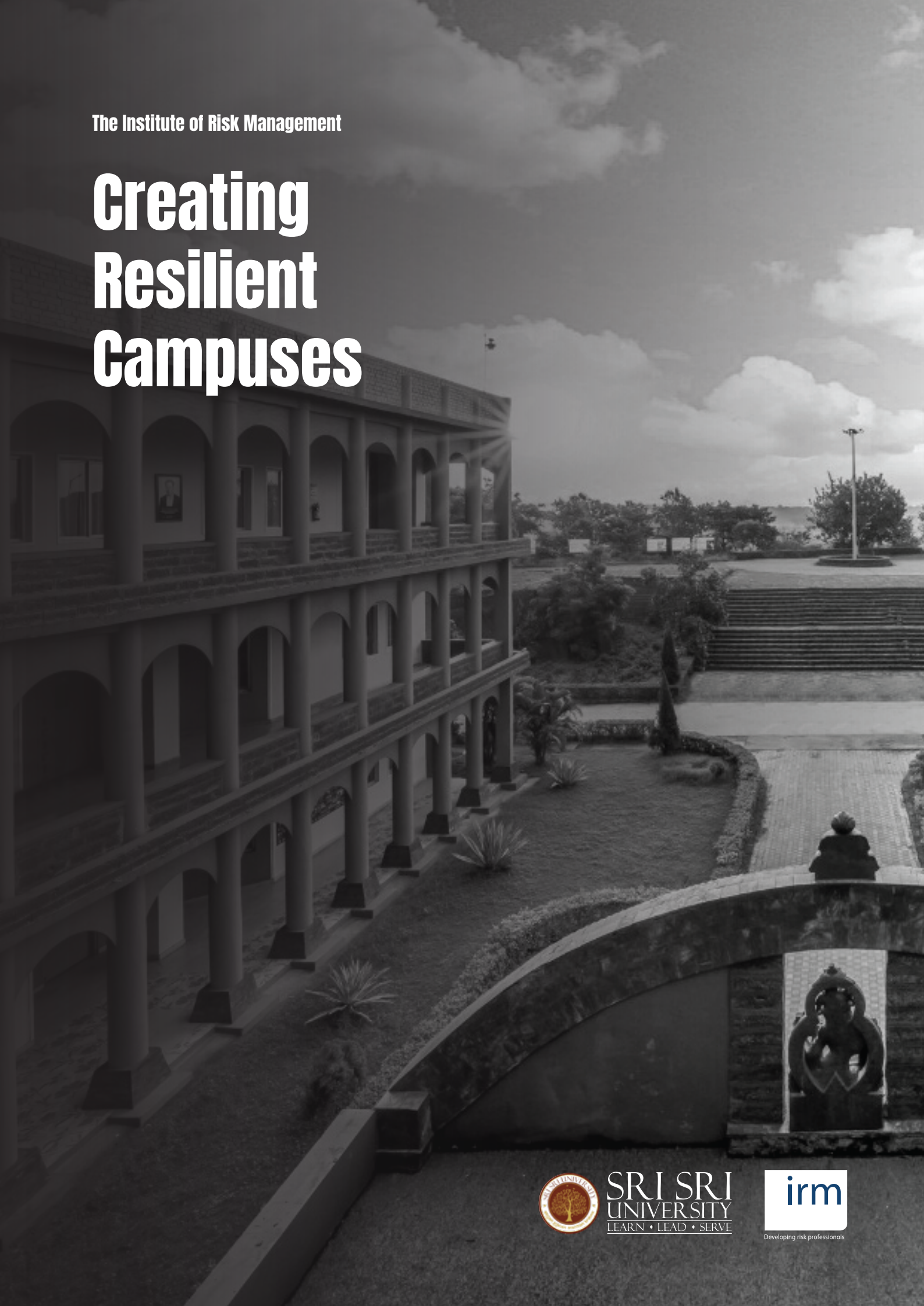
The Institute of Risk Management

Creating Resilient Campuses



SRI SRI UNIVERSITY
LEARN • LEAD • SERVE

irm
Developing risk professionals

Disclaimer

Executive Summary

Higher Education Institutions (HEIs) in India operate in an increasingly complex environment marked by rapid regulatory changes, technological advancements, funding challenges, and unexpected crises. These dynamics expose universities to a wide array of risks that can threaten their strategic objectives, finances, reputation, and the safety of students and staff. Building resilience in this sector requires a proactive and structured approach to Enterprise Risk Management (ERM) – a holistic framework for identifying, assessing, and managing risks and opportunities across an organization.

In practical terms, this means that risk considerations become part of the institutional culture and "business as usual" processes, rather than an isolated administrative task.

A robust ERM program is based on the following principles –

- Governance and Culture - Oversight responsibilities for ERM at the board and senior management level.
- Strategy and Objective-Setting - Risk information informs strategy and performance management.
- Review and Revision – ERM components are monitored and adjusted based on outcomes.
- Information, Communication, and Reporting - Sharing of timely risk information across the organization.

Universities can undertake the following initiatives to foster a strong risk culture -

- Consistently messaging the importance of managing risks.
- Defining the risk appetite that articulates the amount and type of risk the university is prepared to pursue or retain.
- Encouraging an open culture where concerns are discussed without fear of blame.
- Understanding the root causes of incidents and improving systems.
- Conducting regular workshops or online training on basic risk management concepts for faculty and staff.
- Getting students involved in risk initiatives to amplify culture.

In the Indian context, regulators such as the University Grants Commission (UGC) and National Assessment and Accreditation Council (NAAC) are increasingly focused on good governance practices, though explicit ERM mandates in higher education need to still emerge.

By voluntarily adopting ERM, Indian universities can stay ahead of regulatory curves, demonstrate accountability and achieve their goals sustainably.

TABLE OF CONTENTS

ABBREVIATIONS

AI	Artificial Intelligence
AICTE	All India Council for Technical Education
ARO	Academic Risk Observatory
CCTV	Closed Circuit Television
CIO	Chief Information Officer
CRO	Chief Risk Officer
COSO 2017	Committee of Sponsoring Organizations of the Treadway Commission's Enterprise Risk Management framework updated in the year 2017
COVID-19	Coronavirus disease of 2019
ERM	Enterprise Risk Management
ERP	Enterprise Resource Planning
EU	European Union
GDPR	The General Data Protection Regulation
GST	The Goods and Services Tax
HEI	Higher Education Institutions
HR	Human Resources
HVAC	Heating, Ventilation, and Air Conditioning system
IA	Internal Audit
IRM	Institute of Risk Management
ISO 31000	International Organization for Standardization – Risk Management
IP	Intellectual Property
IT	Information Technology
KPI	Key Performance Indicator
KRI	Key Risk Indicator
LMS	Learning Management System
MBA	Master of Business Administration
NAAC	National Assessment and Accreditation Council
NBA	National Board of Accreditation
NCAA	The National Collegiate Athletic Association
NEP 2020	The National Education Policy of India introduced in the year 2020
NIRF	The National Institutional Ranking Framework
NRFE	National Risk Framework for Education
POSH	The Sexual Harassment of Women at Workplace (Prevention, Prohibition, and Redressal) Act, 2013
PPE	Personal Protective Equipment
RACI Matrix	A responsibility assignment matrix
RIMS	The Risk and Insurance Management Society, Inc.
RMC	Risk Management Committee
RUSA	Rashtriya Uchchattar Shiksha Abhiyan
SEBI	Securities and Exchange Board of India

SOP	Standard Operating Procedure
TOR	Terms of Reference
UBIT	Unrelated Business Income Tax
UGC	University Grants Commission
URMIA	University Risk Management and Insurance Association
VUCA	The volatility, uncertainty, complexity and ambiguity of general conditions and situations

CHAPTER 1 - INTRODUCTION

Higher Education Institutions (HEIs) in India operate in an increasingly complex environment marked by rapid regulatory changes, technological advancements, funding challenges, and unexpected crises (such as the COVID-19 pandemic). These dynamics expose universities to a wide array of risks that can threaten their strategic objectives, finances, reputation, and the safety of students and staff. Building resilience in this sector requires a proactive and structured approach to Enterprise Risk Management (ERM) – a holistic framework for identifying, assessing, and managing risks and opportunities across an organization. This white paper presents a comprehensive step-by-step guide to implementing ERM in Indian universities, with the aim of strengthening governance and sustainability in higher education.

For regulatory bodies and university leadership, understanding ERM is essential. ERM is more than a compliance checkbox; it is a strategic tool to ensure institutional objectives are achieved with controlled risk exposure. When implemented effectively, ERM helps universities to anticipate and mitigate potential threats, while also enabling them to confidently pursue opportunities aligned with their mission. Global best practices in ERM, codified in frameworks like ISO 31000 and COSO ERM 2017, emphasize that risk management should be integrated into all aspects of decision-making and campus operations. In practical terms, this means that risk considerations become part of the institutional culture and "business as usual" processes, rather than an isolated administrative task. A robust ERM program ensures that: (1) risks (and opportunities) are discussed at the highest levels of governance, (2) a culture of risk awareness permeates the institution, (3) both negative and positive aspects of risk are considered (avoiding purely reactive thinking), and (4) risk information informs strategy and performance management. These outcomes are particularly crucial in higher education, where stakeholder expectations (students, parents, regulators, funding bodies) for accountability and continuity are high.

CHAPTER 2 - UNDERSTANDING ERM FRAMEWORKS FOR HIGHER EDUCATION

Before diving into the implementation roadmap, it is important to understand the foundational frameworks and standards that inform effective ERM. The three primary references for this guide are ISO 31000:2018, COSO ERM 2017, and relevant guidance from the Institute of Risk Management (IRM). Aligning an ERM program with these globally recognized frameworks ensures that the approach is robust, standardized, and in line with proven best practices.

Figure 1

1. **ISO 31000 (Risk Management – Guidelines):** ISO 31000 is an international standard providing high-level principles and a generic process for risk management applicable to any organization, including universities. In essence, ISO 31000 outlines a comprehensive approach to identifying, analysing, evaluating, treating, monitoring, and communicating risks across an organization. It emphasizes that risk management should be integrated (part of all organizational processes), structured and comprehensive, customized (tailored to the organization's context), and inclusive (engaging stakeholders). ISO 31000's framework includes: ensuring leadership and commitment, designing a fit-for-purpose risk management framework, and continuously improving. The standard's risk management process (which we will follow in our roadmap) involves iterative steps: communication and consultation with stakeholders, establishing the context (internal and external context, and criteria for risk assessment), risk assessment (risk identification, analysis, and evaluation), risk treatment, and ongoing monitoring and review of risks. This process is often depicted as a cycle, reinforcing that risk management is not a one-time project but a continuous journey.

2. **COSO ERM 2017 (Integrating with Strategy and Performance):** The COSO ERM framework, updated in 2017, is particularly useful for aligning risk management with an organization's strategic management. Developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in partnership with PwC, this framework highlights the importance of embedding risk considerations into strategic planning and execution. COSO defines ERM as "the culture, capabilities, and practices integrated with strategy-setting and performance that organizations rely on to manage risk in creating, preserving, and realizing value." A key feature of COSO 2017 is its focus on how risk management drives value – not just preventing losses but also enabling

better decision-making. The framework is organized into five interrelated components, each with a set of principles:

1. **Governance and Culture** – Sets the tone at the top. This component establishes oversight responsibilities for ERM at the board and senior management level and emphasizes ethical values and desired behaviours. A good governance structure reinforces the importance of risk management and ensures a risk-aware culture throughout the institution. (For example, a university's board of governors should actively discuss major risks, and leadership should model prudent risk-taking aligned with the university's values.)

2. **Strategy and Objective-Setting** – Aligns ERM with mission and planning. Risk management is integrated into the strategic planning process – when universities set their strategic goals (academic programs, research initiatives, expansion plans, etc.), they also establish their risk appetite and consider risks to those objectives. According to COSO, risk appetite must be established and aligned with strategy; the institution's business objectives then serve as a basis for identifying and assessing risks. In a university context, this means, for instance, if an institution has an objective to launch online programs, it should concurrently assess the risks (technology, quality, competition) and clarify how much risk it is willing to accept in pursuit of that objective.

3. **Performance** – Implements risk management in practice. This involves identifying and assessing risks that could impact the achievement of objectives, prioritizing risks by severity (in light of the defined risk appetite), and selecting risk responses. For a university, "performance" means during operations – whether academic, financial, or operational – risks are continuously identified (e.g., dropping enrolment, funding cuts, data breaches) and evaluated. Risk responses might include accepting the risk, avoiding, reducing (mitigating), or sharing it (e.g., via insurance). COSO also encourages taking a "portfolio view" – looking at the university's risk profile as a whole, rather than siloed lists, to understand aggregate exposure.

4. **Review and Revision** – Reflects on performance and change. Universities should periodically review how well their ERM components are functioning and make adjustments. This means monitoring outcomes (did our risk mitigations for this year work? did any new risks emerge?) and learning from incidents or near-misses. For example, if a university's risk reviews show that many departments struggled with IT outages, that might signal a need to revise the IT risk mitigation strategy or invest more in infrastructure.

5. **Information, Communication, and Reporting** – Supports ERM with information flows. Effective ERM requires continual gathering and sharing of timely risk information across the organization. In a university, this could involve reporting top risks and mitigation status to the Board/Risk Committee quarterly, internal communications about new policies or incidents to relevant faculty and staff, and even communicating certain risks to students or external stakeholders when appropriate. Both internal channels (like risk dashboards to management) and external disclosures (perhaps in annual reports or accreditation self-studies) fall under this component.

- By aligning with the COSO components, a university ensures that risk management isn't an adjunct activity but is interwoven with governance, strategy, operations, and feedback loops of the institution. Throughout this guide, we will cross-reference how

each step corresponds to these components (e.g., establishing governance structures maps to Governance & Culture; setting risk appetite is part of Strategy & Objective-Setting; the risk assessment process is under Performance, etc.).

- **IRM Guidance (Risk Culture, Appetite, and more):** The Institute of Risk Management (IRM) has produced practical guidance that is highly relevant for cultivating the qualitative aspects of ERM, especially in non-profit and educational contexts. Two key pieces from IRM are the Risk Culture: Resources for Practitioners guide and the Risk Appetite & Tolerance Guide.

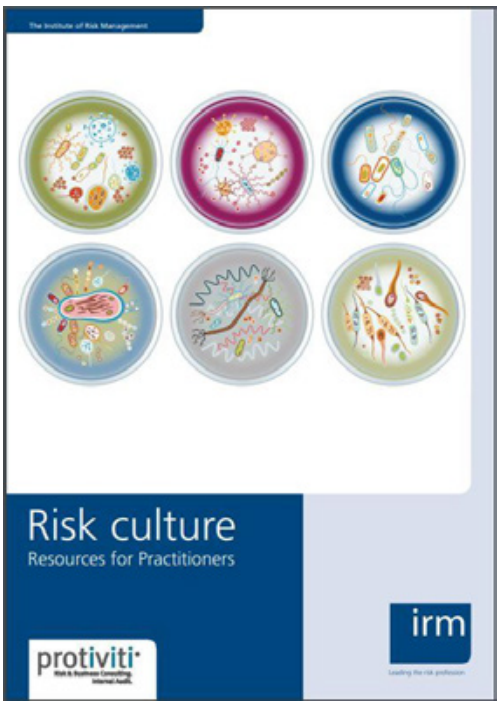


Figure 2: IRM's Risk Culture: Resources for Practitioners Guide

Risk Culture: IRM defines risk culture as "the values, beliefs, knowledge, attitudes and understanding about risk shared by a group of people with a common purpose". In a university, this "group" is the entire campus community – from the board and vice-chancellor, down to faculty, administrators, and even students. A strong risk culture means that people are aware of risks, openly communicate about uncertainties, and make decisions in line with the institution's risk management expectations. IRM emphasizes that an effective risk culture enables and rewards individuals for taking the right risks in an informed manner. For example, faculty might feel empowered to start innovative research programs (which carry some risk) because they know there are processes to manage research ethics and funding risks, whereas they would avoid reckless actions like bypassing lab safety protocols because the culture does not tolerate it. We will later discuss techniques to assess and improve risk culture (such as tone at the top, training, and incentive alignment).

Risk Appetite and Tolerance: According to IRM and other governance codes, the principle of risk appetite emanates from the Board – it is a core responsibility of top leadership to articulate how much risk the institution is willing to accept in pursuit of its objectives. The

IRM guidance (2011) helped demystify this concept by encouraging organizations to develop a risk appetite framework that includes clear risk appetite statements and measures. In practice, for a university, this might mean the Board issues a statement like: "We have a low appetite for risks that compromise student safety or academic integrity, a moderate appetite for strategic growth initiatives (new programs, campuses) with strong controls, and a high appetite for innovative research that could fail but offers high impact, provided compliance and ethical safeguards are in place." Such statements give direction to management when making decisions. IRM also differentiates risk tolerance – often defined as the acceptable variance in outcomes or the boundaries of risk-taking (the thresholds beyond which the university must not go). For instance, while a university might accept fluctuations in annual research funding (say ±10%), it might set a hard tolerance that it will not incur a deficit beyond a certain amount or breach specific regulatory requirements. By providing "questions for the boardroom" and practical examples, IRM's guidance helps ensure the concept of risk appetite is not nebulous but a living part of governance. In our roadmap, we will incorporate steps to define and approve a risk appetite statement aligned to IRM and COSO recommendations.

In summary, these frameworks are mutually reinforcing: ISO 31000 gives a high-level process and principles (a universal language for risk), COSO ERM provides a structural and strategic alignment perspective, and IRM offers deep dives into culture and appetite which are particularly useful in shaping behaviours and governance in an academic institution. An ERM program for Indian higher education that aligns with ISO 31000 and COSO will meet international standards of rigor, while incorporating IRM's insights will help ensure the program is genuinely effective in practice (since culture and clear appetite are often where organizations falter).

Case Study: Learning from a Crisis

Problem Statement

A scramble to manage IT capacity, cybersecurity for remote access, health regulations, and financial strain from decreased revenue during a pandemic.

Context

In 2020, "Global Tech University" (the name of the institute has been masked to preserve anonymity) faced a sudden shift to online learning due to a pandemic. The university had never formalized its risk management processes. In contrast, another institution, "Sunrise University," had an ERM framework in place – they had earlier identified "pandemic/health crisis" as a strategic risk and developed contingency plans. When COVID-19 hit, Sunrise University activated its risk response plans (for example, scaling up online infrastructure and adjusting budgets), enabling a smoother pivot to online classes and timely communication with stakeholders.

