UNC GREENSBORO

Enterprise Risk Management Program Framework

February 2025

On the Cover

Park, J. (2018, August 4). PIC2161_2018_Brand_Light_Pole. [UNCG photo by Jiyoung Park- 8/4/18 – 2018 Brand Light Pole Banner.]. Retrieved August 1, 2021, from https://uncg.merlinone.net

ADMINISTRATIVE STATEMENT

The following information applies to this document:

1. The title of this document is the "UNC Greensboro Enterprise Risk Management Program Framework," or shortened for internal use, the "ERM Framework."
2. This plan is considered a public document and available to all University stakeholders.
3. The information contained in the framework was prepared for use by UNC Greensboro (UNCG), specifically Enterprise Risk Management and the overall University enterprise risk management program.
4. For more information, please consult Enterprise Risk Management:

   Enterprise Risk Management
   (336) 256-1102
   1200 W. Gate City Boulevard
   Greensboro, NC 27403
   risk@uncg.edu

TABLE OF CONTENTS

Enterprise Risk Management Overview

Introduction

The UNCG Office of Enterprise Risk Management is responsible for developing, implementing, and maintaining an enterprise-wide risk management program. This program performs the activities within the risk management process to support the creation and protection of UNCG's value, improve performance, encourage innovation, and support achieving objectives.

Enterprise risk management promotes an ongoing, risk-conscious culture across the University to enable decision-makers to perform a risk-reward analysis of choices and make decisions with an understanding of the implications of such actions while pursuing the mission and goals of UNCG. It is not intended to be a one-time process or a prescriptive method for managing individual risks, but instead, a tool for leadership to use in addressing existing and emerging risks within their portfolio of activities.

To achieve UNCG's strategic objectives, risks are considered and managed enterprise wide. Therefore, this framework is intended for reference and use by the entire UNCG community. Effective risk management is integral to strategic planning, business decision-making, day-to-day operations, and organizational resiliency. While management and compliance of the ERM Program are under the leadership of the Associate Vice Chancellor for Campus Enterprises, university leadership will regularly assess the status of risks and how they are managed and provide further direction and leadership in the spirit of the University's mission and values.

Program Overview

The purpose of the ERM Program at UNCG is to provide a comprehensive structure to proactively manage risks and opportunities that university leadership collectively agrees are the most important to achieving the institution's strategic objectives.

Objectives

The objectives of the ERM Program include:

- Identifying and assessing a broad array of risks that could negatively and positively impact achieving institutional goals and objectives.
- Ensuring appropriate ownership and accountability of risks.
- Developing and implementing appropriate risk management and monitoring plans by risk owners.
- Providing a program structure that engages functional leaders across the campus to identify and prioritize risks.
- Providing senior leadership with key information to make risk-informed decisions and allocate resources effectively.

Scope

Risk is defined as the effect of uncertainty on objectives, both positive and negative. To support this definition, ERM addresses risks and opportunities that may impact UNCG's strategic goals and objectives. As such, ERM looks across the entire institution using a forward-thinking approach and open communication. ERM also examines potential risks and opportunities outside of the institution that could have an impact, including but not limited to regional, national, and global risks that have the

potential to impact both higher education and UNCG. ERM examines risk from these perspectives to capitalize on thought leadership, identify lessons learned, and benchmark upon best practices. ERM examines potential risks and opportunities based on the following risk categories:

- **Strategic Risks** – Risks or opportunities related to our strategic plan anchored by Transformation – Student Transformation, Knowledge Transformation, and Regional Transformation.
- **Operational Risks** – Risks or opportunities related to managing day-to-day university programs, functions, activities, facilities, infrastructure (including technology), and the efficient, effective, and prudent use of university resources.
- **Life and Health Risks** – Risks or opportunities related to the campus population's injury, damage, health and safety, including impacts caused by accidental or unintentional acts, errors or omissions, and external events such as natural disasters.
- **Financial Risks** – Risk or opportunities 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, overall debt, etc.
- **Compliance Risks** – Risks or opportunities related to violations of state and federal laws and regulations, local municipal law, accreditation standards, University policies and procedures, and contractual obligations, including contractual agreements.
- **Reputational Risks** – Risks or opportunities related to the University's reputation, such as the risk of failure to meet stakeholder expectations as a result of any event, behavior, action, or inaction.

ERM does not directly manage or oversee the areas of internal audit, compliance, integrity, privacy, or information security. However, ERM is a close partner and collaborator with these areas of the University that oversee these functions.

Guiding Standards and Best Practices

Several operating standards, requirements, and best practices that are professionally accepted to aid the development, implementation, and maintenance of an ERM Program have been used to develop the ERM Program and align the Program with accepted best practices.

Using these standards and resources, the UNCG ERM Program is structured based on the ISO 31000 standard, incorporating some COSO principles for integrating ERM with strategy and performance. Each of these is explained in more detail below.

