R·I·T

Guide to Risk Assessment and Response

Contents

List of Figures

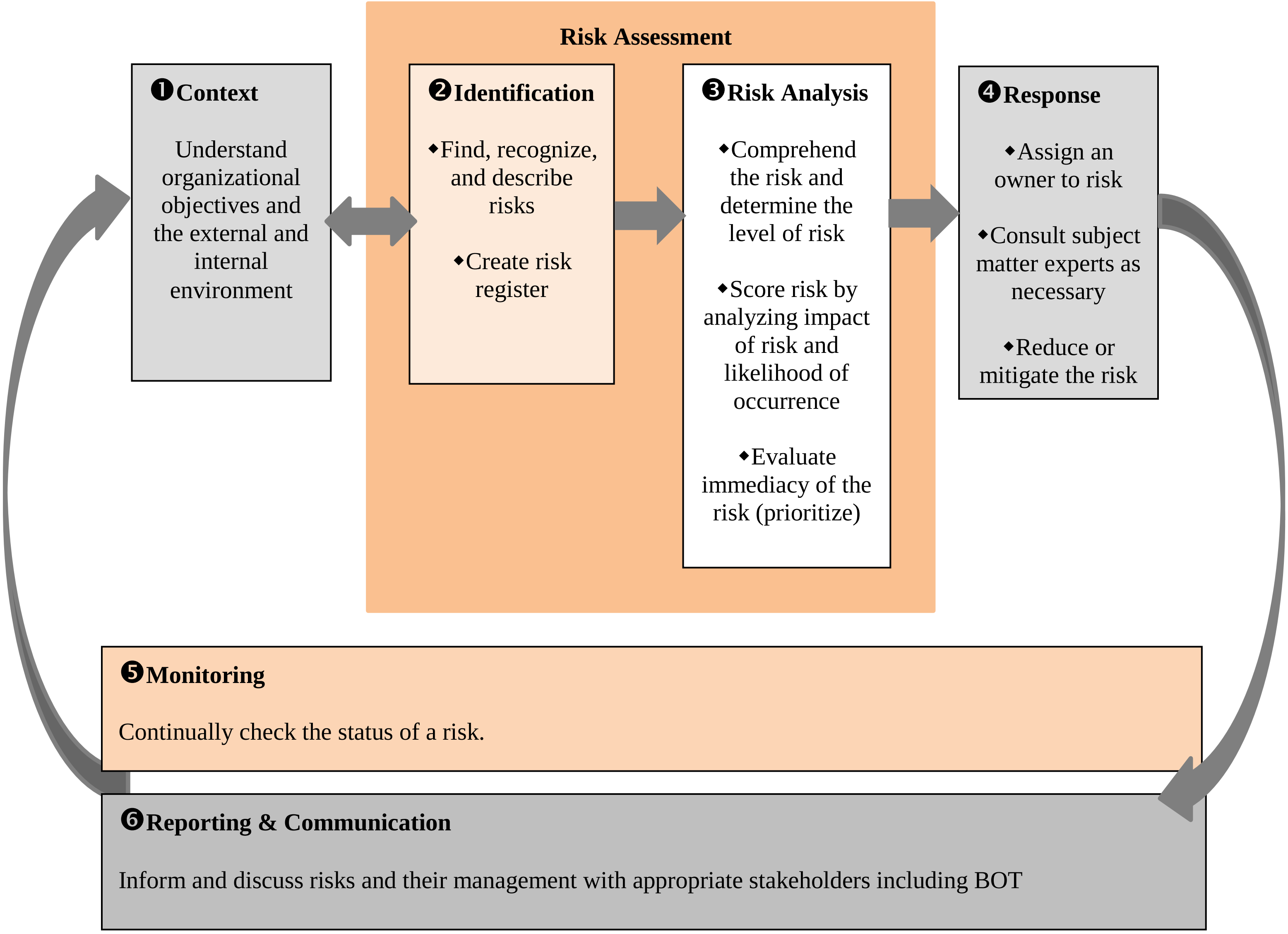
List of Tables

Overview

Enterprise risk management (ERM) is 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.

