Importance of security compliance in building any software application

Class 12

12/4/2025

Acknowledgement

The series of the IT & Japanese language course is Supported by AOTS and OEC.

Ministry of Economy, Trade and Industry

Overseas Employment Corporation

What you have Learnt Last Week

We were focused on following points.

- Usage of control and loop flow statement
- Performing Linear Algebra in Numpy
- Inspecting and Understanding Data
- Why Requirement Analysis is so important in the process?
- Review case studies that demonstrate successful requirement analysis practices
- Machine Learning algorithms
- Software development Life cycle
- Gitflow, Waterfall and agile methodologies

What you will Learn Today

We will focus on following points.

- Discuss the types of security and security mindset
- A Comprehensive Guide to General Security Compliance
- Why Need to follow Security Compliance Rule?
- Discuss case study regarding the security compliance
- Quiz
- Q&A Session

What is Security?

Introduction to IT Security and Its Importance in Business

Understand what IT security is and why it plays a critical role in modern business operations and data protection.

Importance in IT & Business

1. Safeguards sensitive information
2. Ensures business continuity
3. Maintains customer trust
4. Meets legal and regulatory requirements

Example Scenario: A bank secures customer data using encryption, firewalls, and user access controls to prevent breaches and fraud.

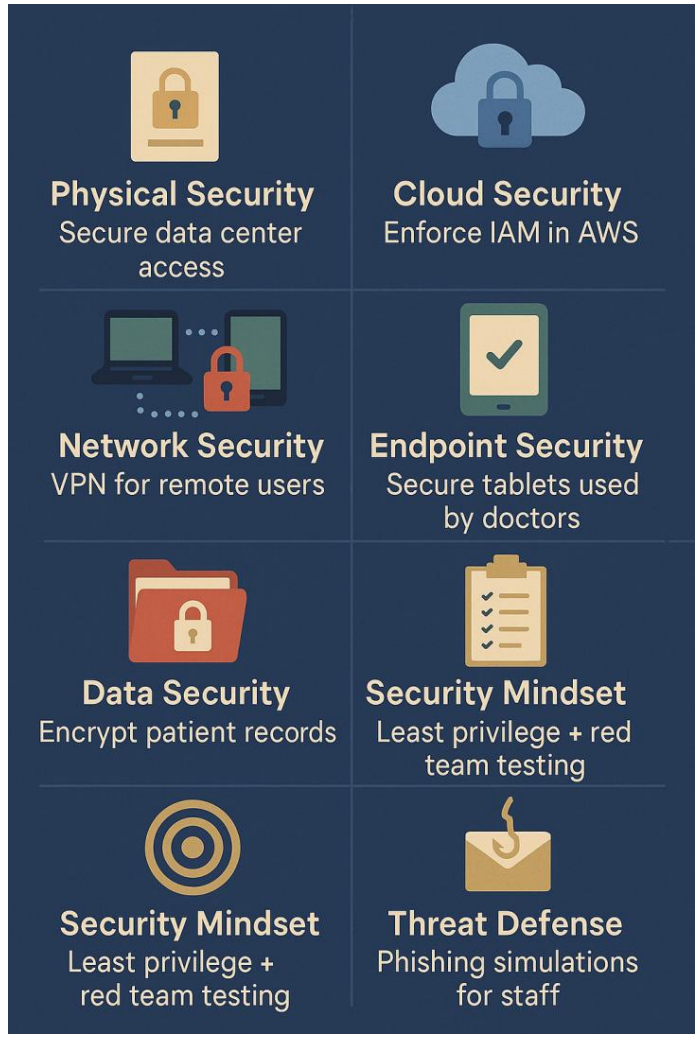
Types Of Security

Exploring the different types of security in the digital World

1. Physical Security:
Restricting physical access to systems and data centers.
Example: Biometric scanners at server rooms.

2. Application Security:
Securing apps from vulnerabilities during and after development.
Example: Input validation to prevent SQL injection.