ISO 31000 – Risk Management

The International Organization for Standardization (ISO) 31000 is an international standard published in 2009 and updated in 2018 that provides principles and guidelines for managing risks organizations face. It outlines a generic approach to risk management, which can be applied to different types of risks (financial, safety, project risks) and used by any organization. The standard provides a uniform vocabulary and concepts for discussing risk management. It provides guidelines and principles that can help to embark on a critical review of the organization's risk management process.

For more information on ISO 31000 or to review the standard, view the ISO 31000 webpage.

COSO Enterprise Risk Management

In 2004, the Committee of Sponsoring Organization of the Treadway Commission (COSO) published the Enterprise Risk Management Integrated Framework to enhance an organization's ability to manage uncertainty and increase its value using an enterprise risk management framework. In 2017, COSO updated the document to incorporate the linkage of ERM to an organization's strategy and performance to improve the value and outcomes of an organization.

For more information on COSO Enterprise Risk Management, view the COSO webpage.

Authorities and References

The following listed authorities and references support this framework.

- UNCG Board of Trustees Compliance, Audit, Risk, and Legal Affairs Committee Charter
- UNC System Policy 1300.7 - University Enterprise Risk Management and Compliance
- International Organization for Standardization (ISO) 31000 – Risk Management
- Committee of Sponsoring Organization of the Treadway Commission – Enterprise Risk Management, Integrating with Strategy and Performance

Enterprise Risk Management Structure

Organizational Structure

The ERM Program is a collaborative effort amongst various stakeholders through various levels of our organization, each with specific roles in the ERM process.

Board of Trustees CARL Committee

It is the policy of the UNC Greensboro Board of Trustees, as exercised through its Compliance, Audit, Risk Management, and Legal Affairs (CARL) Committee, to provide oversight and assistance to the University in its efforts to promote a culture of compliance; ensure the timely development of operational policies and procedures that are consistent with relevant laws and regulations; and promote collaboration among and between compliance, audit, risk management, legal, and ethical functions at the University. In exercising these duties, the CARL Committee assists the Board in fulfilling its oversight responsibilities related to establishing, implementing, and evaluating a University-wide ERM program. A complete list of the CARL Committee's duties associated with ERM can be found in the CARL Committee Charter.

Chancellor's Council

The Chancellor's Council is a body of University officers appointed by the Chancellor to serve as senior advisors. Members of the Chancellor's Council are responsible for several aspects of the ERM program. These responsibilities include:

- Establishing and pursuing the mission, vision, and goals of the institution
- Determining the University's risk tolerance for each risk category
- Serving as Risk Executives for risks directly under their portfolio of responsibilities and collaborating with their delegated Risk Owners
- Ensuring risks under their purview are managed appropriately
- Providing direction to the Enterprise Risk Management Committee

Enterprise Risk Management Committee

An Enterprise Risk Management Committee (ERMC) is in place to aid in the identification, assessment, prioritization, and mitigation planning of risks that have the potential to impact the institution. The ERMC comprises a cross-functional representation of campus leaders who provide strategic direction and insight to achieve the ERM Process. A complete list of ERMC responsibilities and the committee scope can be found in the ERMC Charter located in Annex 1 of this framework.

Risk Owner

A Risk Owner is a member of a divisional leadership team who is accountable for managing the risk within their purview on behalf of the Risk Executive. This includes but is not limited to assessing the risks to determine the severity, velocity, and likelihood of its occurrence, determining if the risk is improving with additional control measures, stabilizing, or declining. It is the responsibility of the Risk Owner in partnership with other applicable subject matter experts to:

- Align risk to university strategic goals and objectives
- Ensure alignment with risk appetite
- Assess existing risk mitigations and controls
- Recommend future remediation strategies and risk tolerance
- Monitor and report on risk conditions

Risk Partners

For the ERM process to be successful, it must include all University stakeholders and provide a mechanism for new and emerging risks to be reported and explored. To foster a culture of risk awareness, the ERM Program views all internal and external stakeholders as risk partners. Risk partners can include departments and units on campus, committees or workgroups established to accomplish a task or solve a problem, or external affiliates we work closely with, such as other institutions and the UNC System Office.

Office of Enterprise Risk Management

The Office of Enterprise Risk Management provides university-wide coordination of the overall ERM program. In doing so, the Office of ERM is responsible for:

- Maintaining the ERM Program Framework and facilitating ERM processes
- Administering the University's ERM software
- Working directly with Risk Owners to accurately document and evaluate risks and establish risk action plans as needed
- Supporting the ERMC committee.

Three Lines of Defense

Organizations adopt the Three Lines of Defense to establish risk management capabilities. It distinguishes the areas of the University responsible for owning and managing risk, oversight of risk, and independent assurance of risk. Each of the three lines of defense has direct accountability to UNCG's executive management team and/or the Board of Trustees CARL Committee. The maturity and effectiveness of ERM within the University may be reflected in the effectiveness of the implementation of the Three Lines of Defense model. The greater the level of integration, the greater the likelihood of achieving a culture of risk consciousness and organizational resiliency.

