Course 3 Week 1

Complaince Frameworks & Industry Standards

- Security Event → An event on a syste or network detected by a security device or application
- Security Attack → A security event that has been identified by correlation and analytics tools as malicious activity that is attempting to collect, disru deny, degrade or destroy information system resources or the information itself
- Security Incident, ~~An~~ attack or security event that has been reviewed by IBM security analysts and deemed worthy of deeper investigation.

Challenges - 12K attacks in 81+M

Challenges -> [illegible] normal threats

Data

48% Outsiders

31.5% Malicious Insider

23.5% Inadvertent Actor.

2024 Data.

37% Unauthorized access

20% Malicious code

20% sustained probe/scan

11% Suspicious activity

8% Acct or Credentials abuse.

4% Denial of service.

Complaince Basics

Security	Privacy	Complaince.
-> designed protection from theft & Damage, disruption or misdirection	How information is used, who that information is shared with, or if that information is used to track users.	-Tests that security measure are in place -> Which and how many depend on the specific

Physical controls
↳ servers
↳ Data centers

Technical controls
↳ Encryption
↳ what 'log' data is collected

Operational controls.
↳ How a server is configured, operated monitored and patched

Compliance.
- often cover additional non-security requirements such as business practices, vendor agreements and organizational control

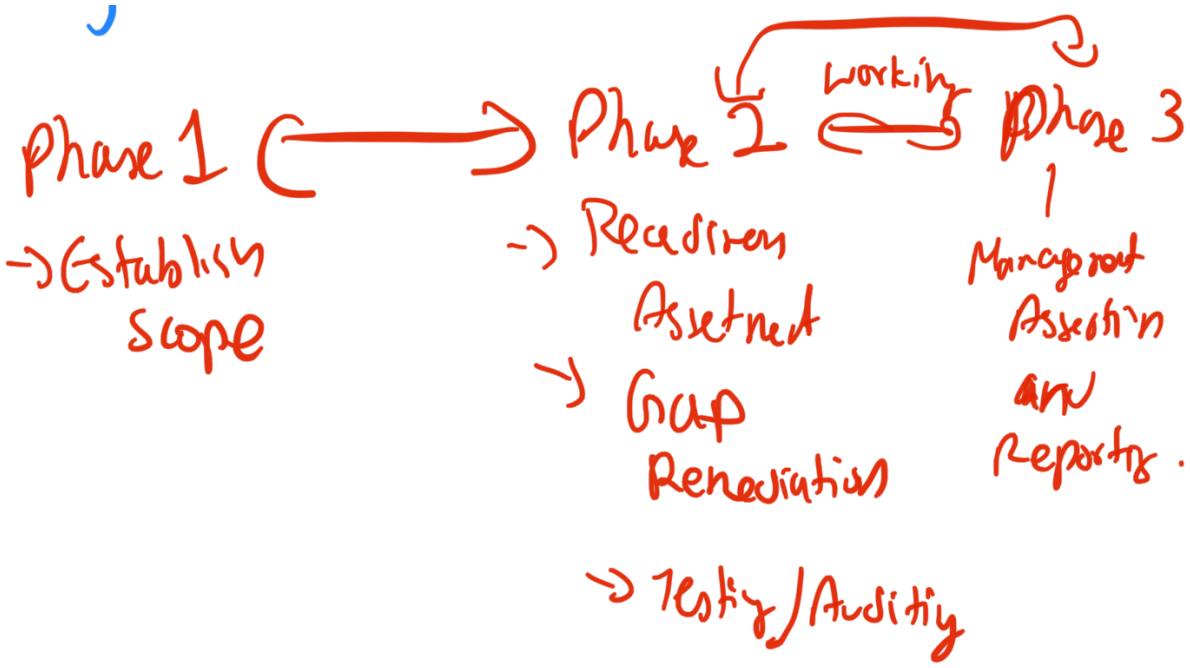
"Security & Compliance are deeply interlinked, but not the same."

Compliance
↳ Controls
↳ Validate
↳ External
↳ Proven

↳ Foundational: SOC, ISO

↳ Industry: HIPPA, PCI, DISS

Any typical compliance process:-



Scoping

→ "controls" are based on the goal/ Compliance - SOC-SOO

→ Ensure all components in scope are compliant to technical control

→ Ensure all processes are compliant to operational controls

Testing and Auditing may be

→ Internal / Self Assessments

→ External Audit.

→ Audit Recertification schedules can

be quarterly, bi-quarterly annually etc

US Cybersecurity Federal Law.

→ Computer Fraud and Abuse Act (CFAA) → 1984.

→ Federal Information Security Act of 2002 FISMA

→ Federal Information Security Modernization Act of 2014 (FISMA 2014).

assign specific responsibilities to federal agencies, NIST, OMB in order to strengthen IT systems.

General Data Protection Regulation (GDPR) Overview.

25 May 2018

↳ Complaince
↳ Data Protection
↳ Personal Data.

5 Key General Data Protection Regulation Obligations.

1.) Rights of EU Data Subjects.
2.) Security of Personal Data
3.) Consent
4.) Accantability of Complaince.
5.) Data Protection by Design and by By Default.

↑ this is the most important one.

Internation Organization for Standards

ISO 27001 → to keep information assets secure.

ISO 27018 - Privacy

ISO 27017 - Cloud Security.

System and Organization Controls Report (SOC) Overview.

SOC1 → Used for financial systems.

SOC2 → addresses a service organization's controls that are relevant to their operations and compliance.

→ Restricted use report contains substantial detail on the system, security practices, testing methodology and results.

SOC3 → Report to provide interested Parties with CPA's opinion

Auditor Process.

What are Auditors looking for...

1.) Accuracy
2.) Completness
3.) Timeliness
4.) Resilience Notice
5.) Consistency.

Industry Standards.

Health Insurance Portability and Accountability Act

Payment Card Data Security (2004) Standard (PCI DSS)

↳ Introduced by American Express.
scanning vendors.

Critical Security Controls.

Centre for Internet CIS. Controls

Basic
Foundational
Organizational