

Week 4: Governance and Strategic Planning for Security

Prem Joshi (2537632)

Manthan Siddhpura (2524128)

Dev Gajera (2538542)

Yashkumar Bhingradiya (2528447)

Naman Vaidya (2540087)

1. Understanding Governance Components (EduFlex LMS)

Security Governance vs. Security Management

- **Security Governance (The School Board / Trust Executives):** Focuses on high-level strategy and legal compliance (e.g., GDPR, Family Educational Rights and Privacy Act (FERPA), or Children's Online Privacy Protection Act (COPPA)). They answer: "Are we keeping our students' data safe and meeting our legal duties?" They set the budget and approve the overall risk tolerance for the LMS.
- **Security Management (The IT Director / LMS Administrator):** Focuses on day-to-day operations. They answer: "Are the LMS firewalls configured correctly? Are student passwords forced to change? Is data backed up?" They implement the practical controls required by the Board's strategy.

Key Governance Processes (ISO/IEC 27014:2013)

Applied to EduFlex, these four core processes look like this:

1. **Evaluate:** Assessing the risks of a school environment—such as students trying to hack the LMS to change grades, teachers falling for phishing emails, or third-party plugins introducing vulnerabilities.
2. **Direct:** Issuing executive orders mandating strict data access rules (e.g., "No student shall access another student's grade records").
3. **Monitor:** Reviewing monthly reports on system uptime, failed login attempts, or the results of student data privacy audits.
4. **Communicate:** Providing regular updates to parents, teachers, and regulators about how EduFlex secures its virtual learning environment.

Role of Policies, Standards, and Guidelines

- **Policies (Mandatory Laws):** The high-level rulebook. Example: "EduFlex is committed to protecting student data privacy and ensuring only authorized users can access the LMS."
- **Standards (Mandatory Technical Rules):** The specific technical setup. Example: "All LMS administrator and teacher accounts must use Multi-Factor Authentication (MFA). Student passwords must be at least 10 characters long."
- **Guidelines (Best Practices / Advice):** Helpful tips for users. Example: "A guide for teachers on how to securely invite guest speakers to a virtual classroom without leaking the class meeting link."

2. Policy Development Exercise

EduFlex LMS Information Security Policy

1. Purpose & Scope

- **Purpose:** This policy aims to protect the integrity, confidentiality, and availability of the EduFlex LMS. It ensures that student grades, personal information, and educational materials are protected from data breaches, unauthorized modifications, and cyber threats.
- **Scope:** This policy applies to all users of the EduFlex LMS, including students, parents/guardians, faculty (teachers), administrative staff, and any third-party IT vendors managing the LMS infrastructure.

2. Roles & Responsibilities

- **School Board / Headteacher:** Authorizes security funding, reviews compliance reports, and holds ultimate legal accountability for data protection.
- **LMS Administrator (IT Department):** Responsible for patching the LMS software, managing user roles, monitoring system access logs, and enforcing technical controls.
- **Teachers / Staff:** Responsible for keeping their login credentials secure, locking devices when unattended, and inputting grades accurately.
- **Students & Parents:** Responsible for using the platform appropriately, following digital citizenship guidelines, and reporting any security bugs or cyberbullying to staff.

3. Standards & Procedures

- **Role-Based Access Control (RBAC):** Users are granted access strictly based on their role. Students can only view their own progress; teachers can edit grades for their specific classes; administrators hold backend system access.
- **Data Encryption:** All student PII and academic records must be encrypted while stored (at rest) and while being accessed over the internet (in transit via HTTPS).
- **Patch & Plugin Management:** The LMS software and all integrated plugins (e.g., video conferencing, quiz tools) must be updated within 14 days of a security patch release to prevent exploitation.

4. Compliance & Enforcement

- Any student found attempting to bypass LMS security controls (e.g., credential harvesting, brute-forcing accounts, altering grades) will face immediate disciplinary action, up to suspension or expulsion.
- Staff members who bypass security protocols (e.g., sharing accounts or exporting student data to unauthorized personal devices) will be subject to HR disciplinary procedures.

5. ISO/IEC 27014 Alignment

This policy aligns with ISO 27014 principles by creating an explicit chain of accountability from the Headteacher down to the student, establishing clear behavioral expectations, and mandating technical monitoring of the platform.

3. Strategic Planning & Security Awareness (SETA)

Schools have a uniquely diverse group of users. A "one-size-fits-all" approach will fail. The EduFlex SETA program divides training by user type:

Core Topics Covered

- **For Staff & Teachers:** Identifying phishing emails targeting staff payroll or student databases; securing virtual classrooms against unauthorized visitors ("room bombing"); securely handling and entering report card data.
- **For Students:** Password hygiene (not sharing passwords with friends); identifying phishing links disguised as free game downloads or homework help; reporting cyberbullying or suspicious messages on the LMS.
- **For Parents:** Creating secure parent-portal passwords; spotting fraudulent emails claiming to be from the school demanding immediate "fee payments."

Delivery Methods

- **Gamified E-Learning (For Students):** Interactive, age-appropriate short games or quizzes built directly into the LMS at the start of the school year covering safe internet use.
- **Bite-Sized Video Training (For Staff):** 5-10 minute video modules delivered during professional development days, focusing on data privacy laws and phishing.
- **Phishing Simulations (For Staff):** Quarterly mock-phishing campaigns testing teachers on typical school-related traps (e.g., a fake email titled "Updated Exam Schedule - Action Required").

Measuring Effectiveness

Metric Type	What We Track	Success Target
Activity Metrics	Percentage of students and staff who complete the mandatory baseline security modules.	100% of staff and 90%+ of students within the first term.
Behavioral Metrics	Teacher click-rates on simulated phishing emails vs. how quickly they report it to IT.	Click rate below 5%; Reporting rate above 60%.
Strategic Metrics	Number of unauthorized account access incidents or compromised student/teacher accounts.	Zero successful account takeovers per academic year.