First Line of Defense

The first line of defense owns and manages risks. Contrary to how risk management is sometimes perceived, individual risks and the controls that mitigate them are not owned by risk or compliance professionals. Instead, operational management and senior leadership are responsible for ongoing activities that include:

- Owning and managing risks
- Identifying, assessing, and mitigating risks
- Implementing corrective actions
- Implementing and maintaining internal controls
- Conducting evaluations of internal controls (which may also include self-evaluations)
- Executing risk and control procedures daily

Second Line of Defense

The second line of defense oversees risk and compliance. Risk-associated functions, including enterprise risk management, are found in this line of defense. Parts of the second line of defense include:

- Ensuring that operational management and senior leadership are implementing effective risk management practices
- Assisting Risk Owners with risk evaluation by considering the institution's risk appetite
- Helping Risk Owners report risk-related information throughout the institution
- Providing updates on the status of risk and resiliency to executive leadership and the Board of Trustees CARL Committee

Third Line of Defense

The third line of defense provides independent assurance. Internal Audit forms the third line of defense and assures the effectiveness of governance, risk management, and internal controls. It assesses the effectiveness of the first and second lines of defense in achieving risk management objectives and the effectiveness and efficiency of the risk management and internal control framework. Internal Audit reports directly to the CARL Committee of the Board of Trustees to remain objective and independent.

Enterprise Risk Management Process

A risk is an event or action that impacts an organization's ability to achieve its objectives, whether positive, negative, or a combination of both. Identifying and prioritizing such risks is designed to include broad input from university leadership and ERM stakeholders, both internal and external to the University. The initial identification of a risk can come from one of any number of channels, forums, and individuals.

Scope, Context, and Criteria

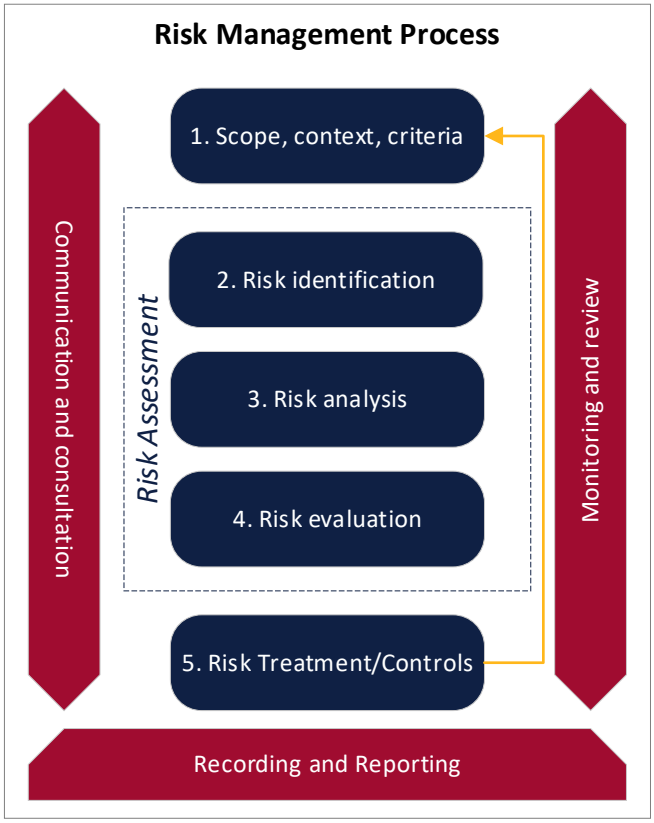
The scope, context, and criteria of the UNCG ERM Program were addressed in this document's Enterprise Risk Management Program Overview and Enterprise Risk Management Structure sections. The scope, context, and criteria established in those sections serve as the foundation for the remaining risk management process elements.

Risk Assessment

Risk assessment is the overall risk identification, analysis, and evaluation process. Risk assessments are conducted methodically and collaboratively, using the knowledge and views of risk stakeholders and the best information available.

Risk Identification

Risk identification aims to find and define risks that may positively or negatively impact the University and can be framed by thinking about topics that can potentially affect the institution's strategic goals and objectives. Issues present within the University, the geographical region, peer universities, the higher education landscape, or throughout the nation and world could all have the potential to have such an impact. Risks are identified through open, transparent, and collaborative communication and are initially identified as inherent or perceived risks.



Industry thought leadership and expertise in enterprise risk and higher education can be excellent resources for understanding the risk landscape. These resources offer best practices that may help proactively expedite the escalation of emerging risks that could affect the institution. The Educational Advisory Board, The Chronicle of Higher Education, EDUCAUSE, United Educators, the Risk and Insurance Management Society (RIMS), and the University Risk Management and Insurance Association (URMIA) are such valued resources.