3. Cloud Security:
Ensuring security of services hosted on cloud platforms.
Example: Role-based access in AWS IAM.



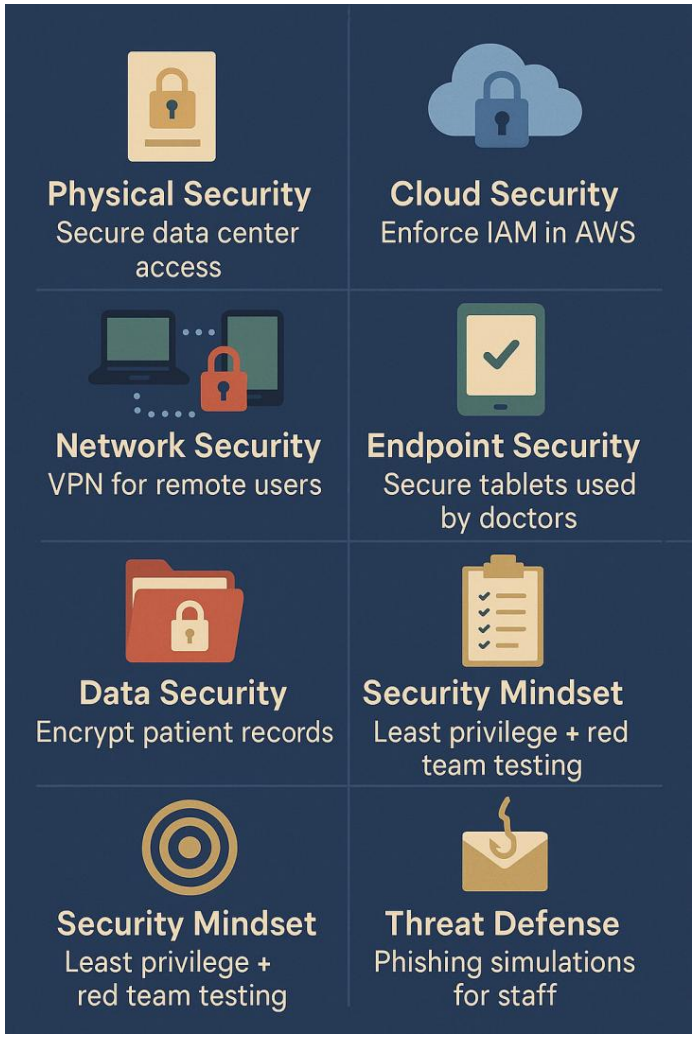
Types Of Security

Exploring the Different Types of Security in the Digital World

4. Network Security:
Protecting data as it travels over networks.
Example: Firewalls, intrusion detection systems (IDS).

5. Data Security:
Protecting stored and transmitted data.
Example: Encrypting files on cloud storage.

6. Operational Security:
Policies and procedures to protect data during operations.
Example: Change management, access logging.



Security Mindset

Building a Security-First Mindset in Organizations

Red Team vs Blue Team:

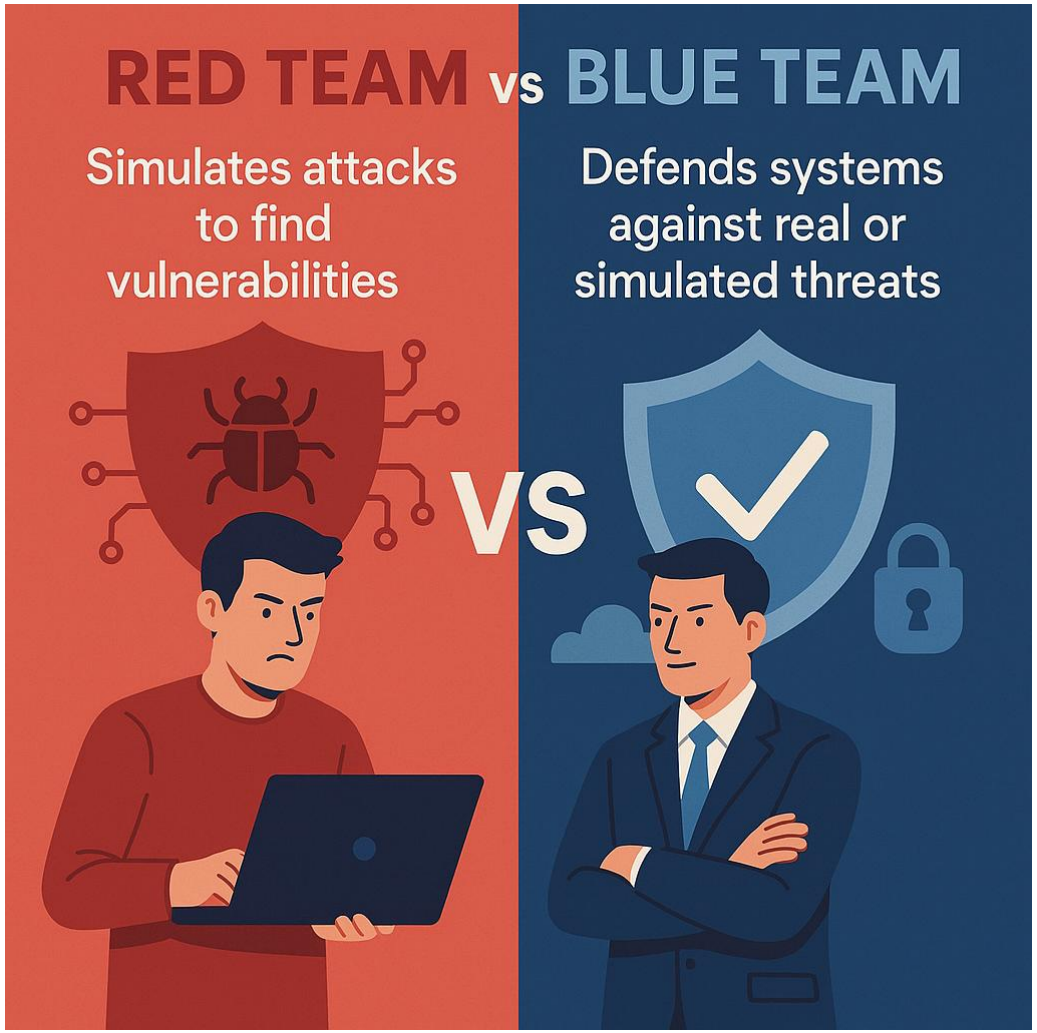
- **Red Team:** Simulates attacks to find vulnerabilities.
- **Blue Team:** Defends systems against real or simulated threats.

Example: Internal penetration testing to improve defenses.

Least Privilege Principle:

Give users the minimum access necessary.

🔑 ***Example:*** A cashier only accesses billing, not HR systems.



Common Threats

Common Threats and Vulnerabilities in Cybersecurity

📌 Social Engineering

- Manipulating people to gain access.

🎭 ***Example:*** Pretending to be IT support to reset a password.

📌 Phishing

- Tricking users via fake emails/sites.

🎭 ***Example:*** A fake login page mimicking a bank portal.

📌 Malware/Ransomware

- Malicious software that damages or locks systems.

🎭 ***Example:*** WannaCry ransomware attacking hospitals or Stuxnet.

📌 Misconfigurations

- Incorrect settings exposing systems.

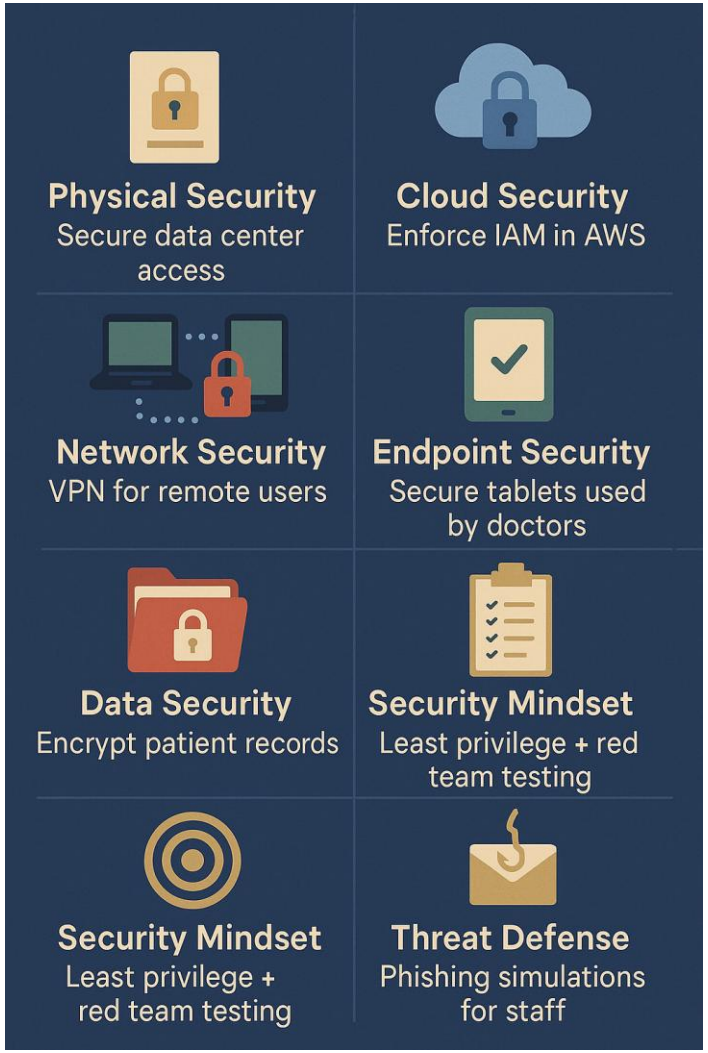
🎭 ***Example:*** Publicly exposed cloud bucket with sensitive data.

