## Literature Review Outline

**Student Name:** Mohammed Ali Harahsheh
**Title:** A Critical Review of Cloud Security Risks in the Higher Education Sector
**Word Count Target:** 2,000 words
**Module:** Research Methods and Professional Practice

## 1. Aim of the Review

To critically evaluate key security risks associated with cloud computing in the higher education sector by synthesizing academic and industry literature. The review will identify major threats, examine diverse mitigation perspectives, and propose appropriate sector strategies for improvement.

## 2. Rationale and Context

The adoption of cloud computing in higher education is accelerating, driven by demands for remote access, digital learning, and scalable infrastructure. However, this expansion also brings a heightened risk of cyber threats, particularly in environments that prioritize openness and decentralization. This review addresses the need for sector-specific understanding of cloud vulnerabilities.

## 3. Literature Search Strategy

Searches will be conducted in:

- **Databases**: Essex Library, IEEE Xplore, ScienceDirect, SpringerLink, Google Scholar
- **Organizations**: Cloud Security Alliance (CSA), NIST, ENISA, EDUCAUSE
- **Search terms**: "cloud security", "higher education", "data breach", "insider threats", "misconfiguration", "shared responsibility", "compliance"

Inclusion criteria will focus on:

- Peer-reviewed articles (2013–2025)
- Industry reports (2020–2025)
- Real-world breach case studies since 2022

## 4. Key Risk Categories to Explore

- Misconfiguration of cloud environments
- Insider threats and IAM weaknesses
- Insecure APIs and integration vulnerabilities
- Confusion around shared responsibility models
- Compliance challenges (GDPR, FERPA, NESA)

## 5. Structure of the Review

1. **Introduction** – Overview, significance, and scope
2. **Sector Context** – Why cloud security in education is uniquely challenging
3. **Literature Search Summary** – Databases, keywords, and selection criteria
4. **Main Risk Themes** – Thematic discussion of threats (mapped to NIST framework)
5. **Contrasting Perspectives** – Varied views on mitigation (tools vs. training, public vs. private cloud)
6. **Gaps in the Literature** – Lack of longitudinal and regional studies
7. **Synthesis & Recommendations** – Tailored actions for academic institutions
8. **Conclusion** – Summary and future research directions

## 6. Preliminary References


- CSA. (2022). *Top Threats to Cloud Computing*.
- Hecklau, F., et al. (2016). *Holistic approach for human resource management in Industry 4.0*. Procedia CIRP, 54, 1–6.
- IBM. (2023). *Cost of a Data Breach Report*.
- NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*.
- ENISA. (2023). *Threat Landscape Report – Education Sector*.
- Another resource's