Risk Management Plan

Kalinga Institute of Industrial Technology

Deemed to be University

Bhubaneswar

1.0 Executive summary

This Risk Management Plan (RMP) provides a structured approach to identify, assess, mitigate, monitor, and report risks that could prevent KIIT DU from achieving its strategic, academic, financial, operational, regulatory, and reputational objectives. It assigns clear governance, introduces a consistent risk assessment methodology, and presents prioritized mitigation measures and monitoring processes tailored to a large multidisciplinary university with diverse stakeholders (students, faculty, staff, regulators, industry partners, and the community).

2.0 Objectives

- Identify and categorize institutional risks.
- Assess likelihood and impact to prioritise resources.
- Define mitigation and control measures to reduce exposure.
- Establish governance, roles, and responsibilities for risk oversight.
- Provide monitoring, reporting and review mechanisms to ensure continual improvement and resilience.

3.0 Scope

Covers university-wide risks across: strategic planning, academic & research quality, financial sustainability, operations (campus services), compliance & accreditation, IT & data security, health & safety, human resources, reputation & communications, and environmental & infrastructure risks. Applies to all KIIT campuses, programmes, and affiliated centres.

4.0 Governance & responsibilities

- Executive Council: ultimate oversight; approves risk appetite and major mitigation investments.
- Vice-Chancellor: executive ownership of enterprise risk management.
- Risk Management Committee (RMC): chaired by a Vice-Chancellor and includes Registrar, Directors, Deans, Finance, IT Head, Security, Legal, Student Affairs, and Representatives from key schools. Meets quarterly.
- Chief Risk Officer Risk Coordinator: day-to-day coordination, risk register maintenance, reporting.

- Departmental Risk Champions: faculty/staff nominated in each school/department to identify local risks and implement controls.
- Internal Audit: independent assurance on risk controls and process compliance.
- Crisis Management Team: activated for major incidents (fire, pandemic, data breach, campus violence).

5.0 Risk Identification

1. Strategic Risks
    - Changing higher-education demand, competition, accreditation loss (NAAC/NBA/ABET/IET).
    - Maintaining consistent demand in admissions for core academic subjects amidst shifting student preferences.
    - Creating new academic programs aligned with emerging industry trends and societal needs to remain competitive and relevant.
2. Academic & Research Risks
    - Decline in teaching quality, plagiarism, research misconduct, loss of key faculty.
    - Challenges in updating the curriculum promptly to align with evolving industry requirements and global best practices.
3. Financial Risks
    - Funding shortfalls, fee collection defaults, currency/exchange risks for international programs.
4. Operational & Infrastructure Risks
    - Campus utilities failure, hostel incidents, construction accidents.
5. Compliance & Regulatory Risks
    - Non-compliance with UGC/AICTE/other statutory requirements, visa/regulatory changes.
6. IT & Cybersecurity
    - Data breach, ransomware, service outages affecting Google Workspace / LMS / administrative systems.
7. Health, Safety & Environment

    - Infectious disease outbreaks, laboratory accidents, fire safety failures.
8. Human Resources
    - Labour disputes, shortages of qualified teachers, high attrition rates.
9. Reputation & Communications
    - Social media incidents, negative press, academic integrity scandals.
10. External / Third-Party Risks
    - Vendor failure, partner university withdrawal, natural disasters (cyclone/flood).

6.0 Risk assessment methodology

- Likelihood (L): 1 (Rare) — 5 (Almost Certain)
- Impact (I): 1 (Negligible) — 5 (Catastrophic)
- Risk Score = L × I (1–25).
- Risk Appetite: defined by Board (example: tolerate low to medium operational risk; avoid high reputational or compliance risk).
- Controls: Existing controls reduce inherent risk → produce residual risk. For each risk, identify owner, mitigation actions, timeline, cost estimate, and KPI.