Real World Applications

Applying Security Concepts in Real-World Business Scenarios

Scenario: Healthcare App

- **Physical Security:** Secure data center access
- **Network Security:** VPN for remote users
- **App Security:** Secure login, input sanitization
- **Data Security:** Encrypt patient records
- **Cloud Security:** Enforce IAM in AWS
- **Endpoint Security:** Secure tablets used by doctors
- **Operational Security:** Regular audits, logs
- **Security Mindset:** Least privilege + red team testing
- **Threat Defense:** Phishing simulations for staff



Task-1

Secure Health Care Application

Let's learn that how to secure the health care application

https://codepen.io/Mise-Academy/full/pvoMNYW

What is Security Compliance & Why It Matters

Security compliance refers to adherence to standards, regulations, and best practices that ensure data and system security.

Purpose:

- ✅ Protect sensitive information
- ✅ Prevent data breaches
- ✅ Meet legal and industry obligations
- ✅ Build trust with customers and stakeholders.

Examples of Security Compliance in Action:

- A hospital encrypting patient data to follow **HIPAA**
- A tech company using data privacy practices for **GDPR**

Key Compliance Frameworks and Control Categories

Global Standards and Types of Security Controls Every Organization Needs

Popular Frameworks:

- ✅ **ISO/IEC 27001:** International standard for ISMS
- ✅ **ISO 27017:** For cloud security
- ✅ **ISO 27018:** For data security in cloud
- ✅ **NIST:** U.S. cybersecurity guidelines
- ✅ **GDPR:** Data privacy law for EU residents
- ✅ **HIPAA:** Health information protection (U.S.)
- ✅ **PCI DSS:** Secure credit card data handling
- ✅ **SOC 2:** Data security for service providers

Types of Security Controls:

- 🔒 **Administrative:** Policies, training, incident response
- 💻 **Technical:** Firewalls, MFA, encryption
- 🏢 **Physical:** Biometrics, security guards, CCTV

Example:

A startup handling online payments implements **PCI DSS** technical controls like encryption and secure payment gateways.

Achieving and Managing Compliance Effectively

Step-by-Step Compliance Process and Tools for Ongoing Monitoring

Steps to Achieve Compliance:

1. **Risk Assessment** – Identify potential threats
2. **Define Security Policies** – Create enforceable rules
3. **Implement Controls** – Apply appropriate protections
4. **Audits & Reviews** – Check and improve compliance regularly
5. **Documentation & Reporting** – Keep clear records

Compliance Management Tools:

☁️ **Cloud Platforms:** AWS & Azure Compliance Centers
🔍 **Vulnerability Scanners:** Nessus, Qualys
📊 **GRC Tools:** ServiceNow GRC, RSA Archer

Example:

A financial app uses **Qualys** for vulnerability scanning and **AWS Security Hub** for real-time compliance alerts.

Why Security Compliance is Crucial for Every Business

Business Value, Legal Mandates & Operational Importance

Business Reasons:

✅ Protect customer data from unauthorized access
✅ Avoid heavy **financial penalties** from non-compliance
✅ Maintain **brand reputation** and stakeholder trust

Example:

- *Target* suffered a breach in 2013 due to third-party vulnerabilities, costing them **$162 million** and damaging trust.

Example:

- *Google* was fined **€50 million** under GDPR for insufficient transparency in data processing.

