of the risk. The RO and RP(s) are responsible for ensuring the Risk Response is formulated, documented, implemented, and monitored.

When formulating a Risk Response, your goal is to determine the most appropriate response for the individual risk.

There are four standard Risk Responses:

- Accept
- Avoid
- Mitigate
- Transfer (or Share)

Standard Risk Responses are not mutually exclusive. An effective Risk Response Plan may require a combination of the standard Risk Responses. Moreover, responses may change overtime based on implemented plans, remaining risks. Finally, accepting the risk and maintaining existing controls without altering the current Risk Response Plan is a Risk Response.

For definitions of each standard Risk Response, *see* Appendix A. Key Terms and Definitions.

A. Considerations: Risk Response

- ☑ The priority of the risk in comparison to other risks in your area

- ☑ Additional costs and resources required to implement a specific risk response, and whether the response is economically feasible

- ☑ Controls and methods that may require change under the response

- ☑ The timeframe required to implement and maintain the response

- ☑ New, unforeseen risks or the impact on other areas based on the risk response

B. Drafting a Risk Response Plan

RIT's ERM Program requires risks and resulting response plans to be documented, revised, and periodically shared with OCE. This is also a recommended best practice for Risk Assessments performed outside the scope of ERM.

When drafting a Risk Response Plan, include the following elements:

- ☑ Risk Category
- ☑ Identified Risk/Issue
- ☑ Risk Statement/Description
- ☑ Residual Risk Impact Score
- ☑ Residual Risk Likelihood Score
- ☑ Residual Risk Score/Risk Ranking (Impact x Likelihood)
- ☑ Responsible Official/Owner (RO)
- ☑ Responsible Person(s) (RP)
- ☑ Risk Response Plan Strategy/Strategies
- ☑ Description of Strategy/Strategies in Place

For definitions of the above terms, *see* Appendix A. Key Terms and Definitions.

OCE is available to assist with drafting Risk Response Plans. Reach out to complianceandethics@rit.edu for assistance, and visit the OCE Enterprise Risk Management website for additional guidance.

V. Report Findings and Response

Throughout the Risk Assessment process, it is critical to keep key stakeholder informed of findings, Risk Response Plans, and progress addressing and reducing risks identified.

During the ERM process, findings will be reported to OCE, which will share identified risks and documented Risk Response Plans and progress with the Board of Trustees (the Board).

Whether working through the annual ERM process or conducting Risk Assessments within your area:

- ☑ Work closely with subject matter experts in impacted areas throughout the process
- ☑ Keep appropriate stakeholders informed of top risks, response plans, and progress towards reducing risk for RIT
    - Key stakeholders include senior leadership in impacted areas, OCE, and the Board
- ☑ Reach out to OCE with questions or for assistance

VI. Monitor Risk Plans

Risk Response is a cyclical process, requiring continuous reassessment, determination of residual risk, adjustment of response plans, and reassessment.

The RIT ERM process is linear and occurs on an annual basis, with a comprehensive assessment conducted once every three years.

However, when monitoring Risk Response Plans, keep in mind:

- ☑ Existing risks should be monitored for change and may require reassessment and revision of the risk response and mitigation plan
- ☑ New risks impacting RIT may emerge at any time and require identification, assessment, response, and monitoring by the Board, President, Senior Leaders, ROs, RPs, and applicable functional managers throughout the University
- ☑ All Risk Response Plans and the effectiveness of implemented controls and activities intended to reduce risk should be reviewed, revised, and shared with key stakeholders at least quarterly

OCE is available to offer assistance to stakeholders in an effort to continuously reduce RIT's risks.

Appendix A - Key Terms and Definitions

Acceptance/Accept: Form of risk response, an informed decision to tolerate or take on a particular risk. Take no additional active measures.

Avoidance/Avoid: Form of risk response, an informed decision not to be involved in, or to withdraw from, an activity, in order not to be exposed to a particular risk. Eliminates uncertainty.