The Context (Step 1) and the Risk Assessment steps (Steps 2 and 3) form the basis for decision-making about which risks are priorities, what the appropriate response should be, and how resources should be allocated to manage the risk to best support the University. The Response (Step 4) involves deciding on and planning for the best way to "treat" or modify the risk, and implementing that plan.

Figure 1: The Enterprise Risk Management Process



Risk Assessment

➊Context

Understand organizational objectives and the external and internal environment

➋Identification

- Find, recognize, and describe risks
- Create risk register

➌Risk Analysis

- Comprehend the risk and determine the level of risk
- Score risk by analyzing impact of risk and likelihood of occurrence
- Evaluate immediacy of the risk (prioritize)

➍Response

- Assign an owner to risk
- Consult subject matter experts as necessary
- Reduce or mitigate the risk

➎Monitoring

Continually check the status of a risk.

➏Reporting & Communication

Inform and discuss risks and their management with appropriate stakeholders including BOT

Any individual may use this guide to assess and plan responses to risks in their area. For example:

1) As part of RIT's annual ERM process, senior leadership and administrators, *i.e.*, vice presidents, associate or assistant vice presidents, deans, directors or other senior officials designated as responsible for a risk ("Responsible Officials"), will identify and assess the *enterprise-level* risks for which they are responsible.

2) RIT senior management or trustees may choose to conduct a risk assessment of a planned, university, strategic initiative to inform decision-making.

3) Vice presidents, deans, directors, or other senior officials may, at their option, use this guide to conduct a risk assessment for their area that considers college, school, division, or department-level risks in addition to enterprise issues.

Results of all risk assessments and response plans *conducted as part of the ERM initiative* will be shared with the Office of Compliance and Ethics (OCE) and will form the basis of discussions with the Risk and Compliance Committees at the University, after which an Institutional Risk Map will be created.

Tools and Resources

OCE is a resource for Responsible Officials and their staff, available to conduct facilitated risk assessment workshops and other educational/training sessions.

Step 1: Establish the Context

The purpose of establishing the context for risk assessment is to set the stage for risk identification. Because "risk" is defined as "any issue that may impact an organization's ability to achieve its objectives," defining the organization's objectives is a prerequisite to identifying risk.

Things to Keep in Mind When Establishing Context for Risk Assessment:

1. What are the goals or objectives of the RIT Strategic Plan your area supports, if any?
2. What are the strategic goals or objectives for your college, school, division, or department?
3. Are there any major initiatives that your area is planning or engaged in currently?
4. Are there any critical activities, functions, or services others rely on your area to provide?
5. Are there any external factors such as legal/regulatory requirements, stakeholder perceptions and expectations, or any relevant social, cultural, political, financial, technological, economic, or competitive factors?

Step 2: Risk Identification

The purpose of the risk identification step is to “generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate, or delay the achievement of objectives” (ISO 31000, 2009).

Things to Keep in Mind When Identifying Risk:

- Be as comprehensive as possible at this stage – identify everything you can.
- Identify events that could hinder attainment of strategic goals (risks).
- Include known risks regardless whether they are “under your control.”
- Think about related risks and cascading or cumulative impacts.
- Involve the most knowledgeable people.
- Use the most relevant and up-to-date information you have.

Questions to Ponder and Discuss:

1. What could affect the university or your area’s ability to achieve or fulfill your strategic goals, initiatives, or key functions, negatively? What uncertainties do you face?
2. What categories of risks could your area or the university face in terms of:
    a. Compliance and Legal Liability
    b. Finances
    c. Operations
    d. Reputation
    e. Strategic Issues
3. What do you see as weaknesses or threats facing your area?
4. Have there been any recent major changes to your area of responsibility or control (new regulations, new programs/activities, organizational changes, etc.) that pose new risks?
5. Are there particular programs, activities, internal controls, or legal/regulatory issues, in your area that worry you or you think may pose significant risk to your unit or the university?