Learning Outcomes

This contrast highlights how universities with proactive ERM were more resilient in the face of a crisis, underlining the need for all HEIs to build similar preparedness.

Case Study: Adapting a Global Framework

Problem Statement

Costly failure involving a major IT breach and a failed overseas partnership due to poor decision-making in a high-risk international project.

Context

Consider "Western University" (the name of the institute has been masked to preserve anonymity) which decided to formalize its risk management following a series of incidents (a major IT breach and a failed overseas partnership). They aligned their new ERM policy with ISO 31000 and COSO. Using ISO 31000, they established a standard risk process and taxonomy. From COSO, they adopted the idea of linking risks to strategic objectives – when discussing a new campus, they explicitly considered risks (financial vi ability, reputational impact, regulatory approvals) as part of strategy setting. They also leveraged IRM guidance: the Board undertook a workshop to articulate its risk appetite, clearly stating the university's stance on key risk areas, and rolled out a "risk culture" survey to faculty and staff. Within a year, Western University's risk reports became far more focused, and the governance committee observed better decision-making – for instance, a high-risk international project was paused after evaluation, saving the university from a potential costly failure.

Learning Outcomes

This example shows how combining ISO, COSO, and IRM best practices can create a robust ERM approach tailored for a university.

CHAPTER 3 - ESTABLISHING ERM GOVERNANCE IN UNIVERSITIES

A critical foundation for ERM success is the governance structure – in other words, the people, roles, and committees that will drive and oversee risk management. In a university setting, this typically involves appointing a dedicated risk leader (such as a Chief Risk Officer (CRO) or equivalent) and setting up a Risk Management Committee (RMC) or similar governance bodies at various levels. Good governance ensures that ERM is championed from the top and that there are clear lines of accountability for managing risks. This section outlines how Indian HEIs can establish such structures, drawing on IRM recommendations and global best practices.

Chief Risk Officer (CRO) – Selecting a Qualified Risk Leader: Universities should designate a senior official to lead the ERM initiative. The title may vary (some institutions call it Director of Risk Management, Chief Risk & Compliance Officer, etc.), but we will use CRO for simplicity. It is highly recommended that this individual be professionally qualified in risk management, for credibility and expertise. For example, candidates who have certifications from IRM (such as the IRM Diploma or Level 5 Certificate) or similar credentials can be ideal, as they possess a strong grasp of ERM frameworks and ethics. An "IRM-qualified" CRO – meaning someone who has met the rigorous standards of the Institute of Risk Management – can bring global best practices to the local context. The CRO should ideally report to the highest levels of the institution: either directly to the Vice-Chancellor/Director or to a Board committee (to ensure independence and authority). In some universities, the CRO role might be combined with other functions like compliance or internal audit, especially if resources are limited, but care must be taken to avoid conflicts of interest and overload. The CRO's key responsibilities will include developing the risk management framework, facilitating risk assessment processes, advising leadership on risk responses, and preparing risk reports for decision-makers.

A strong reporting line is essential. It is advisable that the CRO has direct access to the Board (or its relevant sub-committee) for escalations. In global practice, many universities have the CRO or risk leader periodically present a Top Risk Report to the Board of Trustees/Governing Body. This ensures the governing board is informed and can exercise oversight. As noted in a higher education risk management resource, one should clearly define who provides risk reports to the board – whether it's the president or the CRO – and what those reports should contain. For example, a quarterly risk update might be given by the CRO to the Board's Audit and Risk Committee, highlighting the five to ten most significant risks, their status, and management's actions.

Risk Management Committees (RMCs): Establishing one or more committees to govern risk management is a key step. Typically, universities might have:

- A Board-level Risk Committee (often combined with Audit in some cases, e.g., "Audit and Risk Committee"). This committee, comprising board members (and sometimes external experts), sets risk policy, approves the risk appetite, and monitors top strategic risks. It ensures that management is properly managing risks and can call for deep-dives on specific issues (like cybersecurity or lab safety) as needed. The Board Risk Committee in effect provides oversight and accountability, ensuring ERM stays on the leadership agenda.

- An Executive Risk Management Committee (management-level). This would consist of senior administrators (VC/President, Deans, CFO, Provost, Registrar, etc.) and is chaired by a top executive (for instance, the Vice-Chancellor or a Deputy VC). The CRO usually serves as the secretary or facilitator of this committee. The role of the executive RMC is to discuss and prioritize risks from across the institution, review risk mitigation plans, and resolve inter-departmental issues. It operates as a decision-making body that integrates risk information into management processes. In effect, it is where "silo" risks are brought to a central table and viewed collectively. Some universities call this the "ERM Steering Committee" or "Risk Council." For example, Winston-Salem State University (USA) instituted an ERM Steering Committee chaired by a senior official to coordinate ERM implementation and facilitate reporting to the Chancellor and Board committee.

- **Departmental or Functional Risk Committees/Owners:** While not always formalized as committees, it's important that each faculty or department identifies a "risk champion" or risk owner. Risk owners are responsible for specific risks within their remit (e.g., the IT Director is the owner of technology-related risks, the Dean of Students owns student welfare risks). They may convene their own teams to assess and manage risks operationally. The network of risk owners forms the first line of defence in the university's risk governance (more on the "three lines of defence" concept later). These individuals periodically report up to the Executive RMC about their risk status. A clear definition of roles at this level ensures that risk management activities (like maintaining risk registers and implementing controls) actually happen and are not solely the CRO's burden.

It is crucial to document the charters/terms of reference for each of these committees so everyone understands their duties. For instance, the Board Risk Committee's charter would spell out its authority to review major risks and the requirement that management reports to it. The executive RMC's terms might include meeting frequency, quorum, and its scope (enterprise-wide risks, not minor operational issues). A noted best practice is that internal audit's role should also be clarified in relation to ERM. Internal Audit typically does not own risks, but provides assurance on risk management processes. Some guidance suggests including Internal Audit as a non-voting participant or observer in risk committee meetings to ensure alignment and to allow Audit to factor top risks into their audit plans.

Structure and Reporting Lines: Figure 3 below illustrates a typical governance structure for ERM in a university.

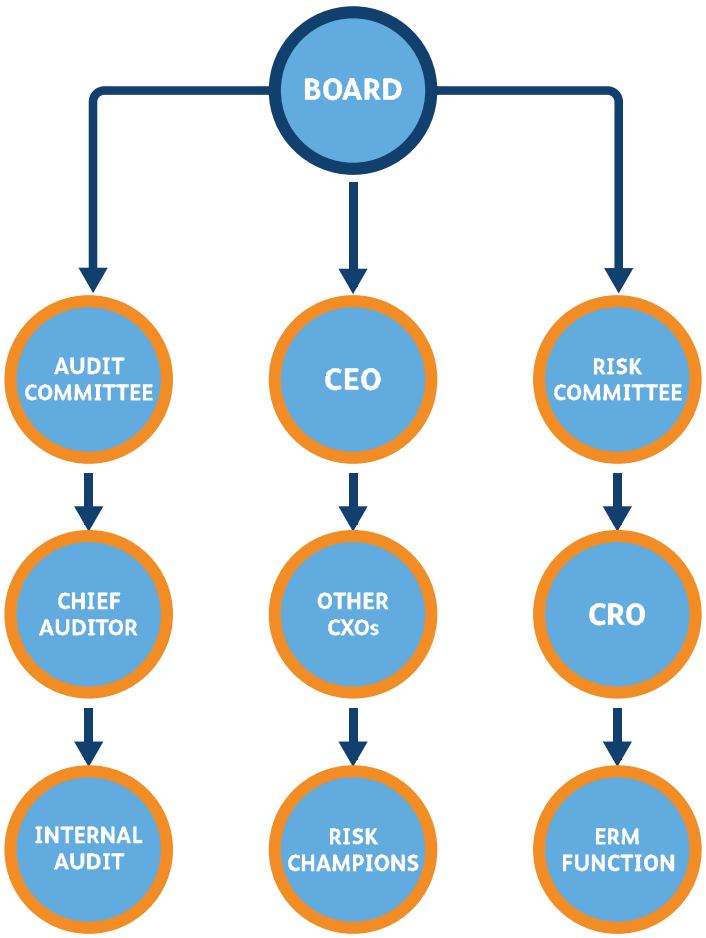


Figure 3: Typical reporting structure for ERM in a university

The CRO and the Executive RMC form the bridge between the operational side and the Board oversight. The CRO coordinates with risk owners across departments (first line), and also works closely with compliance or internal audit functions (second/third line) to gather information and validate controls. The CRO regularly reports to the Board Audit/Risk Committee, which in turn reports to the full Board of Governors on risk exposures and strategies. This multi-tier structure ensures a flow of information: bottom-up (risks identified at ground level are escalated) and top-down (strategic guidance and risk appetite from the Board are communicated down).

No single model fits all. Smaller colleges might merge some of these roles (e.g., one committee might handle both risk and compliance), whereas a large multi-campus university might have sub-committees (like a lab safety committee, IT risk committee) feeding into the central ERM framework. The key is that accountability is assigned – every significant risk should have an owner; every risk mitigation action should have someone responsible and a timeline. Many universities codify this in a Risk Management Policy document, approved by the Board, which officially establishes the CRO role, committees, and responsibilities.

Case Study: Governance in Action

Problem Statement

Data breach at a university due to IT and data security risks being underestimated when viewed in silos.

Context

"Coastal State University" (the name of the institute has been masked to preserve anonymity) decided to strengthen its risk governance after a government audit found gaps in how the university managed financial and compliance risks. They appointed their first ever Chief Risk Officer, who held an IRM certification, to bring expertise. A Board Risk Committee was created, chaired by a prominent independent board member with finance experience. The CRO set up a bi-monthly Management Risk Committee including the Vice Chancellor, Registrar, Deans, and the student affairs head. Early on, this committee found that IT and data security risks were being underestimated in silos – the CIO reported that while they had cybersecurity measures, there was no campus-wide incident response plan. With the committee's backing, the CRO got approval to form a cross-departmental task force to create a cyber risk response plan. A few months later, when a neighbouring university suffered a data breach, Coastal State was able to say, "our Board and management are aware and we have a plan tested," reassuring stakeholders.

Learning Outcomes

This demonstrates how having the right governance structure leads to proactive risk management. The CRO's presence ensured someone was always "on point" for risk, and the committees provided forums to surface and address issues that previously fell through cracks.

CHAPTER 4 - EMBEDDING RISK CULTURE AND DEFINING RISK APPETITE

With governance structures in place, the next foundational step is embedding a supportive risk culture and clarifying the institution's risk appetite and tolerance. These elements set the qualitative environment in which the more technical steps of ERM (risk assessment, mitigation, etc.) will operate. A positive risk culture and clear appetite ensure that ERM is not just a paperwork exercise but actually influences day-to-day decisions and behaviours in the university.

Risk Culture in Higher Education: University culture can be quite decentralized – faculty, administrators, and students each have their own perspectives and may operate with a high degree of autonomy. Embedding risk management into this culture means cultivating awareness and responsibility for risk at all levels. According to IRM, risk culture is about shared values and attitudes toward risk. Some indicators of a strong risk culture in a university include:

- Leadership (Board and Vice-Chancellor) consistently messaging the importance of managing risks and not surprising the institution with unmanaged exposures.
- **Openness in communication:** staff and faculty feel comfortable escalating concerns (e.g., a professor reporting a potential conflict of interest in a research funding, or a hostel warden flagging a safety hazard) without fear of blame. "Bad news" should travel upward quickly.
- Incentives and evaluations that include risk management. For instance, managers might have in their performance objectives something related to risk (like maintaining compliance or implementing internal controls in their department).
- **Widespread participation in risk activities:** if the CRO calls for input on the risk register, many departments respond earnestly; if a training on risk management or crisis management is offered, people attend and engage.
- **Learning from past mistakes:** after an incident (say a lab accident or an exam data leak), the institution focuses on understanding root causes and improving systems, rather than just punishing individuals or sweeping it under the rug. This "just culture" approach encourages transparency.

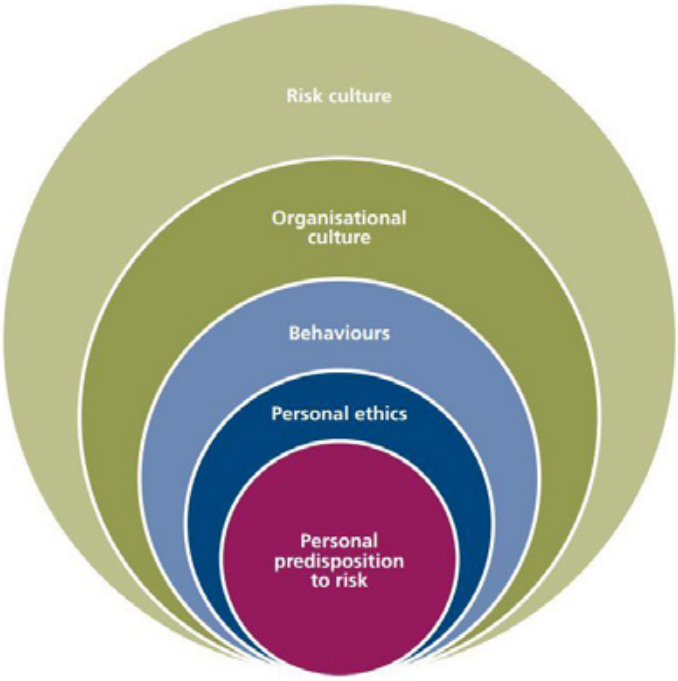


Figure 4: IRMs Risk Culture Framework

To foster this culture, universities can undertake several initiatives:

- **Training & Awareness:** Conduct regular workshops or online training on basic risk management concepts for faculty and staff. For example, a session on "risk management 101 for department heads" where they learn how to identify and assess risks in their context. Another useful practice is tabletop simulations – e.g., simulate a crisis (like a campus flood or IT breach) with the leadership team to reinforce roles and the value of preparedness.

- **Integrate into Academic Governance:** Many universities have Academic Councils or Senates for academic decisions. Ensuring that risk is considered in those deliberations (like adding a section in proposals for new programs, "What are the risks and how will they be managed?") builds culture. Some universities require a risk assessment as part of any major proposal or policy change submitted to the Senate or Board.

- **Student Involvement:** Though students are transient stakeholders, their involvement can amplify culture. For example, including a student representative in the risk committee or getting student unions involved in certain risk initiatives (like campus safety awareness) can spread the culture to the broader student body.

- **Measure the Culture:** IRM suggests using tools like risk culture surveys or scorecards. The university can periodically survey staff on questions like "Do you feel you can report risks without fear?" and "Do you understand how the university handles risks?" The results can highlight areas to improve (maybe people don't know the reporting channels, etc.). Benchmarking these over time can show if culture is getting stronger.

Risk Appetite and Tolerance for HEIs: Defining risk appetite is a governance exercise that has practical downstream effects. A risk appetite statement articulates the amount and type of risk the university is prepared to pursue or retain. It is usually qualitative, possibly supported by some quantitative metrics. As noted earlier, COSO and IRM both place responsibility on the board and top management to set the risk appetite. Here's how an institution might approach it:

- **Categorize by Risk Type:** It can be helpful to express appetite in categories (aligned with the risk taxonomy we'll discuss). For example:

  - **Strategic/Performance Risks**: Appetite could be moderate – willing to take risks in innovation or expansion if they promise high rewards and align with strategy (like starting a new research centre in a cutting-edge field), but only after careful evaluation.

  - **Financial Risks:** Perhaps low appetite for anything that jeopardizes financial sustainability. This might translate to rules like not taking on debt beyond a certain ratio, or requiring a robust business plan for any new venture.

  - **Compliance Risks:** Likely very low appetite – the university does not tolerate breaches of laws/regulations or violations of ethical standards (like academic misconduct).

  - **Safety Risks:** Very low appetite – student and staff safety is paramount, so risks to physical safety or health must be minimized. The university might state it has zero tolerance for risks that can lead to loss of life or severe harm (meaning all such risks must have strong controls).

  - **Reputational Risks:** Often framed as low appetite, since reputation once lost is hard to regain. But since reputation is usually an outcome of other risks (as United Educators cautions, "reputation" itself isn't a standalone risk), the appetite statement might note that the university places high value on maintaining trust and thus will avoid actions that could seriously damage its reputation (for instance, dealing with partners that conflict with its values).

- **Use Scales and Thresholds:** Alongside qualitative statements, some use a numeric scale for appetite – e.g., a 1 to 5 scale where 1 = very low appetite and 5 = very high. Management can then tag each risk with the appetite level. Tolerance thresholds can also be set: for instance, "We target maintaining a minimum cash reserve of ₹X (tolerance threshold), and will not go below that except under extraordinary approved circumstances," which caps financial risk.

- **Approval and Communication:** The draft risk appetite statement should be discussed by the executive leadership and then approved by the Board. It becomes a guiding document. Communicate it across the university (maybe through a policy portal or announcements) so that everyone is aware. It's helpful to give concrete examples in communication – like "Under our risk appetite, initiating collaborations with reputable international universities is within appetite, but entering contracts with unproven partners in high-risk countries would likely be outside our risk tolerance without special due diligence."

- **Risk Appetite in Practice**: Once defined, the appetite should be used when making decisions and in risk assessments. When evaluating a risk, managers should note if it's within or outside appetite. For example, if a risk (say, data privacy risk of a new app) is rated high and beyond the university's stated appetite (because it could violate privacy laws which we said we have zero tolerance for), that's a signal to either not proceed or implement stronger controls until the risk is within acceptable range. IRM's guidance provides "questions for the boardroom" to ensure this happens – e.g., are decisions systematically referencing the risk appetite?

One tool to operationalize risk appetite is a risk rating matrix with appetite lines. Often organizations define what level of risk requires escalation. For instance, on a red-amber-green heat map, any Red (high) risk that is outside tolerance must be reported to the Board and have a mitigation plan that will reduce it within a defined period. Medium (Amber) risks might be acceptable if monitored by management, and Green are largely acceptable as-is. We can incorporate such criteria in the risk management framework. Below is an example of how risk levels might tie to actions:

Risk Level	Risk Score Range (Example)	Action/Response
High (Red)	> 20 (Severe)	Immediate action required. Notify top management and Board; detailed mitigation plan to reduce risk. No new initiatives should push risk here without Board approval.
Medium (Amber)	10–20 (Moderate)	Management attention needed. Implement controls and monitor frequently. Acceptable if kept under review by the Risk Committee.
Low (Green)	< 10 (Low)	Manage through routine procedures. Minimal oversight needed; keep on watch list in case of changes.