Communication: Continual and iterative processes that an organization conducts to provide, share, or obtain information, and to engage in dialogue with stakeholders regarding the management of risk.

Context, External: External environment in which the organization seeks to achieve its objectives, including but not limited to cultural, social, political, legal, regulatory, financial, technological, economic, natural, and competitive environments, whether international, national, regional, or local.

Context, Internal: Internal environment in which the organization seeks to achieve its objectives, which can include governance, organizational structure, policies, resource and knowledge capabilities, information systems, decision-making processes, culture, form and extent of contractual relationships, and relationships with, perceptions, and values of internal stakeholders.

Enterprise Risk Management (ERM): A structured business process designed to identify, evaluate, and respond to risk that could affect the university's ability to achieve its strategic goals and objectives.

ERM Framework: Set of components that provide the foundation and organizational arrangement for designing, implementing, monitoring, reviewing, and continually improving risk management throughout the organization at all levels. Ensures that info about risk derived from the risk management process is adequately reported and used as basis for decision-making and accountability at all relevant organizational levels.

ERM Goals or Objectives: Goals and objectives that ERM activities are seeking to achieve.

Event: Occurrence or change of a particular set of circumstances. Can be one or more occurrences, can have several causes, and can consist of something not happening.

Impact (Consequences): Outcome of an event negatively affecting objectives. Can be certain or uncertain; can be expressed qualitatively or quantitatively. An event can lead to a range of consequences, and initial consequences can escalate through knock-on effects.

Inherent Risk: An issue or event that prevents an organization from meeting its objectives in the absence of any action to control or modify the event.

Likelihood: The chance that something will happen – whether defined, measured, or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically.

Mitigation/Mitigate: Form of risk response involving actions designed to reduce either the impact or likelihood, or both, of a risk and its consequences.

Monitoring: Continual checking, supervising, critically observing, or determining the status in order to identify change from the performance level required or expected.

Probability: Measure of the chance of occurrence expressed as a number between 0 and 5.

Reporting: Form of communication intended to inform particular internal and external stakeholders by providing information regarding the current state of risk and its management.

Residual Risk: The risk that remains after an organization implements procedures or other efforts to mitigate or eliminate risks associated with a business process or risk identified.

Responsible Official (Risk Owner): Person or entity with the accountability and authority to manage a risk.

Responsible Person: Person or entity with oversight and authority to manage the day-to-day actions associated with the identified risk.

Risk (Issue): Any issue that may impact an organization's ability to achieve its objectives; the effect of uncertainty on organizational objectives. Often characterized in reference to potential events, impact, and the likelihood thereof. (*See also* ***Inherent Risk*** and ***Residual Risk***)

Risk Analysis: Process to comprehend the nature of risk and to determine the level of a risk; provides the basis for risk evaluation and decisions about risk response.

Risk Assessment: Overall process of identifying, analyzing, and evaluating risk.

Risk Control: Any process, policy, device, practice, or other action that modifies risk.

Risk Criteria: Terms of reference against which the significance of a risk is evaluated.

Risk Evaluation: Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

Risk Identification: Process of finding, recognizing, and describing risks.

Risk Inventory: List of potential risks identified for further assessment and analysis, which can later form the basis of a Risk Register (*see*, below).

Risk Philosophy: Statement of the overall intentions, direction, and attitude of the university related to risk. The risk philosophy is typically reflected in the ways risks are considered in

both strategy development and day-to-day operations.

Risk Portfolio (Profile): A composite view of highest-level enterprise risk exposures for presentation by management and discussion with the Board; provides information regarding relationships, concentrations, and/or overlaps of risk as they relate to strategic objectives. Description of any set of risks.

Risk Register (log, repository): Record of information about identified risks; the complete list of all risks identified in the ERM process

Risk Response (Treatment): Process to modify or respond to a risk. Can involve one or a combination of: avoidance, acceptance, mitigation, or transfer.