Steps to Follow:

1. Write a brief “risk statement” that describes each risk and provides a little more detail about its sources and causes. Do not include potential impacts or consequences in the risk statement. Aim for a succinct risk statement: not too short, not too long; not too vague, not too detailed; meaningful but not inflammatory. For example:
    - Too vague: “IT infrastructure”
    - Too specific/inflammatory: “IT network and hardware is obsolete, resulting in the potential for loss of university business continuity, loss of irreplaceable data, and privacy breaches”
    - Just right: “IT infrastructure not maintained and/or upgraded to necessary standards.”

2. Consider whether each issue is a risk.
3. Consider which university strategic goal or objective each risk affects.
4. Consider other strategic goals or initiatives for your particular area that the identified risk affects.
5. Identify the Responsible Official for each risk. This is the individual at RIT with the accountability and authority to manage the issue.

Other Tools and Techniques:

- Appendix B – *Potential Risk Areas for Higher Education*, lists common risk areas by major university function.
- Other techniques you can consider to help identify risks may include:
    - Brainstorming
    - Questionnaires
    - Studies
    - Industry benchmarking
    - Scenario analysis
    - Incident investigation
    - Audits or Inspections

Key Terms:

- **Risk**: Any issue that may impact an organization's ability to achieve its objectives. Often characterized in reference to potential events, consequences, and the likelihood thereof.
- **Risk identification**: Process of finding, recognizing, and describing risks.
- **Risk statement (description)**: Structured statement of risk usually containing four elements: sources, events, causes, and impacts/consequences.
- **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.
- **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 that prevents an organization from meeting its objectives in the absence of any action to control or modify the event.
- **Responsible Official (risk owner):** Person or entity with the accountability and authority to manage a risk.
- **Residual risk**: A risk that remains after an organization has implemented procedures or other efforts have been made to mitigate or eliminate risks associated with a business process or risk identified.

Step 3: Risk Analysis

The purpose of a risk analysis is to develop an understanding of the risk in order to inform your decision or analysis of whether a response is required. Here is where you will assess the potential **impact** and **likelihood** of the risks, as well as the immediacy of the risk so you can **prioritize** any responses.

Things to Keep in Mind When Conducting Risk Analysis:

- Consider causes and sources of risk, their negative consequences, the likelihood that they can occur, and other attributes of the risk.
- Consider interdependence of different risks.
- Consider the immediacy of the risk to help you prioritize the risks identified.

Steps to Follow:

1. Identify which risk "category" best fits each risk: compliance and legal, financial, health and safety, operational, or strategic. (*See*, Table 1, *Risk Categories*, below.)
2. Consider the potential impact of each risk by using the risk impact scales shown in Table 2 and 3. If more than one column of the scale relates to your risk, base your rating on the column that reflects the greatest impact. This will likely be the column that also corresponds to the category of the risk. (For example, if you categorized your risk as a "financial" issue, you will likely use the financial column of the impact scale to determine your impact rating.)
3. Consider the likelihood that each risk will occur by using the likelihood scales shown in Tables 4 and 5. Consider the processes and procedures that you already have in place to address or treat the risks you have identified.
4. The impact and likelihood scores will be multiplied to produce an initial risk score for each risk.