Table: Illustrative risk level definitions linked to risk appetite. Each university should customize thresholds and actions. For example, a very risk-averse university might treat anything above "Medium" as needing Board notice, whereas a more risk-seeking research institute might accept more High risks in pursuit of innovation (with understanding of potential losses).

Case Study: Crafting a Risk Appetite Statement

Problem Statement

Lack of clarity due to an undefined risk appetite statement causes knee jerk reactions during controversies.

Context

"Northern University" (the name of the institute has been masked to preserve anonymity) underwent an exercise with its Board. Initially, discussions were abstract, but the IRM qualified CRO facilitated by using scenarios: e.g., "If we had an opportunity to double our research funding by partnering with a private corporation but risk a conflict of interest, would we do it?" The varied responses helped pinpoint appetite. Ultimately, the Board agreed on a formal statement: they have zero tolerance for risks impacting health, safety, ethics, or compliance, a low appetite for financial risks (they set a max deficit tolerance of 2% of budget), a moderate appetite for academic innovation risks (they will invest in new programs with calculated risks) and high appetite for reputational opportunities (willing to take reputational risk in standing up for academic freedom and truth, for instance).

Learning Outcomes

This nuanced articulation meant that later, when a controversial research project came under public scrutiny, leadership could refer to the risk appetite statement – it fell under a risk they were willing to take (academic freedom), and they stood firm, backed by the Board's prior deliberation. The clarity prevented knee jerk reactions and gave stakeholders confidence that the decision was principled. Northern University also embedded these appetite levels into its risk register system – every risk entry has a field showing the appetite level for that category, highlighting if current risk exposure is above or with in appetite.

CHAPTER 5 - ERM IMPLEMENTATION ROADMAP

Having laid the groundwork of governance, culture, and strategy alignment, we now present a step-by-step roadmap for implementing Enterprise Risk Management in a university. This roadmap is structured into a logical sequence of steps, each building on the previous. It aligns with the ISO 31000 process and COSO framework discussed earlier, and it is tailored to the context of higher education. The roadmap details practical actions, responsible parties, and expected outputs at each step. We also include illustrative case studies to show how these steps might play out in real (or realistic) scenarios.

Overview of the Roadmap: In brief, the steps include (1) securing leadership commitment and establishing the ERM foundation (policy, team), (2) identifying and assessing risks (building the risk register and using tools like heat maps), (3) developing and implementing risk responses (treatment plans for key risks), and (4) monitoring and reporting on risks continuously (with adjustments and improvements). Think of it as Plan → Do → Check → Act in the context of risk management.

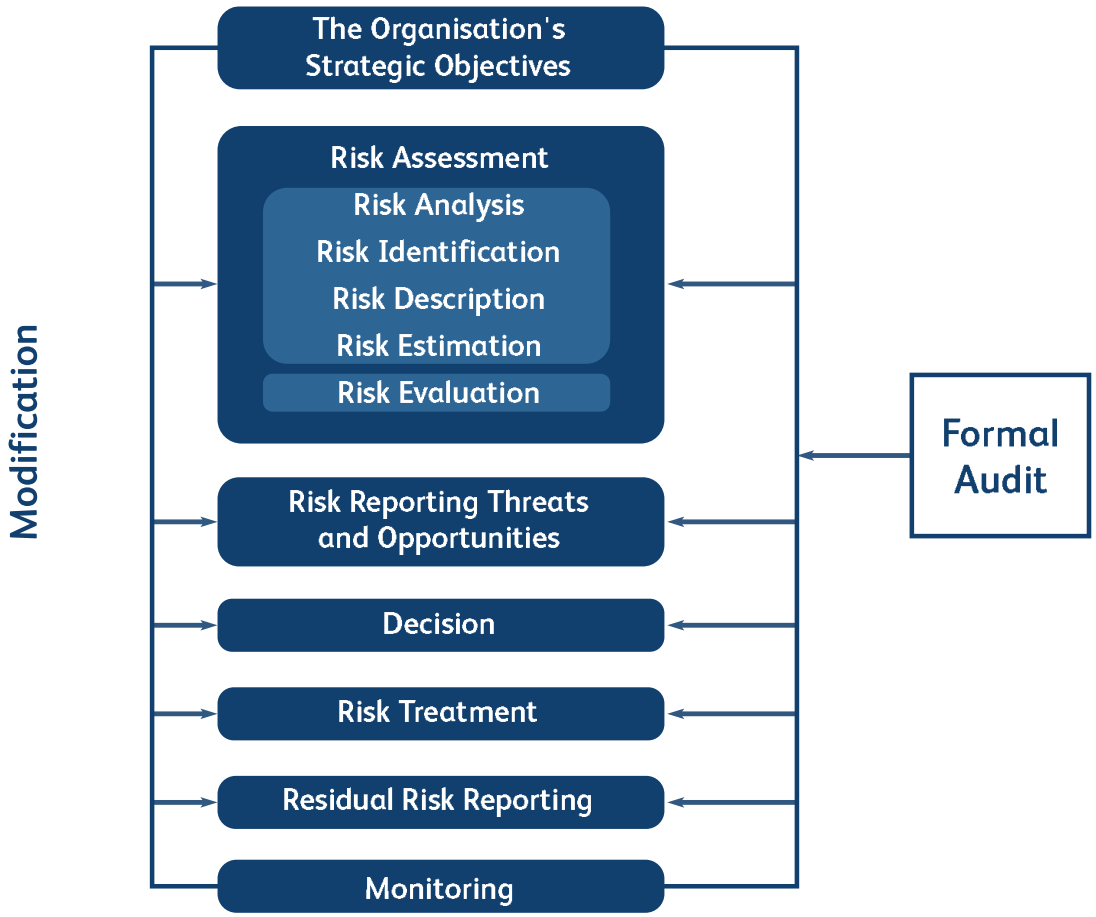


Figure 5: Steps in Enterprise Risk Management

Step 1: Leadership Commitment and Policy Setting

Objective: Formally initiate the ERM program with top-level endorsement, define the scope and objectives of ERM for the institution, and establish the basic framework (policy, roles, resources).

- **Obtain Executive and Board Endorsement:** The Vice-Chancellor/Director and the Board should visibly support ERM from the outset. This could be in the form of a resolution or official statement. Leadership commitment might involve the Board passing a resolution like "The Board endorses the implementation of an Enterprise Risk Management framework in accordance with ISO 31000 and directs management to integrate risk management into university governance and operations." The Vice-Chancellor might send a memo to all departments emphasizing the importance of ERM and requesting cooperation. This top-down communication is crucial to set the tone (tie back to Governance & Culture component of COSO).

- **Establish the ERM Team and Structure:** As part of this step, appoint the Chief Risk Officer (CRO) if not already done. Set up the Risk Management Committee(s) as described in the governance section. Essentially, ensure the human infrastructure is in place. Identify risk champions in each faculty/department. Clarify reporting lines (e.g., CRO will report quarterly to Board's Audit & Risk Committee, etc.).

- **Develop an ERM Policy/Charter:** Create a high-level ERM Policy document. This policy acts as a constitution for risk management in the university. It typically covers: purpose of ERM, scope (does it cover all campuses, all activities including academic, administrative, research, etc. – usually yes, enterprise-wide), definitions of risk terminology (so everyone uses a common language), roles and responsibilities (CRO, committees, risk owners, internal audit's role), the general process to be followed (perhaps referencing ISO 31000 process), and the requirement for periodic reporting and review. Align this policy with ISO 31000 principles (e.g., mention that risk management at the university will be inclusive, systematic, and continuously improved). The policy should also reference key related documents that will come, like the Risk Appetite Statement and Risk Register procedure.

- **Set ERM Objectives and Success Metrics:** Right at the start, it helps to define what success looks like for the ERM initiative. For example, an objective could be "Integrate risk assessment into annual planning and budgeting cycle" or "All departments to maintain an up-to-date risk register by year-end" or "Reduce surprises (unforeseen significant incidents) by improving risk identification." Setting a few measurable goals (like training 100% of senior staff on ERM basics, or achieving a certain risk maturity level in 2 years) gives the program direction and allows monitoring progress.

- **Additional Parameters to Elevate ERM Rigor:** To ensure depth and technical robustness, institutions should consider the following supplementary metrics and requirements:

Parameter	Description	Target / Threshold
Risk Appetite Statement	Formal board-approved document articulating appetite and tolerance for major risk categories.	Reviewed and updated annually.
Scenario-Based Stress Testing	Requirement that the university conduct at least one multi-risk scenario exercise per year (e.g., combination of cyber + campus closure).	≥ 1 tabletop exercise/year.
Third-Party Assurance Reviews	Mandate periodic (every 3 years) external audits of ERM processes by accredited firms—similar to financial audits.	External review every 3 years.
Incident Response Time	Average time to acknowledge and escalate a reported risk event to RMC or Board.	≤ 24 hours average.
Risk Fund Allocation	Minimum percentage of annual operating budget dedicated to risk management activities (training, systems, insurance).	≥ 0.1 % of annual operating budget.
Integration with Strategic Planning	ERM documentation must show direct linkage between risk appetite and the institution's strategic plan (e.g., new program risks evaluated).	Mandatory linkage in strategic plan.
Publication of Annual Risk Statement	Public disclosure—within the institution's annual report—of Top 5 risks, appetite summary, and mitigation highlights.	Published in annual report.
Student & Staff Awareness Surveys	Annual surveys measuring awareness of ERM processes and reporting channels among at least 80 % of employees and 20 % of student body.	≥ 80 % employee, ≥ 20 % student.
Integration with Internal Audit Planning	Internal Audit function must align at least 30 % of its annual audit plan to identified Top 10 enterprise risks.	≥ 30 % of audit plan.
Cross-Institutional Benchmarking Reports	Participation in biennial benchmarking studies comparing risk maturity metrics across peer group of similar institutions.	Biennial benchmarking participation.

- **Resource Allocation:** Ensure that the ERM function has the necessary resources. This includes budget for training, possibly software (if using a risk management information system or even simple tools like spreadsheets initially), and consultancy if needed (some universities engage external experts at the beginning to help design the framework or do workshops). Even dedicating administrative support for the CRO can help in coordinating meetings, documentation, etc. The Board's commitment should ideally

include providing these resources. An URMIA higher education risk guide suggests it typically takes about 6–8 weeks to develop and approve an ERM framework, and a few months to implement the initial plan and conduct the first risk assessment. So plan for that timeline and allocate time of key personnel accordingly.

- **Awareness Kickoff:** Conduct a kickoff meeting or seminar for key stakeholders (leadership, deans, directors). This can be a half-day workshop where the CRO (or an invited expert) briefs everyone on what ERM is, why the university is doing it, and what to expect. This helps break the ice and gets people thinking about risks. It's also a chance to address any skepticism or fear by framing ERM as a supportive tool, not a bureaucratic overhead.

Deliverables of Step 1: An approved ERM Policy/Charter, a defined governance structure (organization chart for risk governance), appointment of CRO and committee members, and initial communication from leadership endorsing ERM. With these in place, the program has an official identity and mandate.

Case Study: Kickoff and Early Buy-In

Problem Statement

Trust within departments of universities is eroded when there is a lack of strong leadership communication and inclusive policy development.

Context

At "Metro University" (the name of the institute has been masked to preserve anonymity), the new CRO's first task in Step 1 was to draft an ERM Charter. She benchmarked policies from other universities and tailored one for Metro, which the Board's Risk Committee reviewed and approved within two months. To signal commitment, the University President and Board Chair co-signed a letter to all staff saying: "We are launching an Enterprise Risk Management initiative to strengthen our university. This has full support from the top." They highlighted that this would help proactively address risks like campus security, regulatory compliance, and academic continuity. The CRO then held meetings with each Dean to explain how ERM would work, making it clear that this wasn't about policing departments but helping them succeed. Some faculty were initially wary ("Is this just more admin work?"), but after the CRO illustrated how identifying risks could secure their projects (e.g., if a risk to a research project is identified early, they could request contingency funds), attitudes warmed. By the end of the quarter, Metro University had its ERM framework ready, a Risk Committee of senior executives meeting monthly, and every department knew who their risk champion was.

Learning Outcomes

This solid start was credited to strong messaging from leadership and inclusive policy development – the CRO had even included a few faculty in the policy drafting committee to get diverse inputs, which built trust.

Step 2: Risk Identification and Assessment Process

Objective: Systematically identify the risks across the institution, categorize them, and assess their likelihood and impact. This step results in the creation of a Risk Register (a centralized repository of identified risks with their analysis) and initial prioritization of risks. Essentially, this is about gathering a holistic view of what could go wrong (or right, in terms of opportunities) in all areas of the university.

Figure 6

- **Develop a Risk Taxonomy (Categories):** Before diving into brainstorming specific risks, it's helpful to establish risk categories or a "risk universe" tailored to higher education. This provides a checklist to ensure comprehensive coverage. Common categories include: Strategic, Academic/Educational, Financial, Operational, Research, Compliance (Legal/Regulatory), Safety & Security, IT/Cyber, Reputational, and External risks. A predefined taxonomy (like the one in the next section of this paper, which lists 200+ risks) can be provided to departments as a reference. Many organizations find that giving people category buckets jogs their thinking (e.g., "what risks do we have in the Financial category?, in the Student Experience category?"). Note: The taxonomy should be broad enough to include unusual or emerging risks; it should be seen as a living document that can evolve.

- **Identify Risks – Techniques: Use multiple techniques to identify risks:**

  - **Workshops/Interviews:** Conduct risk assessment workshops with each faculty/department or functional unit. In these sessions, the CRO (or risk team) facilitates a discussion. A simple prompt is "What are the top 5-10 things that could significantly hinder your unit's objectives or the university's mission?" Encourage them to also consider past incidents (has anything nearly gone wrong?) and future changes (upcoming events or trends). It's important to have cross-functional workshops as well, because some risks (like a pandemic or a campus-wide IT failure) cut across units.

  - **Surveys:** You can circulate a questionnaire asking for risks. This might help capture input from a wider audience including faculty or staff who might not speak up in meetings. The survey can list categories and examples to trigger responses.

- **Review of External Sources:** Consider risks identified by other universities or industry reports. For example, Deloitte noted five broad risk themes for higher education: business model risks, reputation risks, operating model risks, enrolment supply risks, and compliance risks – these areas should definitely be covered. Also, as a reference, a RSM analysis in the UK found that the top risk register items were in finance, IT, and student numbers (enrolment), reinforcing that those are key concerns. By looking at such studies and news of incidents (like data breaches or campus crises at other institutions), you can identify risks that your own institution might face.

- **Brainstorming with scenarios:** Pose hypothetical scenarios ("Imagine its five years from now and our university has to close a major program – what could cause that?" or "Suppose we double our student intake next year, what risks would that bring?"). Scenarios help people think outside the status quo.

- **Academic and Administrative Processes Mapping:** Sometimes going through each major process (admissions, exams, graduation, hostel management, lab research, procurement, etc.) and asking "what can go wrong here?" ensures no area is overlooked.

- **Establish an Academic Risk Observatory (ARO):** An observatory that aggregates data on systemic risks such as cyber-attack waves, demographic declines, health emergencies etc. and identifies sector trends, and issues early warnings.

Core Functions:

1. **Annual Risk Disclosure**
   Submission Template: Top 10 enterprise risks, residual risk scores, status of mitigation actions, and KRI readings for at least five metrics.

2. **Data Analytics & Intelligence**
   - Risk Aggregation Platform: Database ingesting annual disclosures, with analytics for trend detection, anomaly alerts (e.g., sudden rise in compliance-related risks in a region).
   - Sector Risk Reports: Quarterly bulletins summarizing emerging threats (for example, "Increase in mental health-related incidents among students across urban campuses").

3. **Regulatory Feedback Loop**
   - Early Warning Alerts: ARO issues signals to UGC/NAAC when a systemic risk threshold is crossed (e.g., > 20 % of institutions report escalating cyber incidents).
   - Targeted Interventions: Regulators can then deploy rapid response measures-such as issuing sector-wide cybersecurity guidelines or funding emergency counseling services.

- **Document Risks in a Register:** As risks are identified, record them in a structured Risk Register. Key fields to capture: a description of the risk, category, the potential causes, and potential impacts (qualitatively what could happen). It's also helpful to note any

existing controls managing that risk currently (for instance, if the risk is "fire in campus building," an existing control is "we have sprinklers and an evacuation plan"). We'll assess control effectiveness later, but noting them upfront informs likelihood/impact estimates. Many universities use simple spreadsheets initially for the risk register, later possibly moving to specialized software. The CRO's office should consolidate all inputs into one master register, removing duplicates and clustering similar risks. For example, multiple departments might mention "budget cuts" – that can be rolled into one university-wide financial risk entry.