Peer institutions provide the opportunity to identify the risks being managed within their respective cultures, how they are being addressed, and what emerging risks or opportunities are on their horizon. This network also provides support and opportunities to share best practices, conduct program modeling, and understand lessons learned.

University leadership and the UNCG community are the best and most reliable sources of risk/opportunity identification. As the First Line of Defense, the individuals who learn and work within the University environment provide excellent insights and perspectives regarding areas of potential risk and opportunity. On at least an annual basis, ERM leadership conducts risk meetings with the Chancellor's Council members. These conversational meetings allow ERM to understand what concerns, issues, or opportunities are faced within each leader's area of expertise.

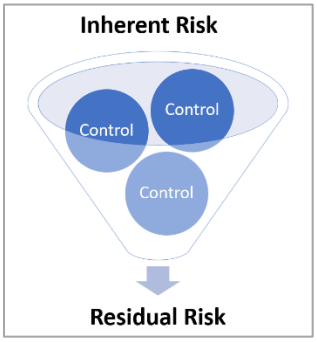
Continuous socialization, training, awareness, and community engagement are part of the key goals of Enterprise Risk Management toward effective risk identification. Whether through professional development training, continuity and disaster recovery planning and exercising, or leadership forums and staff meetings, the objective is for the University community to be able to say something if they see something.

To make risk identification/reporting accessible to the entire UNCG community, the Office of Enterprise Risk Management has established a public risk submission form. Risks submitted through the public submission form are evaluated by the Office of Enterprise Risk Management and shared with the appropriate Risk Executive and Risk Owner.

Risk Analysis

To analyze risks effectively and consistently, a collaborative approach is used that provides risk stakeholders with the data to understand the nature of the risk and its characteristics, including the level of risk. Risk analysis discussions with risk stakeholders and university subject matter experts enable a collective understanding and agreement of a risk's potential impact on the University. This allows university leadership to make risk-informed decisions within the established risk appetite and take advantage of opportunities that will capitalize upon the University's mission and values.

The Risk analysis process explores several factors that ultimately result in a risk score. These include the impact or magnitude of the risk, the likelihood the risk will occur, the risk velocity or how quickly the risk could impact, and the effectiveness of existing treatments/controls. These factors are analyzed through two lenses: inherent risk and residual risk. Inherent Risk is typically defined as the level of risk in place before actions (treatments and controls) are taken to alter the risk's impact or likelihood. Residual Risk is the remaining level of risk following the development and implementation of controls or mitigation measures.



Risk Score Status Calculation

A simplified approach to calculating a risk's likelihood, velocity, and impact is used to understand which risks warrant the most attention. This level of attention is then addressed with the Risk Executives and Risk Owners. To establish a simplified and consistent methodology for deriving risk factor ratings and overall risk scores, an ERM Risk Rating Guide has been created and can be found in Annex 3: Risk Rating Guide.

Risk Prioritization

Following the identification of perceived risks, the result may be dozens of risks brought to the attention of Enterprise Risk Management. In collaboration with the ERM Committee, ERM prioritizes risks with the greatest potential likelihood and severity impact. The goal is to narrow the list of enterprise risks each fiscal year to 5-7 that will be prioritized for assessment with the appropriate Risk Executives and Risk Owners. As a caveat to this approach, risks may materialize unexpectedly (i.e., the unknown unknowns), which might realign the prioritization for assessment and redirect resources accordingly.

Risk Treatments

Risk treatments aim to choose and implement options for addressing risk. Once a risk has been identified and assessed, the Risk Owner and Risk Executive should identify the most appropriate risk treatment(s) based on the University's risk appetite. Risk Treatments may include one or several of the following:

- **Risk Acceptance with Further Monitoring** – the risk and current control activities are within the University's risk appetite and will continue to be monitored for any changes.
- **Additional Controls** – the risk and current control activities are outside the University's risk appetite and will undergo further mitigation and control activities until the risk demonstrates improvement with a reduction in potential likelihood and severity of occurrence.
- **Risk Transfer** – the risk and current control activities are outside the University's risk appetite and will be transferred to a third party for additional management to lessen the burden of the likelihood and severity of occurrence.
- **Risk Avoidance** – the risk and current mitigation activities are outside the University's risk appetite and will be avoided by discontinuing the activities, decreasing the likelihood and severity of occurrence.

Controls

Controls are mitigation measures that reduce the likelihood, velocity, and impact of identified risks. Examples of risk controls include:

- Policies and procedures that direct actions and behavior toward an intended outcome
- Adherence to compliance measures such as federal, state, and local laws
- Implementation of key risk indicators to periodically measure residual risk
- Mitigation activities that lessen a risk's residual risk score.

Risk Owners are responsible for documenting the implementation of risk controls in the University's ERM software and using the effectiveness of risk controls to continually assess the residual risk.