Other Tools and Techniques:

Other techniques you can consider to help analyze your risks may include:

- Business continuity planning
- Business impact analysis
- Market surveys, prospecting
- Measures of central tendency and dispersion
- SWOT analysis
- Threat analysis

Key Terms:

- **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.
- **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
- **Probability:** Measure of the chance of occurrence expressed as a number between 0 and 5
- **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 control:** Any process, policy, device, practice, or other action that modifies risk

Table 1: Risk Categories

Category	Description
Compliance & Legal	Risks related to violations of federal, state or local law, regulation, or university policy, that creates exposure to fines, penalties, lawsuits, reduced future funding, imposed compliance settlements, agency scrutiny, injury, etc.
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	- Operations under surveillance by external regulatory body	-Significant 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 all university offerings -Threat of severe market share loss	-Significant internal and/or external resources need to be committed to address operational issues -Deep and/or sustained operational interruptions	-Escalating internal and/or external resources need to be committed to address operational challenges -Larger, or multiple operational inefficiency(s)	-Escalation of resources that need to be committed to address operational issue -Minor operational inefficiency	-Modest resources need to be committed to internal operational issue -Insignificant operational inefficiency
Strategic	-Impacted 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

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 occur	Event could occur at some point in time	Event may only occur in exceptional circumstances

Quantifying the Risk (Impact x Likelihood = Risk Score):

- The University Risk and Compliance Network (the "Network" or "URCN") will be initially responsible for quantifying identified risks and compiling a Risk Score. 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.

Step 4: Response

The purpose of the response step is to decide, based on the results of your risk analysis, which risks require a response and what your recommended response will be.

Things to Keep in Mind When Formulating Response:

- Each risk score (the product of impact X likelihood) will determine where it falls on RIT's risk "heat map" and what level of review each risk will receive.
- Risk response is a cyclical process of assessing the response, determining whether residual risk levels (after response) are acceptable, developing a new response if necessary, and assessing the response again.
- There are several standard options for risk response, but they are not mutually exclusive; they can be used in combination.
- A decision can be to not respond to the risk other than maintaining existing management or control activities.
- Consider whether some responses are not economically justifiable (*e.g.*, an expensive response for a high impact but low likelihood risk).
- Responding to risk can itself introduce risks. Consider how your response plan will deal with any secondary risks.

Steps to Follow:

1. Consider the overall results of your risk analysis, especially your rating of the risk's impact and likelihood and the resulting risk score.
2. Consider which risk response options you will use to manage this risk: accept, avoid, mitigate, or share (transfer).
3. Consider what steps you will take to respond to each risk.
4. Consider any costs or special resource needs associated with your response.
5. Consider how long it would take to fully implement your response.

Key Terms:

- **Risk response (treatment):** Process to modify or respond to a risk. Risk response can involve one or a combination of: acceptance, avoidance, mitigation, or sharing.
  - **Accept:** An informed decision to tolerate or take on a particular risk.
  - **Avoid:** An informed decision not to be involved in, or to withdraw from, an activity, in order not to be exposed to a particular risk.
  - **Mitigate:** Actions designed to reduce a risk or its consequences.
  - **Sharing (transfer), risk:** Contractual risk transfer to other parties, including insurance.
- **Risk response plan:** Plan to implement a particular risk response.
- **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.

Appendix A - Key ERM Terms and Definitions

General ERM Terms

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.

Risk: 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*, page 7, *above*: **Inherent risk**, defined as an issue that prevents an organization from meeting its objectives in the absence of any action to control or modify the event and Residual risk, defined a risk that remains after an organization has implemented procedures or other efforts have been made to mitigate or eliminate risks associated with a business process or risk identified.)

Terms Related to ERM Program & Context

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.

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

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

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

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.

Terms Related to the Risk Assessment Process

Acceptance: Form of risk response, an informed decision to tolerate or take on a particular risk

Avoidance: 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.

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.

Ignore: Just as the "acceptance" strategy takes no active measures to deal with a residual risk, risks can also be *ignored*, adopting a reactive approach without taking explicit actions.

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.

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: Form of risk response involving actions designed to reduce a risk or its consequences.

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

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 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. Risk response 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.

Sharing (transfer), risk: Form of risk response, involving contractual risk transfer to other parties, including insurance.

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.

Terms Related to ERM-Enabling Activities

Communication & consultation: 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.

