Session 1 of 2: “GRC 101: The What, Why, and Foundations”

20 April 2025

What will we learn

Focus will be:

Lay the groundwork. Help participants understand what GRC is, why it’s important, and introduce the key frameworks (NIST, ISO 27001, SOC 2, PCI-DSS, GDPR, HIPAA).

TITLE

GRC 101: Governance, Risk & Compliance Fundamentals

OBJECTIVES

Understand what GRC is and why it matters. Learn key security compliance frameworks (NIST, ISO 27001, SOC 2, PCI-DSS, GDPR, HIPAA). Explore security questionnaires and knowledge bases. Learn how to identify compliance gaps.

WHY IT'S IMPORTANT

These fundamentals will help you build secure, compliant AI/ML hackathon projects from the ground up.

GRC

Governance, Risk Management, Compliance – an integrated strategy unifying these functions

- GRC = Governance, Risk Management, Compliance – an integrated strategy unifying these functions
- Governance: The policies, processes, and oversight that guide organizational decisions and behavior. (Ensures you “reliably achieve objectives”)
- Risk Management: Identifying and addressing uncertainties and threats to the organization. (Focuses on “addressing uncertainty”)
- Compliance: Adhering to laws, regulations, standards, and ethical practices. (About “acting with integrity” by following requirements)
- Unified Approach: Instead of siloed efforts, GRC aligns these areas to avoid gaps and conflicts

Why GRC Matters

Focus Area

Better Risk Visibility

GRC gives a unified view of risks across the organization, so even small risks aren’t overlooked (Helps prevent minor issues from snowballing.)

Operational Efficiency

Coordinating governance, risk, and compliance efforts avoids duplicate work and inconsistent processes, improving efficiency

Informed Decision-Making

A strong GRC program provides high-quality information on risks and goals, enabling data-driven decisions

Continuous Compliance

GRC helps ensure ongoing adherence to standards/regulations, avoiding costly fines or breaches

Key Security Frameworks (Standards)

NIST Cybersecurity Framework

U.S. guidelines for managing cyber risks. Flexible, outcome-focused approach with five core functions:

Identify, Protect, Detect, Respond, Recover

ISO/IEC 27001

International standard for Information Security Management Systems (ISMS). Provides a framework for establishing and continually improving security controls Organizations can get ISO 27001 certified via external audit

SOC 2 (System and Organization Controls 2)

Security compliance report (not a law, but an industry standard audit) for service organizations. Focuses on protecting customer data via 5 Trust Service Criteria: security, availability, processing integrity, confidentiality, privacy. Often required by enterprises before they trust a vendor

Key Regulations & Standards

GDPR (EU General Data Protection Regulation)

European privacy law governing personal data. Gives EU individuals control over their data and requires organizations worldwide to protect that data properly Strict requirements (consent, data rights, breach notification, etc.) with heavy fines for non-compliance (up to 4% of global revenue)

HIPAA (US Health Insurance Portability & Accountability Act)

United States law protecting sensitive health information (PHI). Applies to healthcare providers and their business associates. Requires administrative, physical, and technical safeguards for health data. Violations can result in substantial fines.

PCI DSS (Payment Card Industry Data Security Standard)

Industry standard (not a government law) for any entity that handles credit card data. Mandates strict security controls to protect cardholder data (network security, encryption, access control, monitoring, etc.). Enforced by banks/card networks; non-compliance can mean fines or losing the ability to process cards

Security Questionnaires & Q&A Libraries

SECURITY QUESTIONNAIRES

These are lengthy sets of questions that companies send to vendors or partners to assess their security and compliance posture Common in B2B sales/procurement (e.g., a client verifying a startup's security). They can cover hundreds of detailed questions on topics like access control, incident response, encryption, etc

Purpose: To determine if a third-party can be trusted with sensitive data It's a due diligence tool. For the receiving company, answering accurately is crucial (false answers can lead to liability if a breach occurs)

Q&A KNOWLEDGE BASE:

To streamline responding, organizations create a centralized repository of previous questionnaire answers and supporting info This security knowledge library allows quick lookup of answers, ensuring consistency and saving time on future questionnaires. It must be kept up-to-date as policies and systems change.

Example: A SaaS company might maintain a library of answers about their encryption, network security, certifications, etc., so when a new client questionnaire arrives, they can pull from it instead of writing from scratch each time.

Identifying Compliance Gaps

Compliance Gap Analysis

A systematic process of comparing your organization’s current policies and controls against required standards or best practices. Essentially, find the “gaps” – where you are not meeting a specific requirement or where a control is missing.

How to Perform:

Gather requirements from a framework/regulation (e.g., a checklist of controls from ISO 27001 or NIST). Gather information on your current implementation (policies, security measures, answers to questionnaire). Compare line by line to identify discrepancies. Document each gap.

Importance:

This is often the first step in improving compliance. It lets you know what to fix. Regular gap analyses help manage risks proactively and avoid surprises in external audits. It’s cheaper to find and address a gap internally than to suffer a breach or fine later.

Outcome

A list of compliance gaps with severity/priorities. For each gap, a recommended remediation (e.g., “Enable multi-factor authentication to meet requirement XYZ”). This feeds into your risk remediation or project backlog.

Activity

Match the Framework

Instructions: We will look at a few hypothetical project scenarios and decide which compliance frameworks or regulations are most relevant to each. This will test our understanding of the frameworks we discussed

Scenario A: A startup provides a cloud SaaS service for enterprise clients worldwide. They manage customer data and need to prove their security to large companies. Which frameworks/standards should they prioritize

Scenario B: A new healthcare AI app diagnoses medical images and is used by clinics in the US. It handles patient records and personal health data. What compliance regulations apply?

Scenario C: An e-commerce platform for global users that stores customer info and processes credit card payments. What standards or laws must it comply with?

Activity

What to do?

- Take 5 minutes in small groups (or the chat) to discuss each scenario. Identify 1-2 key frameworks or regulations for each.
- After 5 minutes, we'll reconvene. I'll ask for volunteers or use the chat responses to share your answers for A, B, and C. Then we'll spend ~5 minutes reviewing as a group why those frameworks are the right fit.

Key Take Aways

- GRC is essential, not optional, in tech and AI/ML projects.
- It brings risk visibility, compliance, and operational maturity.
- Understanding frameworks helps you think like a security analyst.

Thank You

Any Further Questions?