Risk Action Plans

If a risk is rated as having a high residual risk score, the Risk Owner is responsible for creating a risk action plan. A risk action plan is a plan that addresses how the Risk Owner and risk stakeholders will manage the risk and lower its risk score to an acceptable risk level. Risk action plans are managed within the University's ERM software and should be reviewed and updated annually.

Recording and Reporting

The recording and reporting of risks at UNCG are a shared responsibility between Risk Owners and the Office of Enterprise Risk Management. Risk Owners are responsible for documenting risk-related activities in the University's ERM software. This includes periodic updates to risk information, evaluation of risk control effectiveness, and rescoring risk annually.

The Office of Enterprise Risk Management is responsible for using the information documented by risk owners and preparing and presenting comprehensive ERM reports for executive leadership and the Board of Trustees CARL Committee.

Risk Monitoring Schedule

Risks identified, prioritized, and assessed will generate different risk scores depending on their likelihood, velocity, and severity. As a result, some risks may warrant greater levels of monitoring and oversight than others. The Risk Owners are responsible for constantly monitoring the risk they own and providing, at a minimum, an annual update for each risk in the University's ERM software.

Responsibilities

Each component of the enterprise risk management program has distinct and essential responsibilities. The table below identifies each group and its associated responsibilities.

Program Components	Risk Executive	Risk Owner	ERM	ERM Committee	Chancellor's Council	Board of Trustees CARL Committee
Risk Framework and Governance	I	C, I	R, A	R	I	I
Risk Appetite	R	R	R, A	R	A, C	C, I
Risk Identification	R, C, I	R, C, I	R, A, C, I	R, C, I	C, I	I
Risk Assessment	C, I	R, A	R, A, C	R	I	I
Mitigations/Controls	A	R	R, C, I	R, C, I	C, I	C, I
Process Improvement and Training	I	R, C, I	R, A	C, I	I	I
Risk Reporting and Monitoring	A	R	R	R	C, I	C, I

Key
R: Responsible – Performs the action/task
A: Accountable – Accountable that the action/task is completed
C: Consulted – Consulted before, during, and after performing the action/task
I: Informed – Informed before, during, and after performing the action/task

ANNEX 1: ENTERPRISE RISK MANAGEMENT COMMITTEE CHARTER

Purpose

This charter establishes the ongoing Enterprise Risk Management (ERM) process and structure for UNCG. The Enterprise Risk Management Committee (ERMC) facilitates discussion of ERM topics, best practices, and items of inter-departmental concern in the areas of internal controls, safety, risk management, and compliance. The ERMC serves as the primary assembly to facilitate a successful implementation of an enterprise-wide risk management program and enables effective risk mitigation campus-wide in support of UNCG's strategic objectives.

Authority and Background

Section 1300.7 of the UNC Policy Manual (University Enterprise Risk Management and Compliance) requires each constituent institution to establish an ERM process that aligns with the institution's programs, activities, and management systems and that supports the University's strategic and other goals. The ERMC is the University's representative body to identify, monitor, evaluate, and communicate to those in governance significant risks the University faces, along with actions management is taking to ensure effective risk mitigation.

Mission

The ERMC's mission is to provide oversight, guidance, and coordination of university-wide efforts to identify, assess, communicate, manage, monitor, and mitigate risks that may adversely impact the University's strategic goals. The ERMC will collaborate on a holistic strategy to identify and address the full range of risks (strategic, operational, life and health, financial, compliance, and reputational) the University faces.

Although some risks may affect a specific unit or division, risks often are interconnected across the University, and a traditional silo approach to managing these risks is less effective. Systemically sharing institutional knowledge and risks across functions is vital to the ERM process, including embedding an enterprise-wide risk management culture into all our activities. The ERMC fosters this culture by engaging in risk-based discussions and communicating results in both an upward and downward approach.

Responsibilities

The primary responsibilities of the ERM are:

- Engage in and promote ERM discussions across the University to foster a culture of awareness for the risks the University faces and risk management efforts.
- Promote linkage between identified enterprise risks and the University’s strategic plan.
- Develop and maintain the University risk register/inventory.
- Identify the most significant enterprise risks and monitor whether existing risk mitigation actions effectively manage the risks.
- Ensure the top and key emergent risks identified are assigned to responsible risk executives and risk owners to draft Risk Action Plans to be monitored and reviewed by the ERMC.

- Receive periodic updates regarding identified risks and their controls and mitigation efforts, both implemented and planned.
- Periodically review the ERM process to explore opportunities to improve the process for identifying and mitigating enterprise risks.
- Monitor external and internal forces and factors influencing the University's risk enterprise landscape.
- Review this charter and the ERM Framework periodically and update as needed.