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

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

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
- CEO 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

Student and Campus Life, continued

- 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
- SGA activities
- Study abroad
- Transportation risks
- *See also compliance and privacy risks*

Appendix C - ERM Program Purpose, Goals & Objectives, ERM Guiding Principles, and University Risk Philosophy

ERM Program Purpose, Goals & Objectives

The purpose of RIT's ERM program is to enhance the University's ability to achieve its mission, vision, and strategic objectives and strengthen its competitive position by fostering a university-wide culture of risk awareness. The ERM Program is intended to provide a structured, consistent, and continuous process for the early and proactive identification and reporting of material risks to senior management and the Board of Trustees.

In support of this overall purpose, the following goals and objectives have been identified:

1. Create a culture of risk awareness where employees understand and consider risk in decision-making:

    a. Ensure that all RIT employees are aware of the risks related to their roles and activities and understand their responsibilities for identifying, managing, and reporting on risk in a systematic and timely way;
    b. Provide best practice information, education, training, and facilitation resources to the University community;
    c. Build on the University's current risk management activities and practices.

2. Reduce operational surprises and losses.

3. Facilitate greater transparency and openness regarding risk.

4. Enhance enterprise decision-making by providing senior management and trustees with timely and robust information that improves their understanding of enterprise-level risks:

    a. Assess risks in the context of strategic objectives;
    b. Identify related risk factors across the University;
    c. Anticipate and respond to changing social, financial, economic, environmental, and legal/regulatory conditions;
    d. Assist management in safeguarding University assets, including people, financial resources, property, and reputation;
    e. Assist management in optimizing the use of University resources by aligning resource allocations with the areas of highest risk and the greatest impact on the University's strategy.

5. Improve the efficiency and effectiveness of university risk management efforts:

    a. Provide the University community with a common language, framework, and set of procedures for identifying, assessing, responding to, and reporting on risk posed in new and ongoing endeavors across the organization's entire range of assets and operations;
    b. Provide enterprise-level coordination of existing University functions for identifying, assessing, and reporting on risk;

c. Integrate risk ownership and management activities at all levels of the university.
d. Where possible, use and strengthen existing management processes, reporting and approval channels, and organizational structures;
e. Establish and maintain a university risk register that allows for the tracking and reporting of risk trends and of risk response plans;
f. Review the effectiveness of enterprise risk management practices regularly.

Guiding Principles of RIT's Enterprise Risk Management Program

RIT seeks to establish a risk-aware university culture where consideration of both upside and downside risk is integrated into decision-making at all levels of the University. These guiding principles support that culture and set expectations for the behavior of University employees and administrators regarding risks.

1. All individuals, regardless of their role at the University, are empowered and expected to report to senior management any perceived risks or failures of existing control measures, without fear of retaliation.

2. Risk management is integral to the management and future of the University and is a shared responsibility at all levels of the University.

3. Ownership and management of risk will be retained within the University function, department, or unit that creates the risk or is best capable of responding to it.

4. The University's risk philosophy will guide strategic and operational decisions at all levels.

5. RIT encourages an open and honest discussion of the University's environment, strategy, risks, and actions taken in pursuit of its objectives.

6. All good faith reports of risks are responded to promptly and with integrity by a University official (or designee), and information about risks is shared promptly with senior management and other key stakeholders.

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 aims. RIT does not seek to eliminate *all* risk; rather, RIT 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, taking into account their impact on the RIT Community, and RIT's standing, reputation, financial position, and performance.

Appendix D - Sample Board Reporting Form

Risk Management Report to Board

Date:	
Risk Identified:	
Risk Owner:	
Board Committee(s):	
Description of Risk:	
Likelihood: (rate 1-5)	
Impact: (rate 1-5)	
Risk Score: (likelihood x impact)	
Risk Tolerance:	SET BY SENIOR LEADERSHIP BASED ON TOTALITY OF CIRCUMSTANCES
Response/Treatment Plan:	
Likelihood After Response/Treatment:	
Impact After Response/Treatment:	
Risk Score After Response/Treatment: (likelihood x impact)	