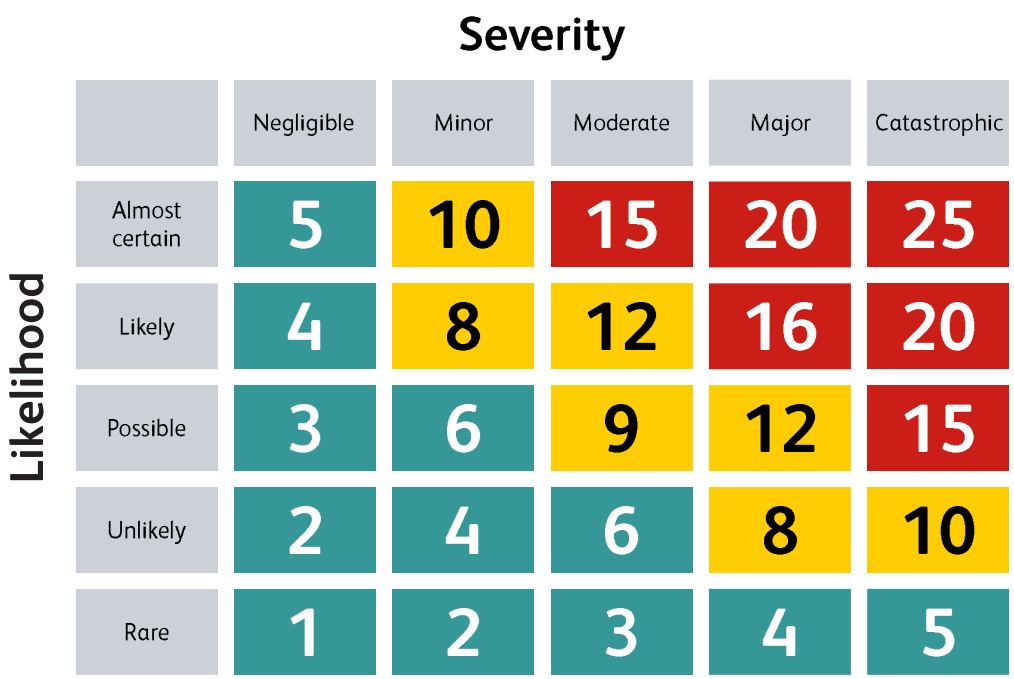
- 

Figure 7: A typical risk rating matrix

- **Assess Likelihood and Impact (Initial Risk Scoring):** For each risk identified, the next task is to estimate:

  - **Likelihood (Probability):** How likely is the risk to materialize? Use a qualitative scale (e.g., 1 to 5, where 1 = Rare, 5 = Almost Certain) with definitions. In higher ed, a "Rare" might be something that could happen once in 10+ years; "Almost Certain" might be something seen every year or inevitable under current conditions.

  - **Impact (Consequence):** If the risk happens, what is the severity of impact? This usually is evaluated on multiple dimensions: financial loss, safety impact, reputational damage, operational disruption, etc. To simplify, some combine into one overall impact score (1 to 5, e.g., 1 = Negligible, 5 = Catastrophic). In a university, a Catastrophic impact could be something that causes loss of life, or threatens the institution's survival (like insolvency or loss of charter), whereas Minor might be a manageable inconvenience or small financial hit.

  - Some frameworks also include other criteria like velocity (how fast it hits) or detectability, but to keep it simple, likelihood and impact are core.

  - It's often useful to create a risk scoring matrix (like 5x5) to guide this. For consistency, define what each score means. For example, Impact 4 (High) might be

defined as "Significant impact: e.g., a financial loss over ₹1 crore, or serious injury to an individual, or major disruption of operations for a week, or national media coverage damaging reputation." This helps different people to calibrate their scoring similarly.

- In the workshops, once risks are listed, ask participants to score them. Take consensus or average if needed. The CRO can later adjust for consistency across departments.

Figure 7: A typical risk "heat map" used in universities, plotting risks on a matrix of Likelihood (Y-axis) vs Impact (X-axis). The coloured grid indicates risk severity (green = low, red = high). The numbers in cells represent risk scores (Likelihood × Impact). Such visual tools help prioritize which risks need urgent attention (e.g., those in the red zone above the university's risk appetite). In this example, a risk scored 25 (almost certain & very high impact) is extreme and would demand immediate action.

- **Prioritize Risks:** After scoring, you can rank the risks to see the most critical ones. Typically, focus will be on the "high-high" risks (high likelihood, high impact) and also those with either high impact (even if low likelihood, like a rare but catastrophic event) or high likelihood (chronic issues). This list of Top X Risks (top 10 or 20) will be what you present to the senior management and Board first. Prioritization helps in allocating effort – not all risks can be addressed at once, so identify the ones that matter most. This doesn't mean low risks are ignored; they'll just be monitored periodically.

- **Validate and Challenge:** It's good to review the initial risk list with a critical eye. The executive risk committee should discuss: "Do these cover our strategic objectives? Any blind spots? Are any of these essentially duplicate or caused by another?" Also, watch out for people listing issues that are not actually risks but outcomes or general categories (for example, someone might list "Reputation" as a risk – but as United Educators' guidance notes, reputation damage is an outcome of other risks . So you'd refine that to "Risk of reputational damage due to X (cause)"). The CRO should help refine wording: risks should ideally be stated as cause → event → impact (e.g., "Inadequate IT security (cause) could lead to a major data breach (event) resulting in loss of confidential student data and reputational damage (impact)"). This helps in later thinking about mitigations.

By the end of Step 2, you should have a comprehensive list of risks facing the university, each assessed for significance, and a clear idea of the most pressing risks. Often this is the first time an institution sees all its risks in one place – it can be eye-opening. For instance, a university might realize that while each department was managing its issues, at the enterprise level certain themes (like "talent retention of faculty" or "legacy IT systems failure") are pervasive and critical. It's not uncommon to identify 100-200 distinct risk entries in a large university's initial risk register, which then get grouped into categories (we'll present an exhaustive taxonomy in the next chapter).

Case Study: Uncovering Hidden Risks

Problem Statement

Severity of operational issues are underestimated due to universities not developing a business continuity plan.

Context

"Eastern Institute of Technology" (the name of the institute has been masked to preserve anonymity) embarked on risk identification and was surprised by the outcome. Each department provided their top 5 risks. The academic departments focused on things like "losing good faculty to other colleges" and "drop in student quality." The facilities department listed "aging electrical infrastructure" as a risk of fire and outage. Finance listed "tuition revenue decline due to demographic change." When the CRO aggregated them, one risk that hadn't been explicitly stated stood out indirectly: the risk of campus shutdown. Many separate risks (infrastructure failure, lack of disaster plan, public safety incidents) all pointed to the institution's ability to continue operations. Realizing this, the executive team added "campus operations interruption" as a strategic risk on the register, with causes ranging from natural disasters to infrastructure issues. They tasked a subcommittee to develop a business continuity plan – something they never prioritized before. During the identification process, another interesting discovery was that several departments listed mental health of students as a growing risk (counselling centre overload, potential for self-harm incidents). This hadn't been on the leadership's radar as an 'enterprise risk' – it was seen as an operational issue – but given its frequency across departments and possible severe impact, the Risk Committee elevated it. They decided to invest more in student wellness programs as a risk mitigation.

Learning Outcomes

This case underlines that a thorough risk identification brings to light cross-cutting issues that may otherwise be underestimated if viewed in silos.

operational issue – but given its frequency across departments and possible severe impact, the Risk Committee elevated it. They decided to invest more in student wellness programs as a risk mitigation. This case underlines that a thorough risk identification brings to light cross-cutting issues that may otherwise be underestimated if viewed in silos.

Step 3: Risk Treatment and Response Planning

Objective: For the priority risks identified, develop and implement appropriate risk responses (mitigation plans) to manage the risks within acceptable levels. This step turns analysis into action – assigning owners and actions to either reduce the likelihood of risks, lessen their impact, transfer the risk, or avoid it completely, depending on the risk appetite and context.

- **Evaluate Risk Response Options:** Recall the classic "**4 T's**" of risk treatment: **Treat, Transfer, Tolerate, Terminate** :

  - **Treat (Mitigate):** Take actions to reduce the risk's likelihood or impact. This is most common. E.g., for cyber risk – invest in better security systems and training (reduces likelihood of breach), have backup servers (reduces impact of downtime).

  - **Transfer:** Shift the risk to a third party, usually via insurance or contracts. Universities often insure against property damage, liability claims, etc. Also, outsourcing a risky operation (with proper contractual terms) is a form of transfer (though some residual risk remains). E.g., if lab experiments are very risky, maybe partner with a specialized facility.

  - **Tolerate (Accept):** Decide to accept the risk as is, usually because it's low enough or the cost of mitigation is too high relative to benefit. This must be in line with risk appetite. Some risks we simply monitor. E.g., a small likelihood risk that a meteor strikes the campus – you tolerate since nothing practical can be done.

  - **Terminate (Avoid):** Stop the activity that causes the risk. In some cases, if a risk is too dangerous and uncontrollable, you avoid it. E.g., if running a bungee-jumping event during student fest is deemed too risky and not essential, you cancel that activity (avoid the risk entirely). In strategy terms, an example is deciding not to pursue opening a campus in a politically unstable region if the risks are beyond appetite.

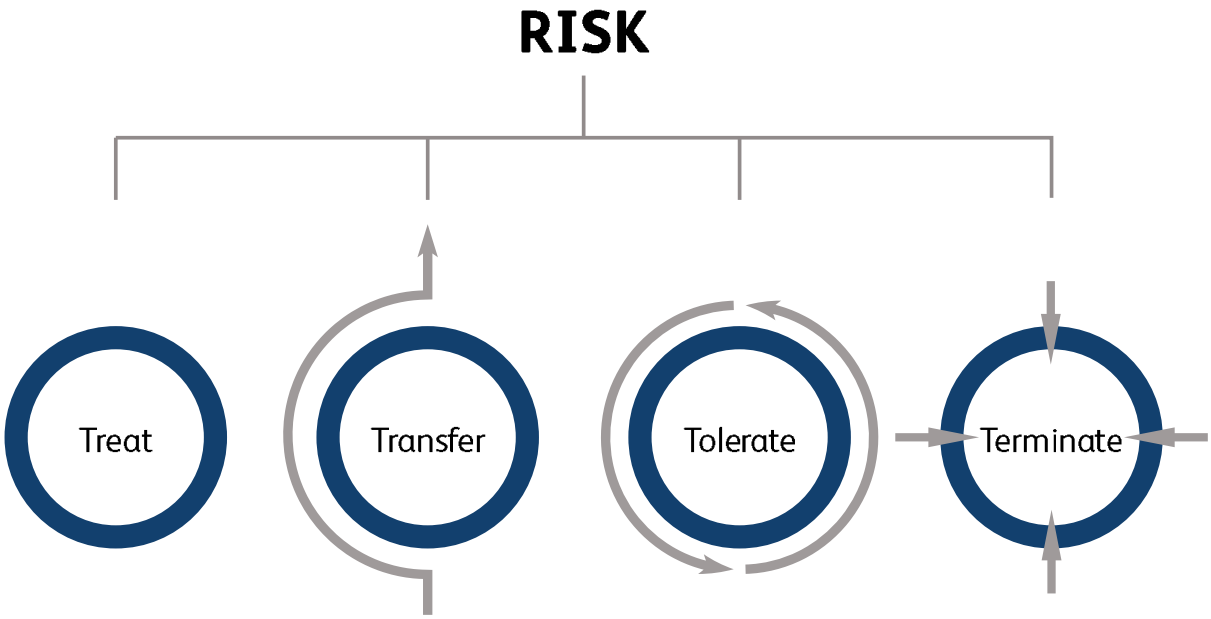


Figure 8: The classic "4 T's" of risk treatment

- For each major risk in the register, go through these options. Often a combination is used. For instance, for a risk of "fire in dormitory," the response might be: Treat (install alarms, do drills), Transfer (buy fire insurance), Tolerate (residual risk of fire you live with

because you can't eliminate all chance), and clearly not Terminate (you can't avoid housing students altogether, unless that's a strategic choice).

- **Develop Action Plans (Mitigation Plans):** For risks chosen to be treated, make specific action plans:

  - **Define actions:** e.g., "Develop a Disaster Recovery Plan for IT systems" or "Conduct active shooter response training for campus security staff" or "Diversify investment portfolio to mitigate endowment risk".

  - **Assign ownership:** every action gets an owner (person or department) and a deadline. E.g., CIO to implement new firewall by Q3, or Dean of Students to roll out new mental health initiative by next semester.

  - **Allocate resources:** ensure the plan has the budget or people needed. If a mitigation needs funding, include it in the next budgeting cycle or get a special approval.

  - **Set performance indicators:** for some actions, you can set risk key indicators to track. E.g., after mitigation, what will you monitor to know if risk is reducing (like number of cyber attack attempts detected vs prevented).
  - Document these in the risk register alongside each risk (some registers have columns for mitigation actions, status, etc.).

- **Consider Risk Appetite in Responses:** If a risk's current level is above the university's risk appetite/tolerance, the response plan should aim to bring it down within appetite. For example, if the appetite for compliance risk is "zero major compliance violations" and currently the risk of a violation is moderate (perhaps due to some gaps in processes), the mitigation must reduce that risk (maybe by hiring a compliance officer or conducting policy training). In reports, it's useful to note post-mitigation risk level expectations (sometimes called residual risk). If after actions the risk is still above appetite, that's a flag that more needs to be done or leadership acceptance is needed.

- **Leverage Controls and Internal Audit:** Many risks are managed by internal controls (policies, procedures). For significant risks, ensure that adequate controls exist and are effective. If not, part of the mitigation plan may be to design new controls or improve existing ones. For instance, risk of grade manipulation might be mitigated by stricter controls in the grading system and periodic audits. Internal Audit can be a partner by reviewing the design of controls for top risks and suggesting improvements. In risk committee meetings, after plans are implemented, IA can later report whether those controls are indeed working (closing the loop with the third line of defence).

- **Emergency/Crisis Preparedness**: Some high-impact risks require detailed contingency plans (often called business continuity or disaster recovery plans). Ensure that for scenarios like campus closure, IT blackout, earthquake, pandemic outbreak, etc., the university has documented what it will do. Who declares the emergency, how communication flows, backup arrangements for classes, etc. The risk management function often coordinates creation of these plans (though execution may reside in emergency management teams). Testing these plans via drills or simulations is also important – that can be part of risk treatment (treating the risk of poor emergency response by practicing it).

- **Insurance Strategy:** Revisit the insurance portfolio of the university as part of risk treatment. Common policies include property insurance, liability insurance (for injuries, etc.), indemnity insurance for board/trustees, possibly cyber insurance, etc. Check that coverage aligns with risk exposures. For example, if "natural disaster causing building damage" is a top risk, do you have sufficient property and business interruption coverage? Also consider if certain emerging risks are uninsurable and need self-funding reserves.

- **Risk Response for Opportunities:** Not to forget, ERM also addresses upside risk (opportunities). If through identification you found an opportunity (say, high demand for a new course), the response could be to exploit or enhance it. For completeness, mention that while most of our focus is mitigating threats, when opportunities (positive risks) are identified, assign them to someone to further develop. This might mean investing resources to increase the likelihood of the opportunity (like leveraging a strong industry partnership to boost research funding).

- **Document and Approve Plans:** The risk committee should review the major mitigation plans. Significant risk responses might need Board or senior management approval, especially if they involve policy changes or big expenditures. E.g., if the plan for "campus terrorism risk" involves setting up armed security at gates, the Board might need to weigh in due to its sensitivity and cost. Documentation also helps accountability – when you revisit risks next cycle, you check progress on these actions.

- **Implement and Track:** Once approved, owners execute the plans. The CRO's office should track progress and update the status in risk register reviews (e.g., "Firewall upgrade – completed" or "Policy drafted, awaiting approval"). A lack of progress on a critical risk mitigation is itself a risk that should be flagged upward if needed.

Case Study: Mitigation in Practice

Problem Statement

Universities are vulnerable to a multitude of risks in the absence of a comprehensive risk treatment plan.

Context

Following the risk assessment, "Midlands University" (the name of the institute has been masked to preserve anonymity) identified "Loss of research data due to cyber-attack" as a top risk (High likelihood, High impact, beyond appetite). Their risk response plan was multi-faceted:

(1) Treat – IT department to implement multi-factor authentication and network monitoring (to reduce likelihood of breach) and create an offline backup of critical research data (to reduce impact if breach occurs).

(2) Transfer – they purchased a Cyber Insurance policy to cover financial losses from a breach.

(3) Tolerate – accepted but set a threshold (if more some residual risk remains, which they than X records are compromised, that triggers a major incident protocol).

(4) Terminate – not applicable, as they cannot avoid using digital systems.

The Board approved a special budget for the IT security upgrade, recognizing the risk's severity. Over the next 6 months, these measures were implemented. In parallel, internal audit reviewed user access controls.

Learning Outcomes

A year later, an audit of ERM showed that Midlands' actions had reduced the risk rating from High to Medium (within their tolerance). They also experienced fringe benefits: the improved cybersecurity prevented a minor malware outbreak that hit peer universities – so their proactive risk treatment paid off in tangible terms. Another example from Midlands for the risk "Decrease in student enrolment ", which was high impact but medium likelihood their strategy combined Treat (increased marketing in new regions, launching attractive courses), Tolerate (they set a threshold of minimum enrolment they could accept and adjusted budgets accordingly), and Transfer in a sense by partnering with an external recruiter firm (sharing the risk of enrolment shortfall with partners through performance-based contracts). This comprehensive risk treatment approach kept their enrolment stable even as demographics shifted.

Step 4: Monitoring, Reporting, and Continuous Improvement

Objective: Establish ongoing processes to monitor the risk environment, track the effectiveness of risk responses, report on risk status to stakeholders, and continuously refine the ERM program. Essentially, this step ensures ERM is not a one-time project but an evolving practice that keeps the university resilient over the long term.

- **Regular Risk Monitoring:** Each significant risk should have a monitoring plan. This could involve Key Risk Indicators (KRIs) – metrics that serve as early warning signals. For example, for the risk "student mental health issues," a KRI might be the monthly count of counselling centre visits; if it spikes, risk may be rising. For financial risks, KRI could be the operating margin or liquidity ratio; for IT risks, maybe number of detected intrusion attempts. Define thresholds for these KRIs that, if exceeded, prompt action or escalation. Risk owners should review their KRIs and control indicators regularly (some monthly, some quarterly, depending on the risk). The ERM team can facilitate by gathering these indicators and maintaining a risk dashboard.

Red	The value of the threshold is higher than 'U'
	The value of the indicator is increasingly high which means a great exposure to a major risk
	Immediate actions should be put in place to manage risk
Orange	The value of the threshold is between 'L' and 'U'
	The value of the indicator is higher than the normal value which means a potential exposure to a significant risk
	Close attention is required by the management to decide whether an action should be undertaken
Green	The value of the threshold is lower than 'L'
	The value of the indicator is normal which means that the company is not exposed to the underlying risk
	No action is required

Figure 9: Template of a Key Risk Indicator system dashboard

- **Incident Tracking:** Despite best efforts, incidents will happen. Establish a process to record risk events or "near misses." When something goes wrong (say a minor lab accident or a network outage), log it and analyse: Was it a known risk on the register? If yes, did the controls work as expected? If not a known risk, then it's an emerging risk – add it to the register and treat it going forward. For known risks, incidents test if your assessment was accurate. For instance, if you rated "lab accidents" as low likelihood but you've had two in a semester, your likelihood needs updating. Use incidents to learn and adjust risk scores and strategies.