Legal and Regulatory Requirements:

📜 Comply with **government mandates**
🏥 Adhere to **industry-specific laws** like HIPAA, GDPR, PCI DSS

In September 2024, MoneyGram discovered an unauthorized third party accessed and acquired personal information of certain customers, leading to the temporary shutdown of all systems

Operational and Strategic Benefits of Being Compliant

How Security Compliance Strengthens Systems and Builds Trust

Operational Benefits:

🛡️ Improves system resilience against attacks
🔍 Helps detect & prevent breaches before they escalate

Example:

🔹 *Microsoft Azure* implements continuous compliance monitoring, enabling early detection of vulnerabilities across cloud infrastructure.

Customer Expectations:

🤝 Clients demand security assurance for partnerships
🗂️ Vendors and partners often request compliance certifications

Example:

🔹 A B2B SaaS company gains **SOC 2 compliance**, helping them close deals with Fortune 500 companies requiring certified vendors.

The Real Cost of Ignoring Security Compliance

Consequences of Violations, Fines, and Business Disruption

Consequences of Non-Compliance:

- Massive **fines** for data leaks (e.g., GDPR fines up to 4% of annual revenue)
- **Legal actions** and lawsuits from affected users
- Risk of **business shutdown**, revoked licenses, or lost partnerships

Example 1:

- *Equifax* faced a **$575 million settlement** after a 2017 data breach exposing 147 million people's data.

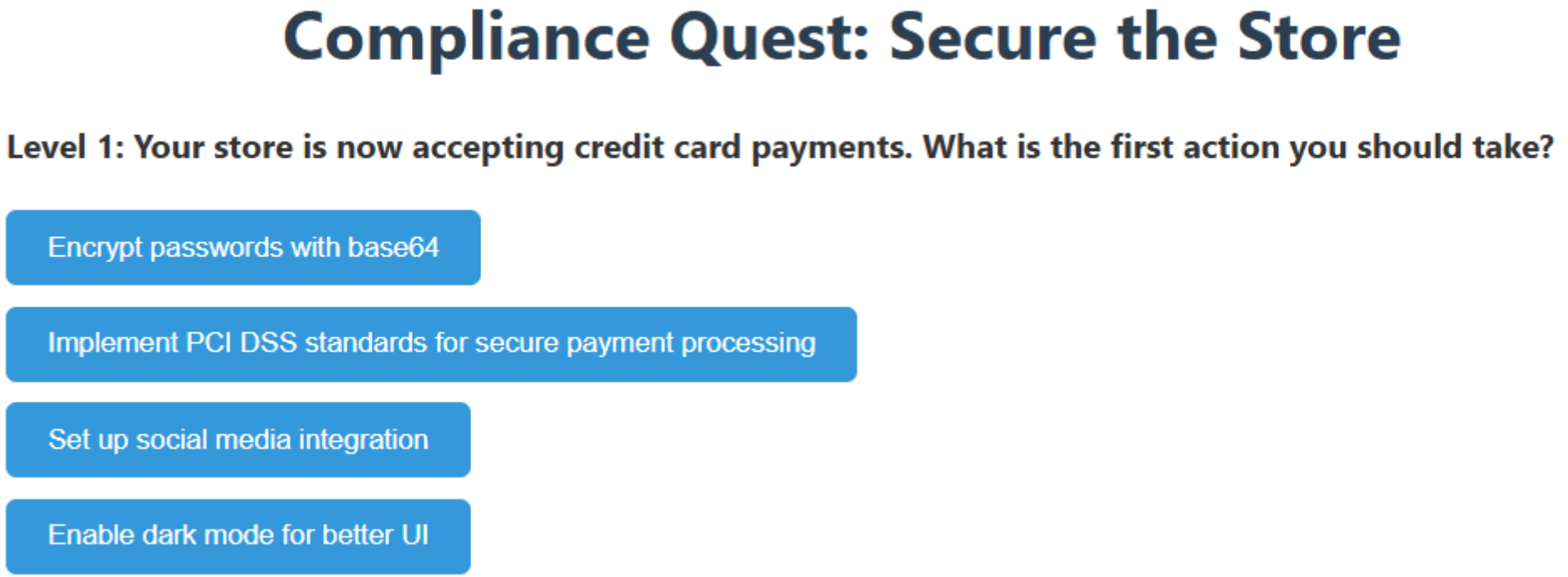
Example 2:

- *British Airways* fined **£20 million** for a 2020 breach where attackers stole customer login and payment data.