Committee Organization

Reporting Structure

The ERMC is a standing committee organized by Enterprise Risk Management, operating under the direction of the Vice Chancellor for Finance and Administration. The committee will function in a review, recommendation, and advisory role for the entire University. The Enterprise Risk Management will report high and emerging risks to the University's Chancellor, Chancellor's Council, Board of Trustees Compliance, Audit, Risk, and Legal (CARL) Committee, and the UNC System Office.

Meetings

The Associate Vice Chancellor for Campus Enterprises, or designee, will chair the ERMC. The Chair or designee will call the meetings quarterly. The date and time may change periodically depending on conflicts with member schedules, and more frequent meetings may be held if deemed necessary. The Associate Vice Chancellor for Campus Enterprises or designee may invite non-committee members with a particular interest or expertise to attend all or portions of ERMC meetings.

Decision Making

A consensus facilitated by the Chair will determine most recommendations and other matters. A simple majority of voting members will decide on issues requiring a vote, as determined by the Chair. Email or other electronic communication (such as Teams) may be used to arrive at a consensus on an issue requiring timely attention and resolution.

Minutes

The Office of Enterprise Risk Management representative will record the minutes from each meeting, and the ERMC will approve the minutes from the prior meeting at each meeting.

Membership and Terms of Office

Each vice chancellor will appoint a member from their division to serve on the committee. Committee members should report directly to the division vice chancellor and be familiar with operational processes and risks within and across their responsibilities. Committee members serve indefinite terms of service at the will of their respective vice chancellor.

Current Membership

The ERMC is comprised of the following representatives:

Division/Area	ERMC Representative	Risk Executive
ERM Committee Chair	Associate Vice Chancellor for Campus Enterprises and Risk Management	-
Academic Affairs	Senior Vice Provost	Provost and Executive Vice Chancellor
Enrollment Management	AVC for Enrollment Management	Vice Chancellor for Enrollment Management
Finance and Administration	Associate Vice Chancellor for Campus Enterprises and Risk Management	Vice Chancellor for Finance and Administration
Information Technology Services	Associate Vice Chancellor for Enterprise Infrastructure	Vice Chancellor for Information Technology Services
Institutional Integrity and General Counsel	Associate General Counsel	Vice Chancellor for Institutional Integrity and General Counsel
Intercollegiate Athletics	Executive Associate Athletic Director	Athletics Director
Research and Engagement	Director for Strategic Initiatives	Vice Chancellor for Research and Engagement
Student Affairs	Associate Vice Chancellor and Dean of Students	Vice Chancellor for Student Affairs
University Advancement	Assistant Vice Chancellor for Advancement Operations	Vice Chancellor for University Advancement
University Communications	Associate Vice Chancellor for University Communications	Vice Chancellor for Strategic Communications
Internal Audit (Non-voting)	Director of Internal Audit	-

ANNEX 2: RISK APPETITE

Overall Risk Appetite

Overall, the University has a balanced risk appetite. As a part of the ERM program framework, the Risk Appetite Statement articulates the amount of risk the University is willing to accept in pursuit of its mission and strategic goals. With clearly defined boundaries, risk appetite varies according to the activity undertaken. Accepting risk is subject to ensuring that potential benefits and risks are understood and measures to mitigate risk are established.

Based upon industry best practices and thought leadership, the UNCG Risk Appetite Statement characterizes the University's appetite for each risk as conservative, balanced, and entrepreneurial, according to the following definition:

- **Conservative** – Little to no tolerance for risks that can negatively impact the University's strategic objectives.
- **Balanced** – Not all risks can be controlled due to internal and external factors. Still, adequate controls are in place to mitigate negative impacts and capitalize on positive effects on the University's strategic objectives.
- **Entrepreneurial** – Capitalize on risks that can positively impact the University's strategic objectives while effectively managing the potential for negative impact.

Strategic Risk

The University's appetite for strategic risk is entrepreneurial. Achievement of the University's mission is not possible without assuming risks in a managed way. Managed risk-taking is encouraged when it enables the pursuit of opportunities that can positively impact the University Mission. Such risk-taking can also result in an unfavorable outcome. In pursuit of the mission, vision, and strategic plan, there is an entrepreneurial appetite for risks that could positively and negatively impact the University.

Operational Risk

The University's appetite for Operational risk is balanced. The operations of a public university are continually exposed to risks that are both internal and external and have the potential to impact service delivery. Effective risk and resiliency management can mitigate many operational risks but not eliminate them. In pursuit of strategic goals toward an ecology of infrastructure and support and efficient and effective business practices, there is a balanced appetite for risks that could impact the opportunity to conduct business as usual due to an event that is either natural or human-caused, planned, or unplanned.

Life and Health

The University's appetite for life and health risk is conservative. The safety of the UNCG community is a top priority of the University. There is a conservative appetite for risks that could expose students, faculty, staff, and visitors to unsafe environments or activities that have the potential to result in severe injury or death, including physical and emotional health and well-being.