- **Periodic Risk Reviews:** The Risk Management Committee (executive level) should have a standing quarterly (or at least biannual) meeting dedicated to ERM review. In these meetings, they would:

  - Review the top risks and any changes in their status (e.g., did any risk increase/decrease? Are new risks emerging?).

  - Check progress on risk mitigation action plans (are we doing what we said we would?).

  - Consider any changes in context: e.g., new regulations, new strategic initiatives, changes in external environment (like economic shifts, technological change) that may introduce new risks or alter existing ones.

  - Review any incidents or audit findings related to risks.

  - Update the risk register as needed (risks may be closed if no longer relevant, or re-scored).

  - Prepare a summary report for the Board Committee.

- At the Board Committee level, typically there's a risk report at least quarterly. The format might be an overview of top 10 risks with their ratings and trends (are they stable, improving, worsening), summary of actions taken, and any recommendations for

Board decisions (for instance, "Risk of regulatory non-compliance is rising; Board support needed to push for more compliance staff"). One example from URMIA suggests some institutions provide quarterly updates to senior leadership and an annual report to the Board (or a committee of the Board). The content can alternate between broad updates and deep-dives on specific risks each quarter.

- **Adaptability and Emerging Risks:** ERM must remain nimble. Each year (if not more frequently), conduct a formal update of the risk assessment to capture emerging risks. For example, five years ago, very few universities had "global pandemic" on their risk register; now it's a known category. Similarly, emerging technology like AI usage in education might introduce new risks (plagiarism via AI, data issues) that should be picked up. Encourage a culture where anyone can bring up a new risk at any time – maybe the CRO sets up a simple online form or email for submitting "risk suggestions" that will be evaluated.

- **Continuous Improvement of ERM Framework:** Based on experience, refine the ERM process itself. Solicit feedback from participants: did the risk workshops yield useful info or were they too cumbersome? Is the risk scoring methodology working or do we need to adjust criteria? Also, as maturity grows, you might integrate ERM deeper: for instance, integrating risk management into strategic planning cycles formally (each strategic initiative must go through a risk review). The IRM risk culture guide emphasizes that embedding risk management into everyday decision-making is a sign of mature risk culture. Aim for ERM to be part of the annual planning, budgeting, project management, and performance review processes of the university.

- **Documentation and Knowledge Management:** Keep good records of risk registers, meeting minutes, and risk reports. Not only is this useful for internal tracking, but it can serve as evidence for accreditation bodies or regulators showing that the university proactively manages risk. Some universities integrate ERM reporting into their annual reports or their accreditation self-study documents to demonstrate governance strength.

- **Benchmarking and External Reviews:** Consider periodic external reviews of your ERM program – maybe every 3-5 years. IRM or other consultants can benchmark your program against best practices or maturity models (like RIMS Risk Maturity Model). Also, participate in higher education risk management forums (like URMIA or local networks) to compare notes. For example, if peer institutions are addressing climate change risks as a new focus, you might learn from them and adopt similar measures.

- **Reward and Reinforce:** When good risk management practices avert a crisis or achieve a benefit, acknowledge it. For example, if a department's risk mitigation prevented a big problem (say, finance's hedging strategy saved money when currency fluctuated), celebrate that in internal communications. This reinforces the value of ERM and keeps people engaged. Conversely, learn from failures (without blame). If a surprise happened that wasn't flagged as a risk, treat it as a learning opportunity to improve the process.

Case Study: Sustaining the ERM Cycle

Problem Statement

ERM models are unsustainable if they are not accompanied by regular risk assessments.

Context

At "South City University" (the name of the institute has been masked to preserve anonymity), after two years of running ERM, they made some tweaks based on monitoring insights. Initially, risk reports to the Board were dense, listing 20+ top risks. The Board members felt overwhelmed and were unable to see the forest for the trees. Taking feedback, the CRO reformatted the report to highlight five broad risk themes with heat maps and trend arrows, and then an appendix with details. South City also established a practice that any proposal going to the Finance Committee for large expenditures must include a section on risk (and reference the risk register). This integration meant that when a new campus construction was proposed, it was accompanied by a risk assessment (materials supply risks, contractor risks, enrolment risk for filling the new campus) which the Finance Committee appreciated for decision-making. On the continuous improvement front, South City's internal audit did a review of the ERM process and found that while most departments were reporting risks, some academic units were not engaging fully (perhaps viewing it as admin). In response, the Provost was enlisted to champion ERM among faculty, and the process was adjusted to be less time-consuming (e.g., an online risk update form instead of long meetings).

Learning Outcomes

Highlighting broad risk themes made Board discussions more strategic. Integrating these adjustments kept ERM sustainable. In one instance, their monitoring paid off: a KRI for research grant dependency (monitoring if more than 50 % of research funding comes from one source) tripped – showing over-reliance on a single government grant. This was flagged, and the university diversified its funding the next year, which proved wise because that grant faced cuts later. Without the KRI, they might not have realized the exposure until it was too late.

CHAPTER 6 - COMPREHENSIVE RISK TAXONOMY FOR HIGHER EDUCATION INSTITUTIONS

One of the most valuable assets of an ERM program is a well-defined Risk Taxonomy – a structured index of potential risks, grouped by categories, with clear definitions. This serves as a reference library that helps ensure no significant risk is overlooked and that everyone uses consistent terminology. In this chapter, we present an extensive risk taxonomy tailored to Higher Education Institutions (HEIs), drawing from global examples and typical university operations. We list over 200 risks that universities around the world commonly face, categorized for clarity. Regulators and universities can use this taxonomy as a checklist or appendix to their risk management policy, customizing it to their context. (Not every institution will have all these risks, but considering each prompts a conscious decision on its relevance.)

Major Risk Categories: We will use the following major categories for organizing the risks:

1. **Strategic & Governance Risks** – High-level risks that affect the institution's mission, strategy, or governance.
2. **Academic & Student Experience Risks** – Risks related to teaching, learning, research, and student outcomes.
3. **Financial Risks** – Anything that impacts financial health, budgets, investments, and funding.
4. **Operational Risks** – Day-to-day operational risks across departments (excluding finance which is separate).
5. **Human Resources Risks** – Concerns related to faculty, staff, and human capital.
6. **Compliance & Legal Risks** – Breaches of laws, regulations, or ethical standards.
7. **Campus Safety & Security Risks** – Threats to physical safety of the community and security of campus assets.
8. **Information Technology & Data Risks** – Digital and cyber risks, data management issues.
9. **Research Risks** – Specific to research activities (some overlap with others, but focusing on research enterprise).
10. **Reputation & External Relations Risks** – Public image, stakeholder relations, external environment changes.
11. **Environmental & Infrastructure Risks** – Facilities, environment, and sustainability-related risks.

Within each, we'll enumerate specific risks with a brief definition. Note that some risks could fit multiple categories; we place them where most pertinent but one could cross-reference.

1. Strategic & Governance Risks

1. **Lack of Clear Strategy** – Absence of a defined strategic plan or mission drift, leading to ad hoc decisions and loss of competitive position.
2. **Governance Failure** – Board or leadership not providing effective oversight (e.g., poor decision-making structures, conflicts of interest on board).
3. **Leadership Succession Risk –** Sudden departure or inability to replace key leaders (Vice-Chancellor, Deans) with equally capable successors.
4. **Political Interference** – External political forces unduly influencing university decisions or autonomy (especially relevant for public universities).
5. **Reputation/Ethics of Leadership** – Scandals or unethical behaviour involving top leadership causing loss of credibility.
6. **Misalignment with Market Needs** – Academic programs not aligned with job market or societal needs, risking relevance of university offerings (strategic risk of obsolescence).
7. **Overexpansion** – Expanding campuses/programs beyond the capacity or demand, leading to financial and operational strain.
8. **Competition Risk** – Other universities (domestic or international) attracting away students, faculty, or research opportunities, undermining the institution's strategic position.
9. **Mergers/Partnership Risk** – Risks associated with merging with another institution or entering strategic partnerships (cultural clash, integration failures).
10. **Institutional Reputation Damage** – Broad risk of events that globally tarnish reputation (could result from any category, but as a strategic risk: e.g., being ranked poorly or a public scandal).
11. **Mission Creep** – Diversifying into areas outside core mission (like a teaching-focused college trying to become research-intensive without capacity) diluting effectiveness.
12. **Intellectual Property (IP) Strategy Risk** – Lacking strategy on managing and commercializing IP from research, potentially losing out on innovation benefits (or legal disputes over IP).
13. **Accreditation Risk** – Failing to obtain or maintain accreditations (national or international) for the institution or specific programs, affecting legitimacy.
14. **Risk Management Failure** – Ironically, the risk that the ERM process itself is not sustained (e.g., ignored by management, leading to blind spots).

2. Academic & Student Experience Risks

1. **Decline in Teaching Quality** – Teaching methods or faculty performance deteriorating, leading to poor student learning outcomes.
2. **Curriculum Obsolescence** – Academic programs not updated to reflect current knowledge or skills, making graduates less competitive.
3. **Low Student Engagement** – Students not engaged in learning or campus life, leading to higher dropouts or poor performance.
4. **Academic Integrity Violations** – Cheating, plagiarism, or exam fraud becoming prevalent, eroding the value of credentials.
5. **Admissions Risk** – Incorrect admissions decisions or processes (e.g., admitting unqualified students due to faulty criteria, or missing out on quality students due to process issues).
6. **Enrolment Fluctuation** – Sudden drop (or surge) in student enrolment numbers beyond forecasts, straining resources or finances.
7. **Student Retention Risk** – High attrition (students not completing programs) due to dissatisfaction, difficulty, or external lures.
8. **Student Demographic Change** – Changing demographics (e.g., lower youth population, or shift in socio-economic mix) impacting demand for programs (enrolment supply risk).
9. **International Student Dependency** – Over-reliance on international student enrolment; changes like visa policies or global events causing enrolment decline.
10. **Student Mental Health Crisis** – Rising cases of student anxiety, depression, or other mental health issues overwhelming support services and affecting student success.
11. **Inadequate Student Services** – Risk that housing, counselling, dining, or career services do not meet student needs, harming experience and retention.
12. **Student Misconduct** – Serious disciplinary issues (e.g., hazing, violence, harassment among students) causing campus unrest and reputational harm.
13. **Academic Program Closure** – Risk that certain programs may become unsustainable (low enrolment or funding) and need closure, causing disruption to current students.
14. **Competition for Top Students** – Other institutions aggressively recruiting top students (with scholarships, etc.), causing talent drain in student body.
15. **Online Education Competition** – Risk of losing prospective students to online programs or edtech platforms if the university doesn't adapt (especially relevant after COVID push to online).

16. **Research Quality Decline** – (Overlap with research category) – but from academic perspective: not producing sufficient quality research, affecting rankings and academic reputation.

17. **Graduate Outcomes** Risk – Graduates not achieving good employment or further study placements, affecting institution's attractiveness and possibly triggering scrutiny of program effectiveness.

18. **Changes in Regulatory Academic Standards** – e.g., new government criteria for curriculum (as sometimes happens in professional programs) making current programs non-compliant or needing rapid change.

3. Financial Risks

1. **Revenue Shortfall** – Overall income less than projections (could be due to lower tuition intake, cuts in government funding, reduced donations, etc.).

2. **Budget Overruns** – Departments or projects overspending their budgets, causing deficits.

3. **Inadequate Reserves** – Not maintaining sufficient financial reserves or endowment to cushion against shocks.

4. **Tuition Dependency** – Over-reliance on tuition as income; risk that any dip in enrolment directly causes financial crisis.

5. **Decline in Public Funding** – Government grants or subsidies reducing (especially for public universities or research grants).

6. **Research Funding Risk** – Losing major research grants or not securing enough funding to support research activities (also risk around shifting funding priorities of grant agencies).

7. **Donation and Fundraising Risk** – Targets for fundraising campaigns not met; key donors pulling back due to economic conditions or dissatisfaction.

8. **Investment Risk** – Losses in invested funds or endowment due to market volatility or poor investment management.

9. **Currency Exchange Risk** – For institutions dealing in multiple currencies (e.g., receiving foreign tuition or grants), volatility causing financial loss.

10. **Inflation and Cost Increases** – Operating costs (salaries, utilities, construction) rising faster than revenue, squeezing margins.

11. **Payroll and Benefits Liability** – Increases in salary commitments, pensions, or benefits that are unsustainable (many universities have large pension obligations).

12. **Fraud and Financial Misconduct** – Risk of embezzlement, fraudulent transactions or corruption within financial operations (e.g., procurement fraud, false expense claims).

13. **Tuition Pricing Risk** – Pressure to limit tuition increases (due to policy or competition) that could constrain revenue, or conversely raising tuition and pricing out some students.

14. **Financial Control Weakness** – Weak internal controls leading to accounting errors, misstatements, or inability to prevent misuse of funds.

15. **Credit Risk** – Inability to service debt or unfavourable terms on borrowing (for those with loans/bonds), or risk of credit rating downgrade for the institution.

16. **Auxiliary Enterprise Risk** – Losses in auxiliary units like campus bookstore, dining services, or hotels (many universities run these as separate businesses).

17. **Capital Project Risk** – Major construction projects running over budget or stalled, causing financial strain and loss of expected utility.

18. **Cash Flow Liquidity Risk** – Short-term cash crunch due to timing of cash inflows vs outflows (even if budget is balanced, a liquidity gap can cause distress).

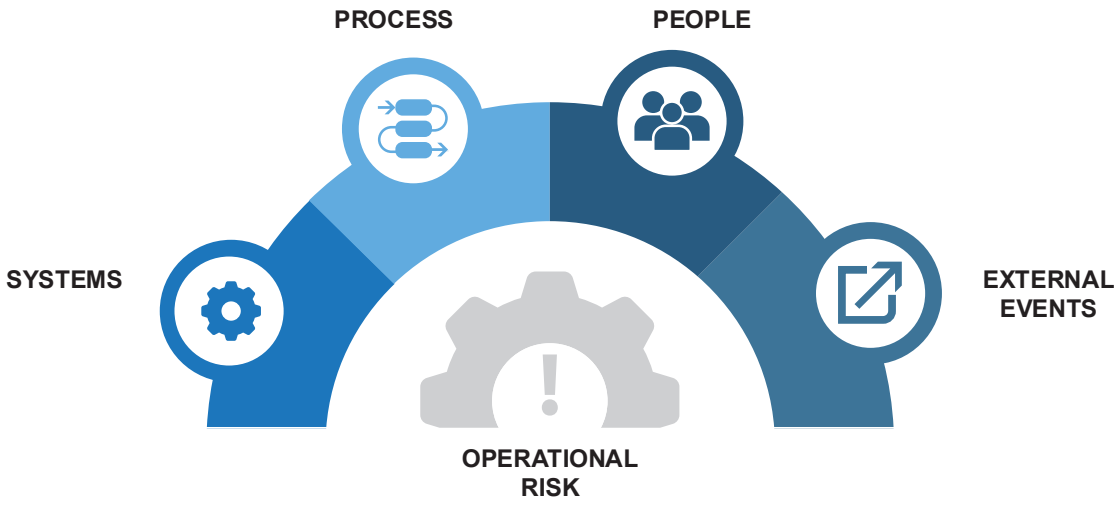
19. **Scholarship & Financial Aid Risk** – Overcommitting on scholarships or aid (especially if reliant on endowment returns that might falter), or failing to provide enough aid to attract needed students.

20. **Mis-estimation of Cost Savings** – Risk that expected savings from initiatives (say automation or restructures) don't materialize, leaving a budget hole.

4. Operational Risks

(These relate to the execution of various administrative and support processes.)

1. **IT System Outage** – Major failure of IT systems (e.g., learning management system down during exams, ERP failure in registration period) disrupting operations.
2. **Data Loss** – Loss of important institutional data (student records, research data) due to accidental deletion, system crash without backup.
3. **Cybersecurity Breach** – Cyberattack compromising sensitive data or systems (could be ransomware locking up systems, or hackers stealing personal data).
4. **Utilities Failure** – Loss of critical utilities like electricity, water, cooling/heating on campus, causing building closures and class disruptions.
5. **Facility Maintenance Lapses** – Risk of critical equipment breakdown (HVAC, lab equipment) due to deferred maintenance; leads to downtime or hazards.
6. **Supply Chain Disruption** – Difficulty procuring essential supplies (lab reagents, IT hardware, even office supplies) perhaps due to vendor issues or global shortages.
7. **Transportation Risk** – If the university runs transport (buses, shuttles) – accidents or failures disrupting commutes or causing injury.
8. **Vendor Reliability** – Key third-party service providers (food services, cleaning, outsourced IT support) failing to deliver or going bankrupt.
9. **Construction Delay/Disruption** – Ongoing construction projects causing more disruption to classes than anticipated, or delay in opening new facility affecting planned expansion.
10. **Timetabling/Scheduling Failures** – Significant issues in scheduling classes or exams (e.g., double-booked rooms, scheduling system error) leading to chaos in academic delivery.



11. **Admissions Process Failure** – Errors in admissions (sending wrong acceptance letters, losing application data) harming intake and reputation.

12. **Exam/Grading Process Failure** – Mistakes in exam administration or grading (like paper leaks, mis-grading at scale) undermining academic integrity.

13. **Library/Knowledge Resource Risk** – Loss or unavailability of critical academic resources (perhaps due to digital subscription issues, physical damage to library collections).

14. **Alumni Data/Relations Risk** – Loss of alumni contact data or mishandling alumni relations leading to reduced engagement and donations.

15. **Campus Event Risk** – Issues during major campus events (graduations, festivals, sports events) – e.g., logistical failures, crowd control issues – causing dissatisfaction or safety incidents.

16. **Cafeteria/Food Service Risk** – Food safety issues (contamination causing illness) or inability to meet dietary needs causing health/reputation issues.

17. **Hostel/Accommodation Management Risk** – Operational failures in dormitories (e.g., mismanagement of allocations, poor maintenance leading to pests or outages).

18. **Document Management Risk** – Important documents (transcripts, certificates) lost or issued incorrectly due to process gaps, leading to student grievances and admin burden.

19. **Business Continuity Plan Gaps** – As part of ops, lacking or not up-to-date continuity plans for various scenarios, meaning response will be chaotic if something occurs.

