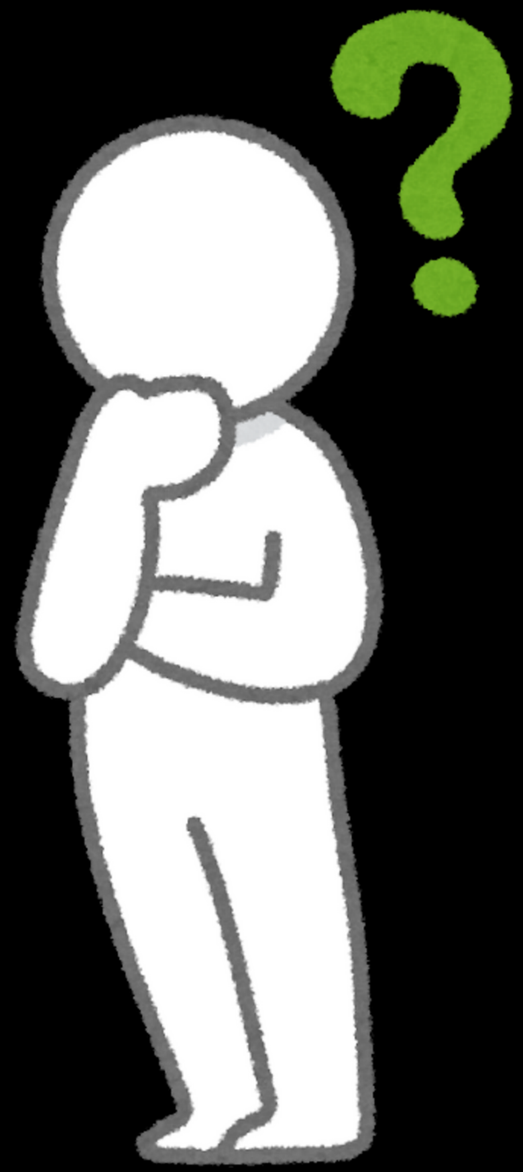
RISK ANALYSIS

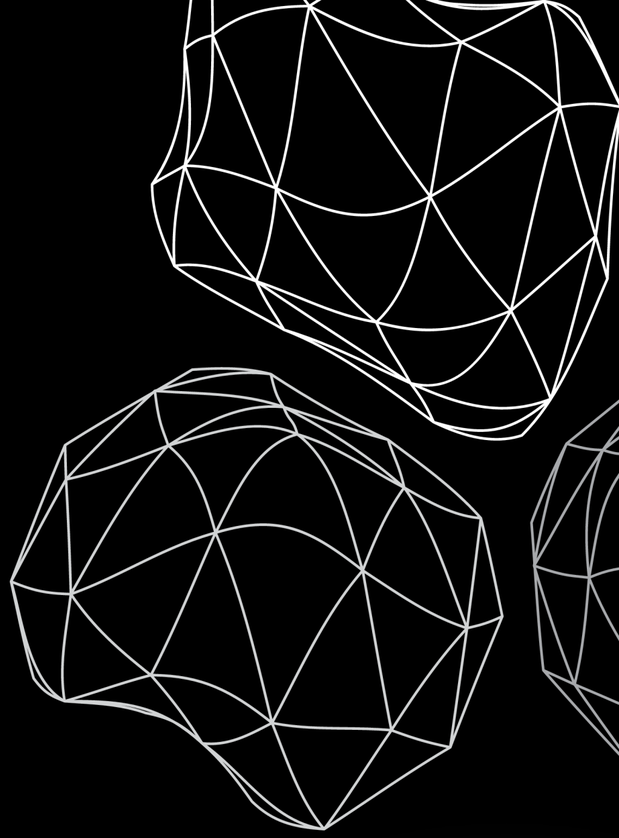
ISRM PROJECT

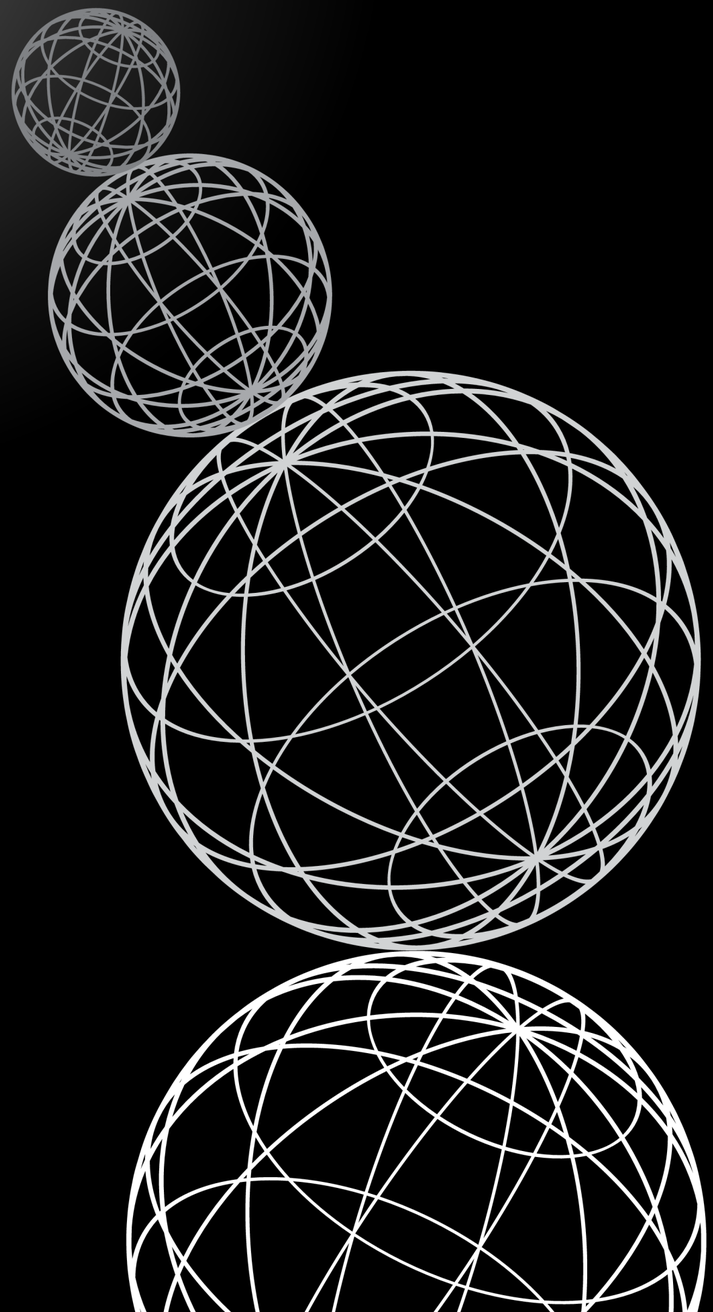
SLIIT

WHAT IS RISK GOVERNANCE?

Risk Governance is the system of policies, processes, roles, and responsibilities an organization uses to identify, assess, manage, and monitor risks—especially in areas like cybersecurity.







IN CYBERSECURITY CONTEXT:

Risk Governance includes:

- Creating cybersecurity policies (e.g., password rules, data usage)
- Defining roles (e.g., who is responsible for IT and security?)
- Ensuring compliance with regulations (e.g., Sri Lanka Data Protection Act)
- Approving security budgets and monitoring risk mitigation efforts

HOW RISK GOVERNANCE FITS IN THE OCTAVE FRAMEWORK

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) focuses on:

1. Identifying Critical Assets (e.g., student data, staff records)
2. Identifying Threats & Vulnerabilities
3. Assessing Risks & Business Impact
4. Developing Risk Mitigation Strategies

Risk Governance is the “control layer” that ensures all these steps are:

- Documented
- Repeated over time
- Supported by leadership

🧭 our Next Process Steps (After Questionnaire Collection)

