Action Plan 1 for Comprehensive Risk Assessment

By following this action plan and checklist, the higher education institution will be well-prepared to conduct a comprehensive risk assessment, gain valuable insights into its cybersecurity posture, and develop an informed strategy for risk mitigation and cybersecurity improvement.

1. Establish a Risk Assessment Team: Form a dedicated team consisting of cybersecurity experts, IT personnel, and representatives from different departments to lead the risk assessment process.
2. Define Scope and Objectives: Clearly outline the scope and objectives of the risk assessment. Determine the assets and systems to be assessed, the timeframe for the assessment, and the desired outcomes.
3. Gather Documentation: Collect all relevant documentation, including network diagrams, system configurations, security policies, incident reports, and previous risk assessments.
4. Identify Information Assets: Identify and categorise all critical information assets, including research data, student records, financial information, intellectual property, and administrative data.
5. Identify Threat Sources: Identify potential threat sources that could target the institution, including cybercriminals, nation-state actors, hacktivists, and insider threats.
6. Assess Vulnerabilities: Conduct vulnerability assessments to identify weaknesses and potential entry points in the institution's IT infrastructure, applications, and systems.
7. Identify Current Controls: Document the existing security controls and measures in place and evaluate their effectiveness in mitigating identified risks.
8. Conduct Interviews and Workshops: Engage with stakeholders, including faculty, staff, students, and IT personnel, through interviews, workshops, and surveys to gain insights into their security concerns and perspectives.
9. Review Incident History: Analyse past security incidents and breaches to identify patterns and trends that can inform potential risks.
10. Perform Threat Modeling: Create threat models specific to the institution's environment, considering the potential impact and likelihood of various threat scenarios.
11. Conduct Risk Analysis: Assess the identified risks based on their potential impact, likelihood, and the effectiveness of existing controls. Prioritise risks based on their severity.
12. Risk Mitigation Recommendations: Develop risk mitigation recommendations and propose security controls to address the identified risks effectively.
13. Cost-Benefit Analysis: Conduct a cost-benefit analysis for proposed security controls to ensure they are feasible and align with the institution's budget constraints.
14. Report and Presentation: Prepare a detailed report summarising the risk assessment findings, including a risk register, recommended actions, and a prioritised roadmap for implementation.

Action Plan 1 Checklist

✅Formed a dedicated risk assessment team

✅Defined the scope and objectives of the risk assessment.

✅Gathered all relevant documentation and information.

✅Identified and categorised critical information assets.

✅Identified potential threat sources.

✅Conducted vulnerability assessments.

✅Documented existing security controls.

✅Engaged with stakeholders through interviews and workshops.

✅Reviewed past incident history.

✅Developed threat models.

✅Analysed risks based on impact and likelihood.

✅Prioritised risks based on severity.

✅Developed risk mitigation recommendations and security controls.

✅Conducted cost-benefit analysis for proposed controls.

✅Prepared a detailed report with a risk register and prioritised roadmap.