20. **Pandemic/Epidemic Response** – Post-2020, the operational risk that infectious disease outbreak could force shifts to remote operation; preparedness for that scenario (stock of PPE, online capability, etc.).

21. **Change Management Risk** – Big operational changes (new software, restructuring departments) not executed well, causing productivity loss or confusion.

22. **Third-Party Educational Partners** – If partnering with third-party for content or global programs, risk they don't meet standards or default, impacting your ops.

23. **Intellectual Property Theft** – Not exactly IT cybersecurity, but operations: risk that research or sensitive academic materials are stolen or leaked by insiders or visitors.

24. **Procurement Risk** – Purchasing processes not competitive or fair, leading to either legal challenges, waste of funds, or being stuck with subpar vendors.

25. **Operational Compliance** – Overlaps compliance, but like not following standard operating regulations (fire codes, data protection in operations, etc.) leading to fines or shutdowns.

5. Human Resources Risks

1. **Faculty Recruitment & Retention** – Difficulty attracting or keeping quality faculty due to competition or dissatisfaction (leading to understaffing or loss of expertise).
2. **Staff Recruitment & Turnover** – Challenges in hiring/retaining competent administrative or support staff (sometimes high turnover in IT or finance can disrupt continuity).
3. **Aging Workforce** – A significant portion of faculty/staff nearing retirement without succession plans, risking knowledge loss.
4. **Skill Gaps** – Staff/faculty lacking new skills needed (e.g., proficiency in online teaching, data analytics), causing performance issues.
5. **Labour Disputes/Strikes** – Risk of faculty or staff unions striking or engaging in job actions over pay or conditions, disrupting classes and services.
6. **Employee Morale and Culture** – Low morale or toxic work culture leading to productivity loss, higher sick leaves, etc.
7. **Misconduct by Staff** – Employee misconduct such as harassment, discrimination, or exploitation (e.g., a professor harassing a student, or a supervisor bullying staff) creating legal and ethical crises.
8. **Misconduct by Faculty (academic)** – Plagiarism in research, falsification of data, sexual harassment cases – these not only are HR issues but reputational and compliance ones.
9. **Inadequate Training** – Not providing sufficient training (e.g., lab safety training to lab techs, or teaching development to new lecturers) resulting in accidents or poor performance.
10. **Diversity and Inclusion Issues** – Failing to maintain a diverse and inclusive environment, leading to discrimination complaints or loss of talent from marginalized groups.
11. **Occupational Health & Safety for Staff** – Workplace injuries or hazards affecting employees (like ergonomic issues, lab accidents affecting technicians).
12. **Overwork/Burnout** – High workloads on faculty or staff leading to burnout, errors, and higher turnover (commonly, junior faculty juggling teaching and research pressures).
13. **Succession Planning Gaps** – Not identifying and grooming internal candidates for key positions, causing leadership vacuum when someone leaves.
14. **Data Protection for HR** – Risk that confidential HR data (pay, health info) is mishandled or leaked (some overlap with IT security but specifically HR-held data).

15. **Compliance with Labour Laws** – Getting afoul of employment laws (e.g., not remitting provident fund correctly, violating contract terms) leading to penalties or lawsuits.

16. **Faculty Performance Management** – Inability to address underperforming faculty due to tenure or lack of evaluation system, causing long-term academic quality issues.

17. **Key Person Dependency** – Too much reliance on a single individual's expertise (IT admin who knows all systems, or one star professor who brings big grants). If they leave or are incapacitated, operations suffer.

18. **Remote Work Challenges** – With more staff possibly working remotely (post-pandemic), managing productivity, engagement, and cybersecurity for remote staff could be a risk.

6. Compliance & Legal Risks

1. **Regulatory Compliance Breach** – General risk of failing to comply with education regulations (e.g., UGC guidelines, AICTE norms, etc.), possibly leading to fines or restrictions.

2. **Accreditation Standards Non-compliance –** Not meeting criteria of accreditation bodies (NAAC or program accreditations like NBA) which can lead to loss of accreditation.

3. **Research Ethics Violation** – Non-compliance with ethical standards in research (e.g., experiments on humans/animals not following protocol, or not obtaining necessary approvals for sensitive research).

4. **Data Protection Law Breach** – Violating privacy laws (like if India implements personal data protection law, or GDPR for EU students' data) by mishandling personal data.

5. **Environmental Law Non-compliance** – Campus not adhering to environmental regulations (hazardous waste disposal from labs, e-waste, emissions, etc.) leading to legal penalties.

6. **Fire and Building Code Violations** – Buildings not up to code (blocked fire exits, unsafe structures) resulting in legal action or forced closure.

7. **Immigration/Visa Compliance** – For universities hosting international students or hiring foreign faculty: failing to comply with visa rules, which can cause legal trouble or loss of ability to host international students.

8. **Financial Reporting Compliance** – Not following accounting standards or regulatory reporting requirements for financials (especially if university issues bonds or gets audited by govt), leading to qualifications or penalties.

9. **Tax Compliance** – If the institution has any taxable activities or benefits (UBIT in some contexts, or GST on certain services in India), not complying could incur fines.

10. **Sexual Harassment Law Compliance** – Not handling sexual harassment complaints as per laws (like India's POSH Act) which could lead to legal suits and fines.

11. **Public Safety Law** – Non-compliance with laws like the Clery Act (in US, requiring crime reporting) or local equivalents; basically, not reporting or addressing campus crimes as required.

12. **Procurement Law** – For public universities, not following required procurement processes (tendering) can be illegal and result in contract invalidations or legal challenge.

13. **Copyright/IP Infringement** – University inadvertently violating IP laws (e.g., using unlicensed software, or publishing materials without permission) and facing lawsuits.

14. **Litigation Risk** – The risk of being sued by students, staff, or third parties (for e.g., wrongful dismissal suits, liability for accidents, academic disputes). While broad, litigation risk implies costs and distractions from any legal case.

15. **Policy Compliance Internally** – Risk that internal policies (Code of conduct, anti-plagiarism policy, etc.) are not followed, leading to internal governance failures (like a conflict of interest not declared).

16. **Emerging Regulations** – Risk that new laws (e.g., new education policy mandates, or foreign collaboration rules) could catch the university off-guard if not monitored and implemented timely.

(Note: Many compliance risks overlap with other categories but are listed here from the perspective of legal obligation.)

Figure 10

7. Campus Safety & Security Risks

1. **Student Safety Incident** – Harm to student on campus due to accidents (lab accident, sports injury) or crimes (assault, robbery).
2. **Fire** – A significant fire in campus building, causing injury, property loss, and operational disruption.
3. **Natural Disasters** – Earthquake, flood, hurricane, or other natural event impacting campus. E.g., Flooded campus affecting facilities and safety.
4. **Pandemic/Health Emergency** – Outbreak of infectious disease among campus population (like COVID-19 or others) requiring emergency response and possible shutdowns.
5. **Violent Intruder/Active Shooter** – The risk of a violent person on campus causing harm (sadly a noted risk in many countries). This includes terrorism or targeted violence.
6. **Infrastructure Collapse** – Structural failure such as a building collapse or bridge failure on campus posing severe safety risk.
7. **Hazardous Materials Incident** – Spill or mishandling of hazardous chemicals/radioactive materials in labs affecting health and environment.
8. **Food Safety Outbreak** – Food poisoning outbreak from campus dining facilities affecting health of many.
9. **Campus Protests/Unrest** – Large student or public protests on campus that may turn disruptive or violent, risking safety and property.
10. **Sexual Assault on Campus** – Incidents of sexual assault or rape, which are high-impact safety and reputational risks, and require careful management and prevention efforts.
11. **Crime (Theft/Vandalism)** – High rates of theft, vandalism, or other crimes on campus, making the environment unsafe and eroding trust.
12. **Transportation Accident** – If campus has busy roads or transport, risk of vehicle accidents injuring pedestrians or passengers (e.g., a shuttle bus crash).
13. **Sports Injury Fatality** – Serious injury or fatality during athletic events or training (for universities with significant sports programs).
14. **Medical Emergency on Campus** – Inability to respond to a medical emergency (like cardiac arrest of someone on campus) due to inadequate first aid or response protocols.
15. **Security System Failure** – CCTV, access control, alarm systems failing or being absent, causing lapse in incident detection or response.
16. **Firearm or Weapon Incident** – Someone bringing a weapon to campus (even if not used) causing fear or potential harm (overlaps with violent intruder risk).

17. **Lab Safety** – Accidents specific to laboratories (chemical burns, explosions, infection from bio samples) harming students/staff.

18. **Field Trip/Study Abroad Safety** – Students or staff getting into accidents or dangerous situations off-campus during official programs.

19. **Mental Health Crisis Event** – A student or staff suicide on campus, or violent act driven by mental health, impacting community wellbeing and requiring crisis management.

20. **Crowd Crush** – At large gatherings (concerts, convocations), risk of stampede or crush due to poor crowd control.

21. **Elevator/Escalator Accident** – Malfunction leading to injury (particularly in high-rise campus buildings or large facilities).

22. **Inadequate Emergency Communication Systems** – Risk that during an emergency, communication systems (mass notification to students/staff) fail or messages not reaching, worsening the impact.

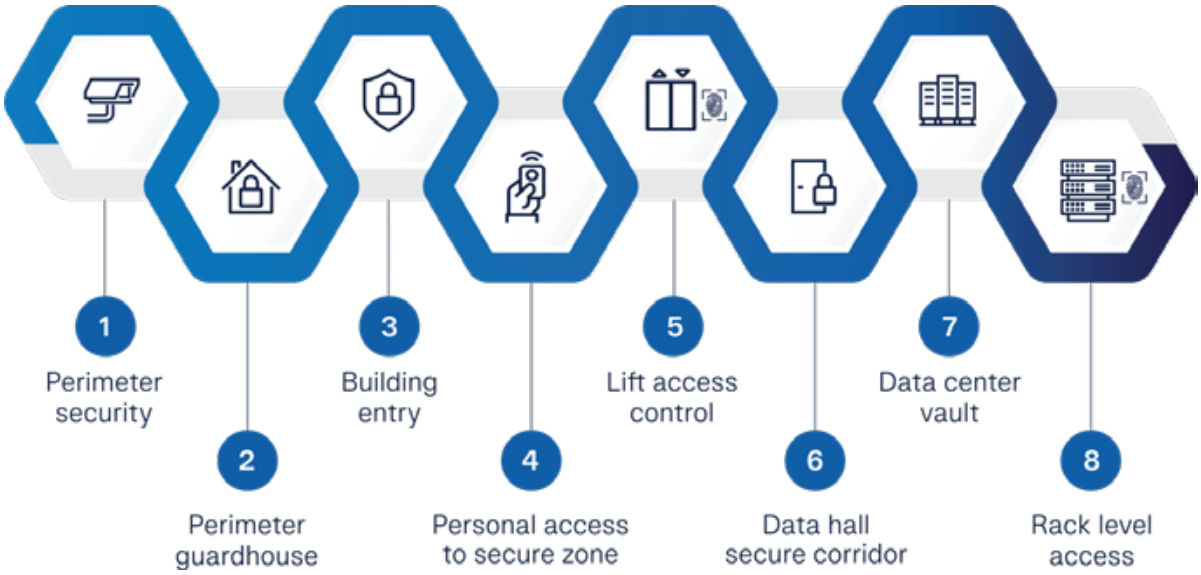


Figure 11: Security Risk Assessment

8. Information Technology & Data Risks

1. **Cyber Attack (General)** – Malicious cyber incidents like hacking, malware, ransomware encrypting data.

2. **Phishing/Social Engineering** – Staff or students being tricked into giving away credentials, leading to breaches.

3. **Data Privacy Breach** – Personal data of students/staff (addresses, grades, health info) leaked or exposed, violating privacy rights and laws.

4. **Legacy Systems** – Outdated IT systems that are no longer supported, at risk of failure or security holes.

5. **Inadequate IT Capacity** – Systems not scaled for peak loads (e.g., registration system crashing when too many students enroll at once).

6. **Cloud Service Dependency** – Heavy reliance on cloud providers (for LMS, email, etc.) – if they have outages, the university is crippled. Also risk of vendor lock-in or losing data if vendor fails.

7. **IT Project Failure** – Large IT implementations (new ERP, etc.) running into serious issues – delays, cost overruns, or not meeting requirements, affecting operations.

8. **Lack of IT Skills** – IT department not having sufficient expertise in new technologies (like cybersecurity, AI, etc.), increasing risk of misconfigurations or inability to respond.

9. **Bring Your Own Device (BYOD)** – Security risks from personal devices connecting to network (if not managed, one infected laptop could spread malware).

10. **Intellectual Property Theft (Cyber)** – Theft of research data or intellectual assets via hacking (state-sponsored attacks on research, etc.).

11. **Social Media Account Hacks** – University's official social media or website being hacked/defaced, causing misinformation or embarrassment.

12. **Poor Data Quality** – Risk that data in systems (like student records or finance) is inaccurate due to errors, leading to faulty decisions or reports.

13. **Lack of Data Governance** – No clear policies on data retention, classification, which can lead to either loss of important data or over-retention (violating privacy).

14. **Emerging Tech Ethics** – Misuse of emerging tech on campus (like facial recognition for attendance raising privacy issues, or AI usage raising plagiarism concerns).

15. **Audio-Visual Tech Failure** – Failure of classroom tech (projectors, online class systems) frequently, disrupting teaching.

16. **Research Computing Downtime** – High-performance computing clusters or lab instruments computer controls failing, delaying research experiments.

17. **Email Spoof/Scam** – Not exactly security breach, but risk that scammers impersonate university officials via email causing financial fraud (e.g., tricking finance to pay a fake invoice).

18. **Regulatory Tech Compliance** – Non-compliance with tech-related regulations (like storing data in certain jurisdictions if law requires local storage).

19. **Misconfiguration** – IT admin error causing exposure (like leaving a database open, or accidentally emailing sensitive data to a group).

20. **Tech Vendor Support Risk** – If a critical software's vendor stops support or goes out of business, leaving the university in a lurch with that system.

9. Research Risks

(Some overlap with other categories but focusing on research context.)

1. **Research Misconduct** – Plagiarism, falsification, or fabrication of research data by researchers, leading to retractions and loss of credibility.
2. **Lab Safety Compliance** – Non-compliance with research safety protocols (radiation safety, biosafety, chemical safety) leading to accidents or sanctions.
3. **Human Subjects Research Risk** – Ethical or legal issues in research involving humans (not getting proper consent, data breaches of participant info, etc.).
4. **Animal Research Risk** – Non-compliance with animal research regulations, risking penalties and public outcry.
5. **Grant Mismanagement** – Funds from grants not used according to conditions, or poor accounting leading to penalties or having to refund agencies.
6. **Intellectual Property Disputes** – Conflicts over IP rights from research (e.g., between university and faculty/inventors, or with sponsors).
7. **Tech Transfer Failure** – Not successfully licensing or commercializing viable research innovations due to weak tech transfer processes (opportunity risk).
8. **Restricted Research Breach** – Violating rules on restricted research (e.g., conducting export-controlled research without clearance, or publishing something sensitive).
9. **Collaboration/Partnership Risk** – Issues with research collaborations (one partner not delivering, or conflict arises over authorship, etc., jeopardizing project).
10. **Research Funding Concentration** – Over-reliance on one funding source (like one government department); if priorities change, many projects may lose funding simultaneously (similar to point 6 of Financial Risks).
11. **Grad Student Risk** – Dependency on graduate students for research; issues like grad student strikes or shortages affecting research continuity.
12. **Research Equipment Failure** – Critical research equipment breakdown with long repair times, halting research (especially if single-copy equipment).
13. **Data Management in Research** – Loss or theft of research data (could be due to IT issues or lab mishandling) compromising years of work.

14. **Publication Risks** – Failure to publish enough (affecting rankings or funding metrics) or sensitive research getting published causing controversy (e.g., dual-use research that can be misused).

15. **Peer Review / Rejection Risk** – High rejection rates of proposals due to certain issues, leading to funding drought (if something systemic like not addressing ethical considerations well).

16. **Field Research Hazards** – For researchers working offsite (geologists, anthropologists, etc.), risks like field accidents or geopolitical risks in research locations.

17. **Industry Partnership Ethics** – Risk that partnering with certain industries (e.g., tobacco, defence) could cause ethical backlash or conflict with university values.

18. **Competition for Talent in Research** – Inability to recruit star researchers or loss of key researchers to other institutions, weakening research output (overlaps HR1, but research-specific impact).

19. **Scientific Reproducibility Risk** – A more esoteric one: if the institution's research is found to be largely non-reproducible, it could hurt reputation (part of broader concern in science community).

20. **Research Infrastructure Capacity** – Not enough lab space or facilities for research needs (leading to turning down projects or overbooking labs, affecting output).

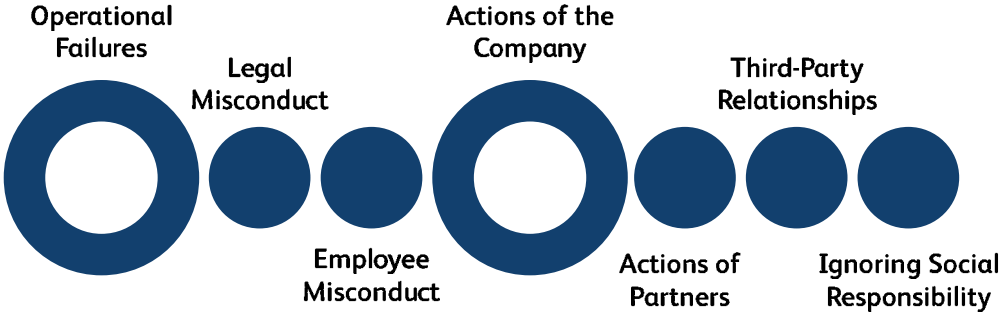
10. Reputation & External Relations Risks

1. **Media Crisis** – Negative press coverage on an issue (e.g., a scandal, controversial speaker on campus, handling of an incident) causing public outrage or image damage.

2. **Social Media Backlash** – Viral spread of negative stories or misinformation about the university on social platforms, potentially from a small incident blown up.

3. **Alumni/Public Perception Erosion** – Alumni or public losing trust in the institution due to cumulative issues or one big incident (affecting donations, support).