Financial Risk

The University's appetite for financial risk is balanced. To maintain its long-term economic sustainability and overall financial strength, the University will maintain strong internal controls and ensure

compliance with applicable governmental and accounting standards. Unpredictable and external factors that have the potential to impact financial resources are challenging to control. In pursuit of the strategic recommendations of efficient and effective business practices, there is a balanced appetite for accepting and taking incremental risks for the long-term benefit of the University's mission and vision.

Compliance

The University's appetite for compliance risk is a blend of conservative and balanced. As a regional leader of higher education, research, and innovation, compliance with federal, state, and local laws and regulations, case law, accreditation standards, university policy and procedures, and contractual obligations is a priority of the University. Changes in the law, regulatory environment, and other unpredictable factors potentially impacting legal/compliance obligations may be difficult to control. In pursuit of the strategic goals, there is a conservative appetite for risks that would suspend programs and institutional activities or subject a community member to legal liability. However, there is also a balanced appetite for risks that impact legal/compliance obligations where the University can demonstrate good faith toward compliance.

Reputational Risk

The University's appetite for reputation risk is balanced. While the health and safety of the UNCG community is the top priority, the reputation of UNCG is one of our most valued assets. To achieve strategic objectives in alignment with the university's mission and values, some risks are necessary to move forward to transform the educational experience, the university community, and our society. However, risks negatively impacting our community will not be pursued. As members of the UNCG community and stewards of the reputation and brand of the institution, there is a balanced appetite toward reputation risk.

ANNEX 3: RISK SCORING GUIDE

Introduction

This Risk Scoring Guide has been created to establish a simplified and consistent methodology for scoring risk at UNCG. Risks are analyzed based on their likelihood, velocity, and impact. To understand the effectiveness of treatments and controls, the risks are rated through two lenses: inherent risk and residual risk. Each scoring factor and lens is defined below.

Scoring Factors

- Likelihood – the probability that a given event will occur.
- Velocity – how quickly the risk could impact UNCG and the reaction time UNCG will have to respond to it once it occurs.
- Impact – the extent to which a risk event might affect the enterprise.

Risk Scoring Lens

- Inherent Risk – the level of risk in place before actions (controls or mitigation measures) are taken to alter the risk's impact or likelihood.
- Residual Risk – the remaining level of risk following the development and implementation of controls or mitigation measures.

Likelihood Reference Chart

Likelihood Measures	Very Low	Low	Moderate	High	Very High
General	• Conceivable but extremely unlikely • Less than 10% probability	• Possible but unlikely • 10% - 40% probability	• Likely to happen • 40% - 60% probability	• Very likely; will probably occur • 60% - 90% probability	• Almost certain; extremely likely • > 90% probability
Peer Experience	• Has not occurred in higher education	• Looming concerns it will happen in higher education	• Has occurred in higher education	• Has occurred recently in higher education	• Has occurred several times recently in higher education
Event Frequency	• Could happen only in extraordinary circumstances	• May happen one time if conditions are favorable	• Happens, but infrequently	• Happens with some regularity	• Happens frequently

Velocity Reference Chart

Velocity Measures	Very Low	Low	Moderate	High	Very High
Time to Impact	• Risk may occur in over a year or more	• Risk may occur in a matter of several months	• Risk may occur in a matter of a few months	• Risk may occur in a matter of days to a couple of weeks	• Risk may occur very rapidly with little or no warning, instantaneous
Reaction Time	• There will be over a year for reaction and response planning before the serious consequences of the risk hit	• There will be several months for reaction and response planning before serious consequences of the risk hit	• There will be a few months for reaction and response planning before serious consequences of the risk hit	• There will be days to a couple of weeks for reaction and response planning before serious consequences of the risk hit	• There will be very little or no time for reaction and response planning before serious consequences of the risk hit

