OWASP

RANCHI

Join the WhatsApp Group!

GRC 101 – Governance, Risk & Compliance

OWASP
RANCHI

Presented by: Harsh Priye (GRC Specialist at Cisco)

Contents

01. Understanding GRC

Understanding what is GRC and why GRC is important.

02. What is audit and categories of audit

Understanding what is audit and types of audit.

03. Frameworks in security / GRC

Learning different GRC frameworks.

04. Career in GRC and Security

Discussion on the career path for students in GRC / Security.

What is GRC?

- **Governance:** The framework for setting direction/expectations, policies, and internal controls and decision-making.
- **Risk Management:** Identifying, assessing, and mitigating risks to business objectives.
- **Compliance:** Adhering to laws, regulations, and industry standards/ frameworks.

“GRC is now a business imperative shaping boardroom strategy”

Why GRC Matters?

- Reduces risks related to security breaches, fraud, and regulatory violations.
- Enhances corporate reputation and trust among stakeholders.
- Helps in achieving regulatory compliance with standards like ISO 27001, NIST, GDPR, SOX etc.
- It is a strategic approach to aligning business objectives with IT and regulatory compliance.
- Helps organizations establish policies, procedures, and controls to manage risks and meet legal requirements.

Categories of Audit

- **First Party Audits (Internal)** - First Party, or Internal Audits is an audit conducted by organization on itself to determine whether their systems and procedures are consistently improving their ability to provide information security for itself and interested parties.
- **Second Party Audits (Supplier)**- Second Party Audits are commonly known as Supplier Audits is carried out on a current supplier by a purchasing organization; audit results may then be used as part of the purchasing equation.

  Today there is a tendency for organizations to outsource more and more of their data processing activities.
- **Third Party Audits (Certification)**- Third Party Audits involve an independent outside body coming in to the organization to conduct an audit.

Fundamentals of IT Audit

- IT Audit is a process of evaluating an organization's IT infrastructure, applications, and policies.
- Ensures integrity of financial reporting.
- Ensures compliance with regulatory frameworks and business objectives.

➢ **Objectives of IT Audit:**

- ✓ Identify security/ regulatory violations
- ✓ Assess data integrity
- ✓ Ensure IT governance effectiveness
- ✓ Improve operational efficiency

➢ **Phases of an IT Audit:**

- ✓ Planning Phase
- ✓ Testing Phase
- ✓ Reporting Phase

Key Frameworks: ISO, SOC 2, NIST, SOX

- ISO 27001 – Global standard for Information Security Management
- SOC 2 – Assurance report for security, availability, integrity, confidentiality, privacy
- NIST CSF – Framework for identifying, protecting, detecting, responding & recovering
- SOX IT Audit ensures that the technology and security controls protecting financial systems are reliable, accurate, and tamper-proof

ISO 27001 Overview

- ISMS Focus: ISO 27001 defines how organizations build an Information Security Management System.
- Annex A Controls: 93 controls covering people, process, technology (e.g., access control, logging, physical security).
- Internal & External Audits: Annual cycle ensures evidence, documentation, and continuous improvement.
- Risk-based Approach: Organizations must identify risks and apply controls based on severity, impact.
- Universally Applicable: Works for start-ups, enterprises, banks, SaaS companies across industries.

SOC 2 Overview

- Service Organization: The company being audited (e.g., SaaS provider).
- User Entity: Customers who rely on the service organization’s controls for their workflows.
- Trust Service Criteria: Security, Availability, Confidentiality, Processing Integrity, Privacy.
- Type I: Evaluates design of controls at a point in time.
- Type II: Tests operating effectiveness over 3–12 months.
- Auditor-Issued Report: Shared with customers to prove security maturity.

NIST CSF – Industry Best Practices

- Recognized globally as a cybersecurity best-practices roadmap.
- Identify: Understand assets, risks, business environment.
- Protect: Apply safeguards like access control, training, and encryption.
- Detect: Enable logging, monitoring, threat detection capabilities.
- Respond: Incident response planning, communication, mitigation.
- Recover: Restore systems, improve resilience, lessons learned.

Sarbanes–Oxley (SOX) Act – Fundamentals

- ➢ Ensures integrity, accuracy, and reliability of financial reporting by validating IT controls that support financial systems (SAP, Oracle, ERPs, databases).
- ➢ SOX requires companies to prove that financial data cannot be manipulated or altered due to weak IT controls.

- ➢ Focuses on IT General Controls (ITGCs) affecting financial statements:

- **Access Management:** Only authorized users can access financial systems; timely removal of leavers.
- **Change Management:** All financial-system changes are tested, approved, and documented.
- **IT Operations:** Backup, recovery, batch jobs, incident management, logging.

How Students Can Start

> Learn basics: ISO 27001, SOC 2, NIST, GDPR
> Take beginner courses: Udemy, Coursera, Google Cybersecurity, Hackerade
> Internships in IT audit / compliance
> Get certifications: ISO 27001 LA/LI, CISA/ CISM (later)
> Join communities like OWASP, ISACA

Thank You!

- Connect with OWASP Ranchi
- Let's build a strong cybersecurity community! 🚀