Figure 12: TYPES OF REPUTATIONAL RISKS



4. **Town & Gown Relations** – Poor relationship with the local community or authorities (e.g., disputes with city over zoning, student behaviour off-campus causing friction) harming reputation and operations.

5. **Government Relations Risk** – Actions or stance by the university upsetting government officials or regulators (maybe due to research topics or campus activism), leading to punitive responses or loss of support.

6. **Miscommunication** – University communication failures (wrong info released during crisis, or tone-deaf statements by officials) exacerbating situations and drawing ridicule/ire.

7. **Rankings Drop** – Significant drop in university rankings (national or global) which can hurt reputation and subsequent enrolment of quality students/faculty.

8. **Athletics Scandal** – If the university has a sports program, any scandal (like athlete misconduct, recruiting violations) can cause media storms and NCAA or equivalent penalties.

9. **Notable Alumni/Staff Misconduct** – A very prominent faculty or alum involved in controversy (unrelated to the university directly) but by association affects the university's name.

10. **Cultural Insensitivity Incident** – An event or remark on campus that is seen as culturally or racially insensitive, leading to protests and reputation damage if not handled properly.

11. **Mismanagement of Endowment or Funds** – Public revelation of poor financial management or lavish spending of public money can anger stakeholders and damage credibility.

12. **Failure in Corporate Social Responsibility** – University criticized for not living up to social responsibilities (like not being environmentally conscious, or not contributing to community).

13. **Crisis Response Failure** – The institution's perceived failure to respond adequately to a crisis (e.g., slow response to a campus crime) becomes a story of its own.

14. **Opposition to Change** – If undertaking controversial changes (like cutting certain programs or changing mascots), risk of alienating some stakeholders (reputational cost with that segment).

15. **External Activism** – Risk of being targeted by activist groups (e.g., animal rights protests for research, free speech activists for policies) which can bring reputational challenges.

16. **Misaligned Public Statements** – University official takes a stance on a sensitive public issue (e.g., political) that polarizes stakeholders, possibly affecting donor or applicant pools.

17. **Crisis of Trust** – A broad risk that stakeholders (students, parents, faculty) lose trust in leadership due to cumulative issues, which can manifest as petitions, calls for resignation etc., harming stability.

18. **International Relations Risk** – For universities with global footprint: geopolitical events (like deterioration of relations between countries) impacting partnerships or student exchange, and possibly image if seen as aligned with one side.

19. **Brand Dilution** – If the university affiliates with too many external colleges or franchises its brand (common in some places), risk that a partner's poor quality tarnishes main brand.

20. **Intellectual Climate** – Reputation risk if the university is seen as either too restrictive or too lax on intellectual freedom (e.g., cancelling speakers vs allowing hate speech) – balancing act risk.

11. Environmental & Infrastructure Risks

1. **Environmental Sustainability Risk** – Not meeting societal expectations or upcoming regulations on sustainability (carbon footprint reduction, sustainable campus) leading to image damage or compliance issues.

2. **Climate Change Impact** – Long-term risk of climate change on campus (e.g., rising temperatures, more severe weather affecting infrastructure and costs).

3. **Environmental Hazards** – Campus built on or near environmental hazards (like a polluted site) – risk of exposure or expensive remediation.

4. **Energy Supply Risk** – Electricity or gas shortages (especially if dependent on a single grid or provider) impacting campus operations.

5. **Aging Infrastructure** – Buildings, pipes, electrical systems aging beyond life span, risk of major failures or safety hazards (could cause flooding from pipe burst, etc.).

6. **Capital Project Quality** – Risk that new buildings are poorly constructed (perhaps due to contractor issues), leading to future problems and costs.

7. **Space Utilization Risk** – Not enough physical space for planned growth (or misallocation of space) hindering initiatives; or underutilized space wasting resources – a strategic facility planning risk.

8. **Accessibility Compliance** – Infrastructure not fully accessible (for disabled persons) as required, leading to legal and ethical issues.

9. **Geotechnical Risk** – If campus in earthquake zone or unstable soil, risk of ground issues impacting structures (sinkholes, etc.).

10. **Traffic & Parking** – Insufficient parking or poor traffic management leading to accidents, road rage, deterrence of campus visitors (also community relation issue).

11. **Master Plan Risk** – Not following or updating campus master plan can lead to haphazard development and future infrastructure clashes (like building a facility where expansion was needed).

12. **Construction Safety** – Accidents at construction sites on campus (workers injured, debris harming passersby) – linking to contractor management.

13. **Historical Building Preservation** – If campus has heritage structures, risk of their deterioration or conflict between preservation vs modern needs.

14. **Utility Cost Surge** – Operational risk that costs for electricity, water, etc. dramatically increase (fuel price spikes), impacting budget (financial but tied to environment factors).

15. **Pollution Liability** – If the university causes pollution (labs releasing chemicals, etc.), risk of environmental fines and cleanup costs.

16. **Commuting Disruptions** – If large fraction commute by public transit, strikes or transit disruptions in city can affect class attendance (external dependency risk).

17. **Epidemic in Animal Facilities** – If have farm or vet facilities, an outbreak (like avian flu in a poultry research farm) could cause quarantines or culling, affecting research and finances.

18. **Campus Expansion Community Impact** – New buildings affecting neighbours (shadows, noise) causing disputes or legal challenges slowing projects.

19. **Water Supply Contamination** – Risk that campus water supply gets contaminated (from source or internal pipes) leading to health emergency.

20. **Waste Management Risk** – Improper handling of waste (general or hazardous) causing health/safety hazards or regulatory trouble.

This taxonomy is extensive, but it demonstrates the wide scope of risks that a comprehensive ERM program in higher education will consider. Universities should review such a list and identify which risks are applicable to them, which are currently being managed well, and which might be blind spots. Each risk listed here would ideally have a

definition and owner if relevant to the institution. Not all will make it to a "top risks" list, but awareness is the first step to resilience.

For regulators, understanding this breadth underscores why requiring or encouraging ERM in universities is vital – it's not just financial risks, but everything from student well-being to national compliance to global events can impact an institution. Regulators might use a taxonomy like this to guide audit or review checklists (e.g., ask institutions how they manage each category of risk).

Case Study: Using the Risk Library

Problem Statement

Critical blind spots are overlooked by universities due to lack of knowledge on broad categories of risks.

Context

When "Hillview University" (the name of the institute has been masked to preserve anonymity) built its risk register, they started with a taxonomy similar to the above. Each department was given the category list and asked: "do you have any risks in these areas?" This prompted some departments to recognize issues they hadn't thought of as risks. For example, the library department saw "IT/Cyber" on the list and realized they had a risk around their digital repository security. The athletics department, seeing "Athletics scandal" under reputation, formalized a risk about NCAA compliance which they had informally worried about. The risk office compiled a master list and found over 150 risks. They categorized them and noticed that Operational and Compliance risks were the most populated categories, while Strategic risks though fewer in number had very high potential impact. By having this library, when the Board Risk Committee met, they were impressed by the comprehensiveness and could focus on thematic are as rather than individual silo issues. Over time, Hillview's list shrank to about 100 active risks as some were retired or merged, but each year during the annual risk workshop they revisit the master list to see if any previously inactive risk is emerging (for instance, after a few quiet years, "Global pandemic" was on their list in 2019 but low priority – in 2020 it moved to top, validating why it was good they at least had considered it).

Learning Outcomes

This case illustrates the value of a broad taxonomy: it acts as a safeguard against collective blind spots and helps educate new managers about the full spectrum of institutional risks.

CHAPTER 7: RECOMMENDATIONS FOR POLICY MAKERS AND REGULATORY BODIES

7.1. Mandate ERM in Accreditation Rubrics

Why This Matters

Accreditation is the primary lever regulators use to influence institutional behavior. By integrating ERM explicitly into accreditation criteria, UGC and NAAC signal that anticipating and managing uncertainty is as vital as academic quality or infrastructure.

Key Parameters

1. **ERM Policy & Governance**
   - **Board Resolution:** Evidence of a Board/Vice-Chancellor resolution formally adopting an ERM policy.
   - **Risk Governance Structure:** Organizational chart showing a CRO, Risk Management Committee (RMC) and appointed risk owners at departmental level.
2. **Risk Management Process**
   - **Risk Register Submission:** A snapshot of the master risk register, demonstrating at least two cycles of identification, scoring (Likelihood × Impact), and treatment planning for the Top 10 enterprise risks.
   - **Risk Assessment Methodology:** Clear description of qualitative (workshops, surveys) and quantitative (risk scoring scales, simulation) tools used.
3. **Monitoring & Continuous Improvement**
   - **Key Risk Indicators (KRIs):** At least five institution-wide KRIs, with baseline values, thresholds, and current readings.
   - **Control Effectiveness Reviews:** Evidence that controls for Top 5 risks have been tested (internally or via third-party assurance) within the last 12 months.

Implementation Roadmap

- **Phase 1 (Next Accreditation Cycle):** Require submission of ERM policy, governance structure, and an initial risk register.
- **Phase 2 (Cycle +1):** Introduce evaluation of process maturity (e.g., frequency of RMC meetings, percentage of departments with active risk owners).
- **Phase 3 (Cycle +2):** Include outcomes metrics—such as reduction in risk incident frequency or improved response times—as part of accreditation scoring.

7.2. Incorporate Risk Governance Metrics into NAAC/NIRF Evaluations

Why This Matters

Beyond policy presence, regulators must measure capability. By scoring universities on tangible risk governance KPIs, NAAC and NIRF will incentivize not just "ERM on paper" but real organizational competence.

Detailed Indicators

1. **Chief Risk Officer (CRO) Capability**
   - **Qualification Index:** Percentage of CROs holding IRM qualifications (e.g., IRM Level 5 Diploma or equivalent).
   - **Tenure & Independence:** CRO's average tenure and evidence of direct reporting to the Board or Audit & Risk Committee without operational conflicts.
2. **Risk Team Strength**
   - **IRM Exam Pass Rate:** Number of senior officers (Deans, Finance Head, Registrar, IT Head, Student Affairs Head) who have passed IRM Level 3 or above, normalized per 1,000 faculty/staff.
   - **Training Hours**: Average annual ERM training hours completed per risk owner (target: ≥ 16 hours/year).
3. **Committee Performance**
   - **Meeting Frequency & Attendance:** RMC's scheduled vs. actual meetings per year (target: ≥ 4 meetings/year) and member attendance rate (target: ≥ 90 %).
   - **Agenda Composition:** Proportion of agenda items dedicated to risk topics (target: ≥ 50 % of agenda).
4. **Risk Culture & Awareness**
   - **Survey Score:** Results of an annual Risk Culture Survey (e.g., percentage of respondents who "agree" or "strongly agree" that they can report risks without fear).
   - Incident Reporting Rate: Number of "near miss" or risk-event reports per 100 employees, indicating a proactive reporting culture.

Integration into Evaluations

- **NAAC:** Add a "Risk Governance" sub-criterion worth 4 % of the overall Governance and Leadership score, assessed via a standardized Risk Governance Scorecard.
- **NIRF:** Create a new parameter "Risk Preparedness & Oversight" under Institutional Processes, with a maximum of 25 points, calculated from self-reported data and verified by peer evaluators.

7.3. Develop a National Risk Framework for Education (NRFE)

Why This Matters

Diverse ERM approaches across thousands of HEIs lead to incomparable data and uneven quality. A national framework provides consistency, speeds up adoption, and enables sectoral benchmarking.

Framework Components

1. **Governance Architecture**
   - **Model Orgnization Chart:** Board Risk Committee $\rightarrow$ ERM Steering Committee $\rightarrow$ Risk Owners Network across faculties and functions.
   - **Charters & TORs:** Standardized Terms of Reference for each governance body, specifying roles, authorities, and reporting lines.
2. **Process Standards & Tools**
   - **Risk Identification Protocol**: Templates for workshops, surveys, and scenario analyses, including guidance on stakeholder mapping.

- **Risk Analysis Methods:** Step-by-step instructions for scoring (e.g., defined scales for Likelihood and Impact, Monte Carlo guidelines for financial risks).
- **Treatment Planning SOP:** Guidelines for designing mitigation actions, assigning owners, setting deadlines, and tracking resource allocations.

3. **Risk Taxonomy & KRI Library**
   - **200+ Defined Risks:** Categorized by theme (Strategic, Financial, Operational, Compliance, IT, etc.) with standardized definitions.
   - **Sample KRIs:** For each risk category, two to five example indicators with measurement guidance (e.g., "Percentage of systems with unpatched vulnerabilities").
4. **Reporting Templates**
   - **Executive Dashboard:** Heat maps, tolerance lines, trend arrows, and risk appetite comparisons suitable for Board packs.
   - **Quarterly Report:** Structured template for RMC presentation, including Top 5 risk deep-dives with root-cause analysis.

Governance & Maintenance

- Constitute an NRFE Steering Committee under UGC, with representatives from IRM India, NAAC, NIRF Secretariat, and five regional CROs.
- Hold biannual review workshops to update the taxonomy and KRIs (incorporating emerging risks like AI ethics, climate adaptation).

7.4. Driving Funding & Policy Incentives

Linking ERM to Funding

- **Risk Maturity Grants:** Establish a scheme under RUSA or Innovation Funds that provides additional funding to institutions achieving "Mature" or "Optimized" risk maturity ratings as per NRFE.
- **Performance-Linked Funding Disbursement:** Tie disbursement timelines of grants (e.g., research or infrastructure) to compliance with ERM deliverables—delayed ERM reporting leads to staggered grant release.

Policy Levers

- **Fast-Track Approvals:** Institutions demonstrating high ERM maturity receive expedited regulatory approvals for new programs or campus expansions.
- **Recognition & Awards:** Annual "National ERM Excellence Awards" for HEIs that showcase innovative risk practices, judged by a panel of regulators and IRM experts.

By adopting these technically detailed recommendations—spanning accreditation mandates, KPI integration, national frameworks, observatory functions, and supplementary parameters—policy-makers will catalyze deep-rooted, measurable ERM adoption across India's higher education sector. The outcome will be a network of institutions capable of anticipating and navigating uncertainty, thereby safeguarding student outcomes, research continuity, and public investment in education.

CHAPTER 8 - CONCLUSION AND RECOMMENDATIONS

Implementing Enterprise Risk Management in India's higher education sector is not just about preventing disasters – it is a strategic enabler for universities to achieve their goals sustainably. As we have detailed in this white paper, a step-by-step approach grounded in global best practices (ISO 31000, COSO ERM 2017, IRM) and enriched by IRM's insights on culture and appetite can significantly enhance the resilience of HEIs. By establishing strong governance (with qualified CROs and risk committees), fostering an open risk culture, clearly defining the institution's risk appetite, and systematically managing a comprehensive range of risks, universities can navigate uncertainties with confidence.

For regulators and policy-makers, we offer the following recommendations:

- **Promote ERM Adoption through Guidelines**: Bodies like UGC or AICTE could issue guidelines or frameworks encouraging universities to adopt ERM, much like corporate governance codes in the corporate sector. This could include recommending the formation of Risk Management Committees and periodic risk reporting. Regulators can reference ISO 31000 or COSO as accepted standards, which gives institutions a clear target to aim for.

- **Include ERM in Accreditation Criteria**: Incorporating risk management practices as a criterion in accreditation (NAAC or NBA evaluations) would incentivize institutions to build ERM capabilities. For example, NAAC could assess whether the institution has a risk management policy, evidence of risk assessments, and how it handles risks in practice (similar to how they assess governance and finance).

- **Capacity Building and Training**: Regulators can facilitate workshops or training for university leaders on ERM. Partnering with organizations like IRM India or professional bodies to create certified courses for education sector risk management can build a pipeline of qualified CROs and risk champions. An example is IRM India's efforts to work with AICTE to identify gaps in ERM knowledge; such collaborations can be expanded.

- **IRM-Qualified CROs as a Best Practice**: While not every institution may afford a full-time CRO initially, regulators can encourage at least one senior officer to obtain an IRM or similar certification and handle the risk portfolio. Perhaps in the future, having an "ERM Officer" could become as standard as having an internal audit or compliance officer in universities.

- **Sharing of Risk Intelligence**: Create forums for universities to share their top risks and mitigation success stories (maybe via associations or annual reports). This peer learning can be extremely valuable – e.g., if one college effectively handled a new cyber threat, others can emulate that quickly. Regulators might even collect anonymized risk data to identify sector-wide risks (for instance, if many institutions report "student mental health" as high risk, the ministry could allocate resources or mandate student support improvements sector-wide).

- **Balance Autonomy and Accountability**: As Indian higher education moves towards greater autonomy for institutions (per NEP 2020), ERM should be seen as the internal mechanism that provides accountability. Universities that embrace ERM demonstrate

that autonomy will be exercised responsibly, reducing the need for micro-management by regulators. It's a win-win: regulators get assurance of good governance, institutions get freedom to innovate but with prudent risk oversight.

- **Continuous Oversight**: Regulators can require an annual "Risk Management Statement" from universities (just like companies issue an internal control/risk statement in annual reports). This could outline major risks and how they are managed. Such disclosure drives seriousness in ERM implementation and keeps stakeholders informed.

For university leaders and board members, the journey to embed ERM is a commitment to proactive leadership. Start small but start earnestly: maybe begin with identifying the top 10 risks and forming a committee to monitor them – you will likely see quick benefits in better decision alignment and fewer surprises. As the culture matures, broaden the scope and formalize the processes as described in this guide. Remember that ERM is an ongoing cycle – make it part of the institution's DNA. When a risk materializes (e.g., a crisis hits), an institution with ERM will respond in a coordinated, confident manner rather than in panic. That difference in response can save lives, save money, and save reputations.

In conclusion, building resilience in higher education through ERM is both necessary and achievable. Indian universities stand at an inflection point where global competition, technological disruption, and public scrutiny are intensifying. Embracing a step-by-step ERM implementation can transform these challenges into managed risks and even opportunities. A university that knows its risks is a university that knows itself – its limitations and its potential. By following the roadmap in this guide and customizing it to their context, institutions will not only guard against adverse events but also gain strategic clarity and agility. Regulators, on their part, should foster an ecosystem where such prudent risk management is the norm. The ultimate beneficiaries are the students and society at large – who can trust that our higher education system is robust, forward-looking, and prepared for the future.

Let this white paper serve as a practical manual and a call to action: Integrate risk management into the heart of higher education governance. Doing so will ensure that our universities can fulfil their crucial mission of education and innovation in good times and bad, come what may.