Risk Response Plan: Plan to implement chosen risk response.

Risk Statement (Description): Succinct statement of risk. Includes the risk itself, cause or source, and potential effect or consequences.

Risk Tolerance (Appetite): The amount of risk that an organization is willing to accept in pursuit of its strategic objectives.

Source (of Risk): Element or circumstance which alone or in combination has the intrinsic potential to give risk to risk. Can be tangible or intangible.

Transfer (Share): Form of risk response, involving contractual risk transfer to other parties, including other internal departments or external partners like insurance.

Appendix B - Potential Risk Areas for Higher Education

ACADEMIC AFFAIRS

- Academic freedom
- Academic quality and standards
- Accreditation
- Collective bargaining
- Computer security, back-up systems
- Contractual relationships/dependencies
- Distance learning
- Educational technology
- Facilities quality
- Faculty diversity
- Faculty employment-operational
- Faculty recruitment and retention
- Grievance procedures
- Health & safety of students, faculty, staff (operational)
- International students-operational
- International travel, global activities
- Joint programs
- Libraries
- Reappointment, promotion and tenure
- Student experiential learning
- Student learning outcomes
- Transportation risks
- *See also compliance and privacy risks*

BOARD GOVERNANCE

- Board member independence
- Board performance assessment
- Compensation & assessment
- Governance policies
- Officer codes of conduct
- *See also compliance and privacy risks*

COMPLIANCE AND PRIVACY

- Accounting – GASB/GAAP
- Affirmative action
- Alcohol and drugs- drug free workplace, drug free schools and community act
- Animal research
- Athletics – NCAA/Title IX
- Background checks
- Biosafety
- Bond compliance
- Information security breach response
- Clinical research – human subjects
- Code of business conduct
- Code of ethics
- Conflicts of interest – inclusive of research
- Copyright and "fair use"

Compliance & Privacy, continued

- Credit card privacy regulations – PCI-DSS
- Environmental health & safety
- Export controls
- Federal sentencing guidelines – organizations
- Foreign nationals - SEVIS
- Gramm-Leach-Bliley
- Government grants – grant restrictions
- Grant accounting – reporting and cost accounting, A-133/A-110/ARRA
- Harassment prevention
- Hazardous materials
- Health and safety compliance
- Higher education act
- HIPAA
- HR/employment – Affirmative action/FLSA/FMLA
- Intellectual property rights – Baye-Dole Act
- Laboratory safety - compliance
- Lobbying
- Policy/procedure - university
- Privacy
- Record retention/destruction
- Red flags rules
- Select agents
- Sexual molestation prevention
- Student financial aid – Title IV, HEOA, program integrity
- Student records - FERPA
- Tax compliance
- Whistleblower policy
- New York security breach notification act

DEVELOPMENT & ALUMNI RELATIONS

- Alumni relations
- Capital campaigns - reduced donor support
- Compliance with donor intent
- Computer security, back-up systems
- Endowment – loss of income/investment
- Gift acceptance policies
- Health & safety of employees, visitors-operational
- High-risk investments
- Investment oversight
- Naming policies
- Sale of donated property
- Special event risks
- Transportation risks
- *See also compliance and privacy risks*

ENROLLMENT MANAGEMENT

- Admissions
- Diversity
- Enrollment trends
- Financial aid - operational
- Graduation rates
- Retention
- Student and family demographics
- Student debt
- Study abroad
- Transportation risks
- *See also compliance and privacy risks*

FACILITIES & OTHER OPERATIONS

- Accessibility
- Auto/Fleet
- Business continuity
- Capital planning and projects
- Emergency planning and response
- Energy
- Facilities maintenance
- Outsourcing
- Police operations
- Pollution
- Property disposal
- Safety - operational
- Transportation and parking
- Waste disposal and recycling
- *See also compliance and privacy risks*

FEDERAL, STATE & COMMUNITY RELATIONS

- City relations
- Neighborhood relations
- Regulatory concerns
- State relations
- *See also compliance and privacy risks*