Task-2

Compliant the E-commerce application

Let's learn which international frameworks are used for compliance



https://codepen.io/Mise-Academy/full/KwKONjX

Case Studies

Equifax Data Breach: A Case of Missed Patches and Massive Impact

How a Small Compliance Gap Led to a Huge Disaster

Background:

🔍 In 2017, Equifax suffered a breach affecting **147 million users**.

What Went Wrong:

⚠️ Failed to patch a known vulnerability (Apache Struts CVE-2017-5638)

🔐 Lack of effective vulnerability scanning and update processes

Compliance Gaps:

❌ Inadequate patch management

❌ Poor asset inventory tracking

Outcomes:

💸 Fined **$575 million** by FTC, CFPB, and states

📉 Severe reputation damage and executive resignations

Lesson Learned:

✅ Prioritize **timely patching**

✅ Maintain a comprehensive **asset management** strategy

Capital One Data Breach: Cloud Misconfiguration Consequences

Importance of IAM, WAF, and Shared Responsibility in Cloud Security

Background:
🔍 In 2019, Capital One was breached—data of **100 million customers** exposed.

What Went Wrong:
⚠️ AWS S3 misconfiguration allowed a former employee to access data
🔓 Weak IAM policies and insufficient firewall configuration

Compliance Gaps:
❌ Mismanagement of **Identity and Access Management (IAM)**
❌ No real-time alerting or **audit logs**

Outcomes:
💸 Fined **$80 million** by U.S. regulators
👨‍⚖️ Lawsuits filed by customers

Lesson Learned:
✅ Use **Web Application Firewalls (WAFs)**
✅ Follow **Shared Responsibility Model** in cloud
✅ Enable **real-time monitoring and alerts**

HIPAA Violation: When Patient Data Isn't Properly Protected

Healthcare’s Critical Need for Security Compliance

Background:

🔍 A healthcare provider leaked thousands of patient records due to unencrypted devices and lack of audits.

What Went Wrong:

⚠️ No **data encryption** on laptops or servers
🕵️ Lack of **audit trails** to trace access

Compliance Gaps:

❌ Non-compliance with **HIPAA Privacy & Security Rules**
❌ No regular security risk assessment

Outcomes:

💸 Fined **$3 million**
👨‍⚖️ Negative media coverage and lawsuits

Lesson Learned:

✅ Encrypt **all sensitive health data**
✅ Maintain **audit logs and trail activity**
✅ Conduct **regular risk assessments**

Key Takeaways: Learning from Compliance Failures

What These Breaches Teach Us About Security Compliance

✅ **Patch Management**: Delay in patching creates major risks (Equifax)
✅ **Cloud Configuration**: IAM and WAF are non-negotiable in cloud (Capital One)
✅ **Data Protection in Healthcare**: Encryption and logs are vital (HIPAA case)

Cross-Case Insights:

🔁 Regular **audits and monitoring** help detect early signs
🎓 Ongoing **employee training** improves awareness
🛠️ Design systems with **security built-in**, not added later

Real-World Reminder:

Compliance is **not just a checklist**—it's an ongoing culture of security.

Quiz Section

Quiz

Everyone student should click on submit button before time ends otherwise MCQs will not be submitted

[Guidelines of MCQs]

1. There are 20 MCQs
2. Time duration will be 10 minutes
3. This link will be share on 12:25pm (Pakistan time)
4. MCQs will start from 12:30pm (Pakistan time)
5. This is exact time and this will not change
6. Everyone student should click on submit button otherwise MCQs will not be submitted after time will finish
7. Every student should submit Github profile and LinkedIn post link for every class. It include in your performance

Assignment

Assignment should be submit before the next class

[Assignments Requirements]

1. Create a post of today's lecture and post on LinkedIn.
2. Make sure to tag @Plus W @Pak-Japan Centre and instructors LinkedIn profile
3. Upload your code of assignment and lecture on GitHub and share your GitHub profile in respective your region group WhatsApp group
4. If you have any query regarding assignment, please share on your region WhatsApp group.
5. Students who already done assignment, please support other students

Q&A Session

ありがとうございます。
Thank you.
شکریا

For the World with Diverse Individualities