CHAPTER 9 – ANNEXURES

To support practical implementation and provide ready-to-use resources, the following annexures are included. Each template and tool can be customized to fit an institution's unique context and maturity level.

Annexure 1: Sample ERM Policy Template for Universities

A comprehensive policy document aligned with ISO 31000:2018 and COSO ERM 2017, covering:

- **Purpose & Scope** – Definition of ERM's objectives, applicability across all campuses, functions, and activities.
- **Principles & Commitments** – Leadership endorsement, integration with strategic planning, continuous improvement, and stakeholder engagement.
- **Governance Structure** – Roles for Board/Risk Committee, Chief Risk Officer (CRO), ERM Steering Committee, and departmental risk owners.
- **Process Overview** – End-to-end ERM cycle (Context → Identify → Analyse → Evaluate → Treat → Monitor), with cross-references to ISO 31000 clauses.
- **Reporting & Review –** Frequency of risk reports, key metrics (KRIs), and annual policy review procedures.

Annexure 2: Sample Risk Appetite Statement

A board-approved declaration articulating the university's tolerance and thresholds for major risk categories:

- **Strategic & Growth Risks** – Moderate appetite for expansion initiatives; appetite line at a 15 percent variance from planned enrolment targets.
- **Financial Risks** – Low appetite for budget deficits; hard tolerance of a 2 percent operating deficit.
- **Compliance & Ethical Risks** – Zero tolerance for regulatory breaches or academic misconduct.
- **Safety & Security Risks** – Minimal tolerance for incidents causing bodily harm; all such risks must be mitigated to a residual score of "Low."
- **Reputational Risks** – Conservative appetite; reputational incidents require Board review before public response.

Annexure 3: Roles & Responsibilities Matrix for Risk Governance

A RACI-style matrix mapping ERM roles to key activities:

Activity	Board/Risk Committee	CRO	ERM Steering Committee	Risk Owners	Internal Audit
Approve ERM Policy	R	C	I	I	I
Define Risk Appetite	A	C	C	I	I
Conduct Enterprise Risk Assessment	I	A	R	R	C
Develop Treatment Plans	I	A	R	R	I
Monitor KRIs & Controls	I	R	A	R	C
Report Top Risks to Board	I	A	R	C	I
Provide Assurance on ERM Effectiveness	I	I	I	I	A

(R = Responsible, A = Accountable, C = Consulted, I = Informed)

Annexure 4: Sample Risk Heat Map

A 5×5 matrix plotting Likelihood (Rare to Almost Certain) against Impact (Negligible to Catastrophic), with:

- **Colour Zones:** Green (Low), Amber (Medium), Red (High).
- **Appetite Lines:** A diagonal threshold showing the maximum acceptable risk score (e.g., scores ≥ 15 fall above appetite and require immediate action).
- **Example Plot:** Ten sample risks mapped (e.g., "Cyberattack" at Almost Certain × Major Impact = Red zone).

Annexure 5: Six Indian Case Studies of ERM in Action

Below are six anonymized, composite case studies. Each illustrates a significant risk event, its root cause, the impact incurred, and how the university applied ERM principles-supported by IRM-based training—to resolve the issue and build resilience.

Case Study 1: Midwest State University – Laboratory Safety Breach

Risk Event:

During routine experimentation, a researcher at Midwest State University inadvertently mixed incompatible chemicals in an unhoused fume hood, triggering a violent reaction. The ensuing gas leak forced evacuation of the entire laboratory wing. Although no fatalities

occurred, three staff members suffered respiratory irritation, and research operations halted for 48 hours.

Root Cause:

An internal review uncovered that individual labs had never standardized their hazard assessments. Each faculty member followed their own checklist, and there was no central function to verify safe procedures. Moreover, there was no designated "lab risk owner" responsible for auditing chemical storage compatibility or for ensuring fume hood maintenance.

Impact:

- **Human:** Three hospitalizations for respiratory distress (all recovered).
- **Operational:** Loss of critical data in ongoing experiments; project timelines delayed by weeks.
- **Financial:** Emergency response costs (₹2 lakhs) plus cleanup and restocking laboratory supplies (₹5 lakhs).
- **Reputational:** Media coverage of "unsafe lab conditions" prompted concern among accreditation bodies.

ERM Solution & Outcomes:

The newly appointed IRM-certified Chief Risk Officer (CRO) spearheaded a comprehensive ERM intervention. First, all lab managers completed IRM's Risk Culture module to understand standardized hazard assessment protocols. Next, the CRO established a central "Laboratory Risk Register," assigning each department a risk owner responsible for monthly safety audits. Quarterly tabletop exercises—modeled on IRM's scenario-planning guidelines—tested incident response. Within six months, no further safety breaches occurred, and accreditation auditors praised the systematic approach to lab safety.

Case Study 2: Coastal Central Institute – Financial Aid Fraud Scheme

Risk Event:

Coastal Central Institute discovered that dozens of scholarship awards had been fraudulently approved by a staff member colluding with third-party agents. Applicants submitted forged income certificates, and the staff member bypassed verification controls, diverting roughly ₹30 lakhs in scholarship funds to ineligible candidates.

Root Cause:

The institute's disbursement process lacked dual-control checkpoints. Finance staff were pressured to expedite awards before semester start, and no independent verification of supporting documents was mandated. Moreover, no training on financial-fraud risks had been provided, so staff were unaware of red-flag indicators.

Impact:

- **Financial:** Direct loss of ₹30 lakhs, which had to be recouped through emergency reallocation from operating reserves.
- **Operational:** Scholarship deliveries to genuine students delayed, causing protests and enrolment complications.
- **Reputational:** Parent and student trust eroded; several donors threatened to withdraw future funding.

ERM Solution & Outcomes:

Under guidance from IRM's Financial Risk module, the CRO reengineered the disbursement workflow to include automated document verification and mandatory second-level approval by a designated "Scholarship Risk Officer." All finance personnel underwent IRM-approved training in fraud detection and risk assessment. The institute also introduced a Fraud KRI—the ratio of flagged applications to total awards—to monitor trends. In the following academic year, fraudulent approvals dropped to zero, and donor confidence rebounded, restoring full scholarship funding.

Case Study 3: Northern Tech University – Ransomware Attack on Student Records

Risk Event:

Late one evening, hackers deployed ransomware on Northern Tech University's central student information system, encrypting all enrollment, grades, and personal data. The attackers demanded a ransom of ₹10 lakhs in cryptocurrency. With no viable backups accessible, the university faced a two-day complete system shutdown.

Root Cause:

A vulnerability assessment revealed that critical servers had not been patched for known exploits for over six months. There was no documented cyber-risk appetite governing acceptable levels of vulnerability. The IT team had neither formal risk-management training nor an understanding of how to prioritize patch schedules based on risk severity.

Impact:

- **Operational:** Two days of downtime prevented course registration, exam scheduling, and transcript requests.
- **Financial:** ₹5 lakhs paid to data-recovery vendors; estimated ₹3 lakhs lost in productivity.
- **Stakeholder Confidence:** Students and parents expressed frustration; regulatory bodies issued compliance warnings.

ERM Solution & Outcomes:

Northern Tech's IRM-qualified CRO immediately convened a cyber-risk workshop, using IRM's Risk Appetite and Tolerance Guide to define a Cybersecurity Risk Appetite Statement

(zero tolerance for unpatched critical vulnerabilities older than 30 days). The university's IT Director and two senior analysts completed IRM's Information Security Risk course. A biweekly Vulnerability KRI was instituted to track patch compliance. Additionally, multi-factor authentication and isolated backup servers were deployed. Subsequent audits showed 100 % compliance with patching schedules, and no further ransomware incidents occurred.

Case Study 4: Eastern Arts College – Accreditation Non-Compliance

Risk Event:

In its mid-cycle accreditation review, Eastern Arts College failed to receive renewal due to "inadequate evidence of governance processes." The NAAC peer team noted missing documentation of committee minutes, no formal ERM policy, and insufficient records of risk assessments.

Root Cause:

Although senior leadership often discussed potential risks informally, no formal ERM framework existed. Meetings of ad-hoc risk groups were unrecorded, and there was no centralized policy or risk register. The college had never invested in formal risk-management training.

Impact:

- **Accreditation:** Downgraded from "A" to "B" grade, jeopardizing eligibility for government grants.
- **Financial:** Suspension of a planned ₹50 lakhs research grant until governance issues were addressed.
- **Reputational:** Prospective students questioned the college's stability; application numbers dipped 15 %.

ERM Solution & Outcomes:

Using Annexure 1's ERM Policy template, the newly hired CRO drafted a formal policy aligned with ISO 31000 and COSO 2017 and obtained Board approval within three months. The CRO organized IRM-accredited training sessions for all Deans and administrative heads, creating a common risk lexicon. A central risk register was instituted, and minutes of the newly formed Risk Management Committee were documented and archived. At the next accreditation review, NAAC commended the comprehensive governance overhaul, the college regained its "A" grade, and funding resumed.

Case Study 5: Southern University of Management – Postgraduate Enrolment Collapse

Risk Event:

Over two consecutive years, Southern University of Management experienced a 20 % decline in postgraduate applications in its flagship MBA program. Competing institutions touting online and hybrid delivery models exacerbated the trend, but the university had not anticipated the market shift.

Root Cause:

The university had never conducted a Strategic Risk Assessment for demographic or delivery-model changes. There was no formal risk appetite for enrolment volatility, and marketing efforts continued unchanged despite clear global trends toward digital learning accelerated by the pandemic.

Impact:

- **Financial:** Loss of ₹2 crores in tuition revenue, forcing budget cuts and faculty layoffs.
- **Strategic:** Forced cancellation of planned program expansions and campus renovations.
- Reputational: Ranked lower in national surveys for program competitiveness.

ERM Solution & Outcomes:

Guided by IRM's Strategy & Objective-Setting principles from COSO 2017, the CRO led a scenario-planning workshop with senior leadership, modelling the impact of various enrolment trajectories. A formal Enrolment Risk Appetite Statement was approved by the Board, establishing acceptable thresholds (±10 % year-on-year variance). The marketing and academic teams completed IRM's Strategic Risk module and launched targeted digital offerings and flexible learning pathways. By the next intake cycle, applications rebounded to 95 % of previous levels, stabilizing revenue and enabling the continuation of planned investments.

Case Study 6: Capital City College – Campus Safety Crisis during Student Protests

Risk Event:

A planned student demonstration at Capital City College over campus regulations escalated when a small group vandalized administrative buildings and clashed with security personnel. Multiple students and staff sustained injuries, and local media broadcast images of the unrest nationwide.

Root Cause:

Although student grievances had been rising, no formal risk culture survey or stakeholder-engagement process existed to surface growing concerns. Emergency response protocols were outdated, and the campus security team lacked crisis-management training.

Impact:

- **Safety:** Dozens of injuries requiring medical attention; two serious.
- **Property:** ₹50 lakhs in damages to administrative offices and lecture halls.
- **Legal & Reputational:** Police investigations ensued; negative national coverage shook donor confidence.

ERM Solution & Outcomes:

Capital City's CRO-backed by IRM's Risk Culture and Crisis Management guidance-implemented a multi-pronged ERM response:

1. **Risk Culture Survey:** Conducted an all-campus survey to gauge sentiment, which revealed a breakdown in communication between students and administration.
2. **Crisis Response Plan:** Drafted a detailed Campus Emergency Protocol, including clear escalation paths and media-management guidelines.
3. **Stakeholder Forums:** Instituted monthly "Student-Administration Roundtables" to surface and address issues proactively.
4. **IRM-Certified Training**: Student Affairs and Security Heads completed IRM's Crisis Management and Stakeholder Engagement courses.

Subsequent audits showed a 70 % improvement in the risk culture index, no further protests turned violent, and the college successfully restored its public image through coordinated communication and transparent reforms.

These six case studies demonstrate how structured ERM-underpinned by IRM qualifications and guided by ISO/COSO principles-enables Indian universities to convert crises into learning opportunities, driving sustained improvements in safety, governance, and strategic agility.

LEADERSHIP INSIGHTS ON RISK MANAGEMENT IN HIGHER EDUCATION INSTITUTIONS

I am delighted to know that IRM India and Sri Sri University have joined hands and have prepared a Whitepaper on *Creating Resilient Campuses*. In the days of a VUCA world, AI and its impact on education on one side, how we have to navigate AI challenges and overcome risks posed is a fine balancing act. Risk taking, risk evaluation and risk preparedness are as important for businesses as much as to educational institutes. I am confident this whitepaper will empower our institutes to be prepared to face challenges ahead through innovations and forge ahead successfully. My best wishes.

ANIL SAHASRABUDHE
CHAIRMAN NAAC AND NBA, FORMER CHAIRMAN AICTE

I congratulate Sri Sri University for developing the much needed whitepaper on *Creating Resilient Campuses*. Indian universities can enhance their resilience by adopting structured Enterprise Risk Management approaches tailored to their contexts. Establishing clear risk governance, identifying key vulnerabilities, and crafting mitigation strategies can help institutions weather disruptions effectively. Proactive risk management allows universities to turn challenges into opportunities for growth and improvement. By embedding resilience in their operations, Indian universities can better safeguard their missions and stakeholders.

DR. PANKAJ MITTAL
SECRETARY GENERAL, ASSOCIATION OF INDIAN UNIVERSITIES

Embedding Enterprise Risk Management into the DNA of higher education institutions is no longer optional - it is essential. By fostering a culture of preparedness, accountability, and innovation, our universities can build resilience against uncertainties while ensuring continuity of learning and research. A structured ERM framework not only safeguards governance and reputation but also empowers institutions to thrive amidst change and contribute meaningfully to national development.

PROF. T.G. SITHARAM

CHAIRMAN, AICTE

The evolving global landscape challenges universities to operate with agility and accountability. Enterprise Risk Management provides the framework for sound governance, informed decision-making, and sustained innovation, enabling institutions to navigate complexities with precision and purpose. Our collaboration with Sri Sri University in co-authoring this whitepaper on *Creating Resilient Campuses* reflects a shared dedication to embedding resilience at the heart of academic leadership.

HERSH SHAH

CEO, IRM INDIA AFFILIATE, INDIA'S YOUNGEST ENTERPRISE RISK EXPERT

In an era defined by uncertainty and transformation, building resilient universities requires foresight, governance, and a deep sense of purpose. Enterprise Risk Management must become integral to higher education-guiding leadership decisions, safeguarding institutional integrity, and enabling innovation. The collaboration between IRM India and Sri Sri University in co-authoring this whitepaper on *Creating Resilient Campuses* reflects our shared commitment to developing risk-intelligent, value-based institutions. Guided by Gurudev Sri Sri Ravishankar Ji's vision of blending human values with modern knowledge, we aspire to make Indian higher education a global model of preparedness, accountability, and holistic resilience.

PROF. (MRS.) RAJITA KULKARNI

PRESIDENT, SRI SRI UNIVERSITY

Effective risk management in higher education must move from reactive controls to proactive intelligence. At Sri Sri University, our Enterprise Risk Management framework integrates ISO 31000, COSO ERM, and IRM principles to establish a risk-aware governance culture. This approach ensures that every academic and operational decision aligns with defined risk appetite thresholds, monitored through structured KRIs and stress-testing exercises. The collaboration with IRM India reinforces our belief that universities must institutionalise a Chief Risk Officer function, maintain transparent risk reporting, and participate in sector-wide benchmarking, such as the proposed National Academic Risk Observatory. Through data-driven risk insights, continuous evaluation, and a culture of accountability, we aim to transform resilience from a compliance metric into a strategic differentiator for Indian higher education.

RAVI ONKARI

EX - CHIEF FINANCE OFFICER, SRI SRI UNIVERSITY

About IRM India Affiliate

The Institute of Risk Management (IRM), headquartered in the UK and established in 1986, is the world's leading professional body for Enterprise Risk Management (ERM) qualifications, training & examinations. With 40 years of excellence across 140+ countries, IRM has been at the forefront of driving global risk management standards.

Through IRM India Affiliate, students and professionals across India can register for the ERM exams and pursue a 5-level pathway to Certified Fellowship, earning designations after Level 2. This enables them to join a global community of risk-intelligent leaders.

The IRM India Affiliate is committed to expanding the ERM ecosystem in India by offering the highest standards of education and knowledge, helping organisations achieve better outcomes through IRM qualified risk professionals. IRM is widely recognised as the preferred thought leader in ERM by industries worldwide.

About Sri Sri University

Envisioned by Gurudev Sri Sri Ravi Shankar ji, Sri Sri University was established in 2009 with the mission to reestablish India as a global epicenter for world-class education. The university is rapidly evolving into an international hub for holistic learning, combining the best of Western innovation with the timeless wisdom of the East.

At the heart of Sri Sri University's philosophy is a groundbreaking approach to education that nurtures both intellectual prowess and personal growth. The institution offers a comprehensive array of programs spanning undergraduate, postgraduate, and doctoral levels across diverse disciplines. These include cutting-edge fields such as Management, Computer Engineering, Electric Vehicle Technology, and Forensic Science, alongside traditional areas of study like Ayurveda, Yoga, and Sanskrit & Indic Studies.

The university's curriculum is meticulously designed to foster domain expertise while simultaneously developing crucial life skills, promoting all-round excellence among its students. A unique feature of the educational experience at Sri Sri University is the integration of The Art of Living Programs, which equip students with practical tools to manage stress and enhance creativity effectively. Looking ahead, Sri Sri University is poised to transform into a multidisciplinary educational powerhouse. This expansion will further solidify the university's position as a center of excellence in research and innovation.

With its commitment to blending academic rigor with holistic development, Sri Sri University is set to become a beacon of educational excellence on the global stage. By nurturing well-rounded individuals equipped with both knowledge and wisdom, the university is preparing the next generation of leaders to address the complex challenges of our rapidly evolving world.

IRM India Affiliate
909, Unit No.9, 9th Floor, Corporate Park II,
VN Purav Marg, near Swastik Chambers,
Mumbai, Maharashtra - 400071.
T: +91-7208853274
E: communications@theirmindia.org

Sri Sri University
Sri Sri Vihar, Ward No – 3, Godi Sahi,
Cuttack – 754006, Odisha, India.
T: +91-78944 24562
E: info@srisriuniversity.edu.in

SRI SRI UNIVERSITY
LEARN • LEAD • SERVE

irm
Developing risk professionals