1 interview

2 Map Data into OCTAVE

3 Create Deliverables

4 Draft a Report

TEAM

SIVARAJA KAJAN

BSc (Hons) in Information Technology
Specialising in Cyber Security-SLIIT

KEZOTHARAN G

BSc (Hons) in Information Technology
Specialising in Cyber Security-SLIIT

NOEL KOWSHIK

BSc (Hons) in Information Technology
Specialising in Cyber Security-SLIIT

FARAN R

BSc (Hons) in Information Technology
Specialising in Cyber Security-SLIIT

INTERVIEW ONLY 18 QUESTION

Q1:General Information

1.1 Who is responsible for IT and security within your organization (name, role)?

1.2 Do you outsource any of your IT services? If yes, to whom?

Q2:Cybersecurity Policies and Governance

2.1 Does your organization have written cybersecurity policies (e.g., acceptable use, data classification)?

2.2 Are staff required to read and acknowledge cybersecurity policies?

2.3 Is there a designated Data Protection Officer or Information Security Officer?

Q3:Network and Device Security

3.1 What operating systems are primarily used on computers and mobile devices?

3.2 Are firewalls or antivirus software deployed on all systems?

3.3 Is Wi-Fi access protected by strong passwords and encryption (e.g., WPA2/WPA3)?

Q4:User Account Management

4.1 How are user accounts created and managed (manually, automated, etc.)?

4.2 Are password policies enforced (e.g., complexity, expiration, reuse prevention)?

4.3 Is access to sensitive information role-based?

Q5: Data Protection

5.1 Where is critical data stored (e.g., student records, staff files)?

5.2 Are encryption techniques used for stored or transmitted data?

5.3 Who has access to cloud storage accounts like Google Drive?

Q6: Backup and Recovery

6.1 How often are backups performed (daily, weekly, etc.)?

6.2 Are backups tested regularly for successful recovery?

6.3 Where are backups stored (external drive, cloud, both)?

Q7: Incident Response

7.1 Have there been any past cybersecurity incidents (e.g., ransomware, phishing)?

7.2 If so, how was it handled and what actions were taken?

7.3 Is there a documented plan or team for responding to future incidents?

Q8: Cybersecurity Awareness and Training

8.1 Do you plan to introduce cybersecurity training for staff in the future?

8.2 What topics would be most useful (e.g., phishing, password hygiene, social engineering)?

8.3 Are you open to students conducting awareness sessions for your staff?

Q9: Physical Security

9.1 Are computers or sensitive areas locked when not in use?

9.2 Are visitor logbooks or CCTV systems used at the premises?

Q10: Expectations and Collaboration

10.1 What areas would you like students to focus on during the cybersecurity assessment?

10.2 Are there any tools or platforms you'd prefer us to use (e.g., Nmap, Burp Suite)?

10.3 Do you expect a final report, live demonstration, or both?

Q11: Risk Management and Assessment

11.1 Have you ever conducted a formal risk assessment related to IT or cybersecurity?

11.2 What do you consider to be your most critical digital assets?

11.3 What would be the impact on your operations if your systems were down for 24 hours?

Q12: Application Security

12.1 Do you use any web applications (e.g., online portals, e-learning platforms)?

12.2 Are these applications developed in-house or by third parties?

12.3 Are security updates applied to them regularly?

Q13: Cloud and Third-Party Services

13.1 Besides Google Drive, do you use any other third-party cloud platforms (e.g., Zoom, Microsoft 365)?

13.2 Do you review the privacy and security terms of third-party services before use?

13.3 Are third-party vendors evaluated for their security practices?

Q14: Mobile and BYOD (Bring Your Own Device)

14.1 Are staff allowed to use personal devices for work purposes?

14.2 Are there any security measures enforced on these devices (e.g., antivirus, encryption)?

14.3 What steps are taken if a staff member’s phone with institutional data is lost?

Q15: Future Planning and Budget

15.1 Is there a budget allocated for cybersecurity tools or improvements?

15.2 Are you interested in receiving a basic cybersecurity roadmap tailored to your organization?

15.3 Would you consider implementing low-cost open-source tools for network and endpoint protection?

Q16: Compliance and Legal Obligations

16.1 Are you aware of the Personal Data Protection Act in Sri Lanka and its implications for your institution?

16.2 Do you maintain consent forms for collecting and storing personal information of students or staff?

Q17: Monitoring and Logging

17.1 Would you be interested in setting up basic system or network logging to monitor unauthorized activity?

17.2 Do you have any experience with tools like Wazuh, Graylog, or similar SIEM platforms?

Q18: Long-term Cybersecurity Strategy

18.1 Are you open to developing a long-term cybersecurity strategy with student support (e.g., policy writing, yearly checkups)?

18.2 Would you like us to help you create simple cybersecurity documentation (e.g., incident report template, asset register)?

18.3 Are you interested in future collaboration for awareness programs, digital safety workshops, or IT-related training?

THANK YOU