Impact Reference Chart

Impact Type	Insignificant	Minor	Moderate	Major	Severe
Strategic	• Minor impact on business operations • Would not impede the ability to achieve one or more strategic objectives	• Minor, low-resource attention to assess and respond • Easily reconciled in less than 60 days	• Inconsistencies created across strategic planning or priorities • Increased impact of uncertainty upon objectives	• Undermining of strategic objectives • Contradicts one or more strategic objectives or underlying enabling principles	• Derails a strategic objective • Prompts special Governing Board meeting / external audit • Competence questioned
Operational	• Insignificant impact on operations; issue quickly resolved	• Minor and brief impact on non-critical operations • Loss or damage to non-critical assets	• Minor and brief impact on core functions or critical operations • Significant damage to non-critical assets • Damage to critical assets	• Significant impact on core functions or critical operations • Significant damage to critical assets	• Significant, irrecoverable impact on core functions or critical operations • Business interruption leading to other critical consequence impacts • Major loss/destruction of critical assets
Life and Health	• Minor near-miss event • No first aid or medical treatment is required	• First aid injury or illness • Instances of safety practices inconsistent with safety, policy, and procedures at a single location • Hazardous substance release that is contained	• Injury or illness requiring medical intervention or treatment • Reversible, temporary impairment • Widespread staff perception management does not always prioritize safety • Hazardous substance release that has the potential to cause moderate health effects	• Serious injury or illness requiring hospitalization • Permanent impairment with moderate functional restrictions • Management displaying or tolerating unsafe behavior • Hazardous substance release that has the potential to cause serious health effects	• Permanent impairment • Fatality
Financial	• Adverse impact of <$100K	• Adverse impact of $100K-$1M	• Adverse impact of $1M-$10M	• Adverse impact of $10M-$20M	• Adverse impact of >$20M
Compliance	• Breach of standard operating procedures but not of any mandatory policies or procedures	• Ad hoc, as opposed to systemic; breaches of policies and procedures but not of laws or regulations	• Breach of any laws/licenses, including a notifiable breach resulting in recommendations and active monitoring by regulator • Instances of breach of Operational Policies	• Prosecution • Penalties < $1M • Show cause notice from the regulator or accreditor • Enforceable undertaking • Significant and systemic breach of policies	• Criminal prosecution • Penalties > $1M • Loss of critical license/accreditation • Significant and system breach of Governance policies
Reputational	• Negligible impact; ad hoc mentions or rumors of a negative event on social media	• Adverse local and social media coverage for a brief time • Small pockets of student protests	• Adverse statewide media coverage • Students and staff publicly express their disapproval and disappointment	• Adverse and sustained state media coverage; public perception of UNCG suffers • Calls for management reform, including the removal of some administrators • Key stakeholders threaten to remove their association and support for UNCG	• Prolonged and adverse national media coverage undermining public confidence in UNCG • Major student uprisings; calls for government intervention; administrators publicly chastised by community leaders • Key stakeholders disassociate themselves from UNCG

APPENDIX A: KEY TERMS

Compliance, Audit, Risk, and Legal Affairs (CARL) Committee: A Board of Trustees committee that provides oversight and assistance to the University in its efforts to promote a culture of compliance; ensure the timely development of operational policies and procedures that are consistent with relevant laws and regulations; and promote collaboration among and between compliance, audit, risk management, legal, and ethical functions at the University.

Enterprise Risk Management[1]: A business continuous process, led by senior leadership, that extends the concepts of risk management and includes identifying risks across the entire enterprise; assessing the impact of risks to the operations and mission; developing and practicing response of mitigation plans; monitoring the identified risks, holding the risk owner accountable, and consistently scanning for emerging risks.

Enterprise Risk Management Committee: Part of the first line of defense that gathers regularly to execute the ERM framework on behalf of its risk owner.

First Line of Defense: The operational or business unit that conducts University operations daily and manages risk by implementing and maintaining effective internal control procedures.

Inherent Risk: Risk to the organization without any controls or mitigation efforts to alter the risk's likelihood or impact.

Key Performance Indicator: Metric that measures performance or the achievement of targets.

Key Risk Indicator: Metric that provides information on the level of exposure to a given risk that the organization has at a particular time.

Lines of Defense: a framework designed to identify the roles and responsibilities of business units and ongoing practice of risk management and sustain risk management activities.

Mitigation: Controls, tools, and other mechanisms that are being applied to help manage the risk from becoming an issue.

Residual Risk: The level of risk that remains after controls and mitigation activities have been applied.

Risk: An event or action that impacts an organization's ability to achieve its objectives, whether positive, negative, or a combination of both.

Risk Agility: The ability to alter and adapt risk management infrastructure to respond quickly to a changing environment or organizational disruption.

Risk Appetite: Articulates the amount of risk the University is willing to accept in pursuit of its mission and strategic goals.

[1] Adopted from Risk Management – An Accountability Guide for University and College Boards. 2013 Association of Governing Boards of Universities and Colleges

Risk Assessment: The systemic process of identifying and evaluating potential risks that may be involved in a projected activity or undertaking.

Risk Owner: Typically, a senior management-level individual who is one level below the Risk Executive. This person may be responsible for coordinating the mitigation and monitoring activities and have direct oversight and knowledge of the risk.

Risk Likelihood: The probability that a given event will occur.

Risk Impact: The extent to which a risk event might affect the enterprise.

Second Line of Defense: Consists of ERM function that establishes processes and procedures to ensure the organization operates within its target risk appetite, monitors the overall risk profile, and recommends action when the risk falls outside the tolerance levels approved by the board and executive management.

Third Line of Defense: Internal Audit is the third line of defense and provides independent assurance of the first and second lines of defense.

APPENDIX B: RECORD OF REVISIONS

It is necessary to review and update this Framework regularly. The Office of Enterprise Risk Management will coordinate all Framework review and revision efforts. Table 1 below identifies the changes made to this Framework since it was initially implemented.

Table 1. Documented Changes to the Framework

Date	Part(s) Affected	Item Changed	Revised By