7.0 Prioritized risk register (abridged)

ID	Risk Description	Inherent L	Inherent I	Score	Key Controls / Mitigations	Owner	Residual Score
R1	Loss of major accreditation (NAAC/NBA/ABET/IET)	2	5	10	Continuous SAR/SWOT, internal audits, QA cell, accreditation roadmap	Dean QA	4
R2	Major cyberattack (data breach / ransomware)	3	5	15	Multi-factor authentication, backups, patching, incident response plan, staff training	Head, ICT	6

R3	Large-scale campus health emergency (pandemic/outbreak)	2	5	10	Health protocols, isolation facilities, tele-teaching readiness	Director, Student Affairs	4
R4	Significant decline in enrolment / fee revenue	3	4	12	Market research, diversification of programs, scholarships, industry tie-ups	Registrar / Director, Finance	6
R5	Declining admissions in core academic subjects	3	4	12	Strengthened outreach, alumni engagement, targeted marketing, core curriculum enhancement	Director, Admissions	6
R6	Delay in updating curriculum to match evolving industry requirements	3	4	12	Annual curriculum review cycles, industry advisory boards, faculty–industry collaboration, modular courses	Director, Academics	5
R7	Inability to create new academic programs aligned with industry and societal needs	3	4	12	Continuous market scanning, interdisciplinary course development, partnerships with industry and community	Dean Academics / Program Dev.	5
R8	Major lab safety incident / fatality	2	5	10	Lab safety SOPs, PPE, training, inspections	H&S Officer	3
R9	Reputational crisis due to student/faculty misconduct	3	4	12	Clear conduct policies, communication plan, swift disciplinary procedures	Director, PR	5
R10	Disruption of LMS / Google Classroom affecting teaching	3	3	9	Redundant systems, alternate delivery (recorded lectures), SLA with providers	Assistant Registrar, EAM/ Dean, Academics	3
R11	Natural disaster damaging campus infrastructure	2	5	10	Disaster management plan, insurance, resilient design	Registrar/ Chairman (Safety)	5

8.0 Mitigation strategies (by category)

8.1 Strategic / Accreditation

- Maintain Quality Assurance (QA) cell; institutionalize periodic Self-Assessment Reports (SAR).
- Continuous faculty development, curriculum updates aligned to NBA/ABET/IET criteria.
  Financial
- Diversify revenue (executive education, online programs, industry projects); maintain reserves; strengthen fee collection & financial controls.
  Operational & Infrastructure
- Preventive maintenance schedules; vendor performance management; robust procurement policies.
  IT & Cybersecurity
- Cybersecurity framework (ISO 27001 best practices), regular penetration testing, daily backups with offsite replication, incident response drills.
  Health & Safety
- Regular H&S audits, emergency drills, medical partnerships, clear SOPs for labs and construction sites.
  Compliance & Legal
- Regulatory watch, legal counsel engagement, compliance calendar, training for programme coordinators.
  Reputation & Communications
- Proactive communication strategy, media training for leadership, social media monitoring, transparent incident response.
  Research Integrity
- Research ethics committee, plagiarism checks, data management plans, mentorship for early-career researchers.
  Human Resources
- Succession planning, competitive compensation benchmarks, retention incentives, counselling services.

8.2 Business continuity & crisis response

- Business Continuity Plan (BCP): ensure continuity for key functions (teaching, exams, payroll, admissions, IT).

- Crisis Management Team: predefined roles, contact lists, decision matrix, and emergency communication templates.
- Emergency drills: fire, evacuation, cyber-attack tabletop exercises annually.
- Insurance: adequate cover for property, liability, business interruption, Directors & Officers (D&O) where appropriate.

8.3 Monitoring, reporting & KPIs

- Quarterly RMC reports to the Board summarising top risks, new risks, status of mitigation actions, and residual risk trends.
- Dashboards: track KPIs such as number of incidents, system downtime hours, accreditation action items closed, percentage of risk actions on-track.
- Internal audit performs annual audit of risk controls and reports independently.
- Risk appetite breaches require escalation to the Vice-Chancellor and Board.

8.4 Training & culture

- Regular risk awareness and compliance training for staff and faculty.
- Induction for new employees and students covering safety, IT security, and code of conduct.
- Reward/recognition for departments demonstrating strong risk management practices.

8.5 Review cycle

- Full RMP review annually or earlier if a major incident, regulatory change, or strategic pivot occurs.
- RMC meets quarterly; risk champions report monthly to Risk Coordinator.

8.6 Implementation roadmap (3–12 months)

1. Finalise and approve RMP by Governing Council.
2. Appoint/confirm Chief Risk Officer and departmental Risk Champions.

3. Establish the Risk Register in a central tool (e.g., shared dashboard) and populate with validated scores.
4. Prioritise top 10 risks and allocate budgets for mitigation in the next financial plan.
5. Run tabletop exercises for cyber and health emergencies within 6 months.
6. Integrate RMP controls with internal audit plan and accreditation action plan.