

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

22 April 2025

# Recap from Last Session

- 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.
- 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.

# Security Questionnaires 101

/02

## What are they?

A list of questions from a client or partner assessing your security controls and practices

## Why they matter

Used in vendor risk management to ensure suppliers meet security requirements and industry frameworks

## Common characteristics

Can be lengthy and detailed, covering policies, technical safeguards, certifications, etc.

## Business impact

Necessary for sales/partnerships – completing them builds trust and is often required to close deals

# Handling Security Questionnaires

/03

## SECURITY QUESTIONNAIRES

**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:

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.

## CENTRAL INTAKE

Have a clear process for receiving and tracking questionnaire requests (e.g., via a helpdesk or portal)

## TRUST PACKAGE

Prepare standard docs (e.g. policies, SOC 2 report, certifications) to share proactively

# Compliance Gap Analysis – What & Why

/04

## What are they?

Comparing the current state of security controls against a chosen standard or set of requirements

## Why they matter

Identify gaps – areas where required controls or processes are missing or inadequate

## Use Case

Commonly done when pursuing a certification (ISO 27001, SOC 2, etc.) or meeting new regulations

## Business impact

Provides a roadmap for improvements and estimates effort/cost to reach compliance (what to fix, how long it might take)

# Identifying Compliance Gaps

/05

## 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.

# Think Like a Security Analyst – Beyond Checkboxes

/06

## Understand the “Why”

Know the rationale behind each control or requirement (what risk it addresses, what threat it mitigates)

## Critical Eye:

Don't just verify paperwork – evaluate if the control actually works and is effective against real-world threats

## Ask Questions

Challenge assumptions – “Is this control sufficient? What could go wrong? Are we covering the most likely attack paths?”

## Bridge Compliance & Security

Use compliance activities (audits, reviews) as opportunities to improve security posture, not just satisfy paperwork

- **New Risks:** AI/ML introduce risks like algorithmic bias, lack of transparency, and unpredictable behavior that traditional controls may not cover
- **AI Governance:** Ensure fairness, transparency, accountability in AI outcomes (e.g., bias testing, explainability of models)
- **Frameworks Evolving:** Emerging guidelines (NIST AI Risk Management Framework, draft AI regulations) – GRC must adapt existing processes to include AI-specific checks
- **Critical Thinking Required:** Many AI/ML compliance areas lack clear standards – apply core principles (data privacy, security, ethics) creatively to govern these systems

# Interactive Activity – AI System /08

## Gap Analysis

**Scenario:** You are the GRC analyst for a startup offering an AI-powered loan approval system. The AI model is highly accurate but has never been checked for bias against any demographic group. There is no documentation explaining how the AI makes decisions.

**Requirement:** A new AI ethics guideline in your industry requires “models impacting customers must be tested for fairness and have explainability measures in place.”

**Task:** Identify the gaps between the startup’s current state and the guideline. What would you recommend to comply and ensure the AI system is both fair and transparent?

# Recap & Key Takeaways

- 1. What is GRC?:** Governance, Risk Management, Compliance – an integrated strategy unifying these functions
- 2. GRC in Action:** GRC teams align security efforts with business goals and compliance needs, working across the organization to manage risk and policies.
- 3. Tools & Techniques:** Uses of frameworks (ISO, NIST), maintain answer libraries for questionnaires and gap analyses.
- 4. Critical Mindset:** Don't just check boxes – evaluate the effectiveness of controls and think about real risks (ask “Does this truly protect us? What are we missing?”).
- 5. Emerging Challenges:** Be prepared to apply GRC principles to new areas like AI/ML, adapting for fairness, transparency, and ethics even before formal rules solidify.

# Thank You

/10

In conclusion, GRC in practice is both an art and a science – it uses systematic approaches and tools (the science) and also requires insight, communication, and ethical judgment (the art). With the knowledge and perspectives we've shared, you should be better equipped to operate like a savvy GRC analyst who follows the rules and truly “thinks like a security analyst” to protect and strengthen your organization.

Thank you for participating, and I encourage you to take these lessons into the hackathon and beyond.

Good luck, and stay curious!