FINANCE

- Auditor independence
- Budget challenges, allocations, carryovers
- Cash management
- Contracting & purchasing
- Cost management
- Depletion of endowment principal
- Endowment - loss of income/investment
- Financial aid
- Financial exigency plan
- Financial reporting
- Fundraising
- High-risk investments
- Insurance

Finance, continued

- Internal controls
- Investment oversight
- Investment performance
- Liquidity
- Long-term debt
- Reserve fund
- Revenue risks - tuition dependency
- *See also compliance and privacy risks*

HUMAN RESOURCES

- Background checks - operational
- Benefits
- Code of conduct
- Collective bargaining
- Computer security, back-ups
- Diversity
- Employee handbook
- Employee retention
- Employee succession planning
- Employment
- Employment - affirmative action
- Grievance procedure
- Labor relations
- Non-discrimination
- Performance evaluation
- Termination procedures
- Unionization
- Workplace safety – operational
- *See also compliance and privacy risks*

INFORMATION TECHNOLOGY

- Back-up procedures
- Communications systems
- Cyber liability
- Data integrity and protection
- End-user training
- Incident response – continuity and security
- Network integrity
- Security
- Staffing & support
- System capacity
- System maintenance and upgrades
- *See also compliance and privacy risks*

RESEARCH

- Animal research – operational
- Biosafety
- Clinical research - operational
- Competition for grants
- Data security and back-up
- Environmental & laboratory safety – operational

Research, continued

- Facilities quality
- Funding
- Grant administration, accounting, and reporting - operational
- Hazardous materials-operational
- Human subjects - operational
- Patenting
- Security
- Technology transfer
- *See also compliance and privacy risks*

STUDENT AND CAMPUS LIFE

- Academic support
- Alcohol & drugs
- Athletics-operational
- Career services
- Code of conduct
- Communications, public relations, and marketing
- Crime on campus
- Diversity
- Experiential programs
- Food services
- Fraternities & sororities
- Free speech
- International students
- Privacy
- Residential life
- Safety, health, and wellness (including Mental Health)
- SGA activities
- Study abroad
- Transportation risks
- *See also compliance and privacy risks*

Appendix C – Risk Assessment Categories and Impact and Likelihood Scales

Table 1: Risk Categories

Category	Description
Compliance & Legal	Risks related to violations of federal, state or local law, regulation, or university policy, that create exposure to fines, penalties, lawsuits, reduced future funding, imposed compliance settlements, agency scrutiny, injury, etc. Consider both organizational and personal liability for RIT senior leadership.
Financial	Risks related to physical assets or financial resources, such as: tuition government support, gifts, research funding, endowment, budget, accounting and reporting, investments, credit rating, fraud, cash management, insurance, audit, financial exigency plan, long- term debt, deferred maintenance.
Reputational	A threat or danger to the good name or standing of a business or entity.
Operational	Risks related to management of day-to-day university programs, processes, activities, and facilities, and the effective, efficient, and prudent use of the university's resources. Examples including business continuity, health and safety, technology.
Strategic	Risks related to RIT's ability to achieve its strategic goals and objectives, including competitive market risks and positioning, and risks related to mission, values; diversity; academic quality; research; student experience; business model; enrollment management; ethical conduct; accreditation.

Table 2: Risk Measurement Scale: Impact

IMPACT	Description	SEVERE	HIGH	MODERATE	LOW	INCONSEQUENTIAL
		5	4	3	2	1
Financial	$ impact on operating revenue	>$25M	$15-25M	$5-14.9M	$1-4.9M	<$1M
Legal/Compliance	Legal and/or regulatory ramifications	Cessation of programs/operations by regulatory body Significant lawsuits and/or criminal charges and penalties for the university ***and leadership***	Operations under surveillance by external regulatory body Significant lawsuits and/or criminal charges and penalties for the university	Moderate legal penalties; operations under surveillance internally	Low legal penalties	Minor legal penalties
Reputational	Negative media attention Public criticism (from any cause, i.e. compliance, reliability, environmental, safety, etc.) Reduction of support from funding agencies	Event prevents achievement of specific objectives and financial plan Sustained, serious loss in market share, brand value, and/or public confidence Significant attrition in student and/or faculty retention/attraction	Event has a major impact on strategic objectives and/or financial plan Serious decline in market share, brand value, and/or public confidence Noticeable attrition in student and/or faculty retention/attraction	Event has a moderate impact on strategic objectives and/or financial plan Market share, brand value and/or public confidence will be affected in the short term Some attrition in student and/or faculty retention/attraction	Event has a minor impact on strategic objectives and/or financial plan There is a potential impact on market share, brand value and/or public confidence Consequences can be absorbed under normal operating conditions Potential attrition in student and/or faculty retention/attraction	Event has limited local damage with no wider impact – likely to be no impact on financial plan No material impact on market share, brand value and/or public confidence Limited-to-no attrition in student and/or faculty retention/attraction
Operational	Compromise of operational efficiency and effectiveness	Widespread or long-term shut down of operations Inability to properly market and operate all university offerings Threat of severe market share loss Significant and sustained attrition in staff and/or faculty retention	Significant internal and/or external resources needed/committed to address operational issues Deep and/or sustained operational interruptions Noticeable attrition in staff and/or faculty retention	Escalating internal and/or external resources needed/committed to address operational challenges Larger, or multiple operational inefficiency(s) Some attrition in staff and/or faculty retention	Escalation of internal resources needed/committed to address operational issue Minor operational inefficiency Potential for attrition of staff and faculty retention	Modest internal resources needed/committed to internal operational issue Insignificant operational inefficiency Limited-to-no attrition in staff and/or faculty retention
Strategic	Impact related to RIT's ability to achieve its strategic goals and objectives	Reverses progress on one or more RIT strategic goal or threatens strategic plan failure	Stop progress on more than one strategic goal	Stops progress on one RIT strategic goal	Slows progress on more than one RIT strategic goal	Slows progress on one RIT strategic goals

Revised January 2023

Table 3: Risk Measurement Scale: Likelihood

LIKELIHOOD	EXPECTED (90 – 100%)	LIKELY (60 – 90%)	POSSIBLE (35 – 60%)	UNLIKELY (10 – 35%)	REMOTE (0 – 10%)
	5	4	3	2	1
Description	Event is expected to occur in most circumstances	Event will probably occur in most circumstances	Event is as likely to occur as not to occur	Event could occur at some point in time	Event may only occur in exceptional circumstances

Revised January 2023

Quantifying the Risk (Impact x Likelihood = Risk Score)

- The **University Risk and Compliance Network** (the "Network" or "**URCN**") is initially responsible for quantifying **ALL** identified risks and compiling risk scores.
- **Risk Scores between 12 and 25** will be elevated to the **University Risk and Compliance Committee** ("**URCC**") for review, reevaluation of the risk, and confirmation of the Risk Score.
- **Risk Scores between 16 and 25** as confirmed by the URCC will be elevated to the **Executive Risk and Compliance Committee** ("**ERCC**") for review, reevaluation of the risk and confirmation of the Risk Score.
- **Risk Scores between 20 and 25** as confirmed by the ERCC will be elevated to the **ERM Subcommittee in the Institutional Risk Map**, along with other identified risks deemed appropriate by the ERCC.

Table 4: Risk Prioritization Matrix

Impact Score → / Likelihood Score ↓	Inconsequential 1	Low 2	Moderate 3	High 4	Severe 5
Expected 5	5	10	15	20	25
Likely 4	4	8	12	16	20
Possible 3	3	6	9	12	15
Unlikely 2	2	4	6	8	10
Remote 1	1	2	3	4	5

Key

Red = Priority #1
Orange = Priority #2
Yellow = Priority #3
Green = Priority #4