

■■ 100-Day GRC Study Challenge

This 100-day challenge will guide you through the foundations of Governance, Risk, and Compliance (GRC), building step by step toward advanced concepts, frameworks, and hands-on projects. Mark off each day as you progress!

Phase 1: Foundations (Days 1–20)

Day 1–2: What is GRC? Role of Governance, Risk, and Compliance

Day 3–4: IT Governance (COBIT, ITIL basics)

Day 5–6: Understanding Risk Management (ISO 31000, NIST RMF)

Day 7–8: Compliance basics (laws, regulations, internal controls)

Day 9–10: Security Governance & Policies

Day 11–12: Introduction to Internal Audit and Assurance

Day 13–14: Business Continuity & Disaster Recovery basics

Day 15–16: Ethics & Corporate Governance

Day 17–18: GRC Tools overview (RSA Archer, ServiceNow, MetricStream)

Day 19–20: Case study: Why organizations need GRC

Phase 2: Risk Management (Days 21–40)

Day 21–22: Types of Risks (Operational, IT, Strategic, Compliance)

Day 23–24: Risk Assessment methodologies

Day 25–26: Qualitative vs Quantitative risk analysis

Day 27–28: Threat Modeling (STRIDE, DREAD, OCTAVE)

Day 29–30: Risk Treatment (Accept, Avoid, Transfer, Mitigate)

Day 31–32: Control Frameworks (COSO, COBIT)

Day 33–34: Key Risk Indicators (KRIs)

Day 35–36: Third-party/vendor risk management

Day 37–38: Scenario-based risk assessments

Day 39–40: Mini-project: Perform a risk assessment for a small IT system

Phase 3: Compliance & Frameworks (Days 41–70)

Day 41–42: ISO 27001/27002 (ISMS)

Day 43–44: NIST CSF

Day 45–46: GDPR basics (data privacy)

Day 47–48: HIPAA (healthcare compliance)

Day 49–50: PCI DSS (payment security)

Day 51–52: SOX & Financial Compliance

Day 53–54: FISMA & FedRAMP

Day 55–56: Data protection laws (India DPDP Act, CCPA)

Day 57–58: Industry-specific compliance (Energy, Banking)

Day 59–60: GRC in Cloud environments (AWS, Azure)

Day 61–62: Audit process & evidence collection

Day 63–64: Control testing & monitoring

Day 65–66: Mapping regulations to controls

Day 67–68: Writing compliance reports

Day 69–70: Case study: GDPR vs CCPA

Phase 4: Governance & Strategy (Days 71–85)

Day 71–72: Building GRC frameworks for organizations

Day 73–74: GRC maturity models

Day 75–76: Risk appetite & tolerance

Day 77–78: Enterprise Risk Management (ERM)

Day 79–80: Key Governance documents (policies, charters)

Day 81–82: GRC dashboards & reporting to executives

Day 83–84: Aligning GRC with business goals

Day 85: Mini-project: Draft a GRC strategy for a startup

Phase 5: Advanced Practice & Tools (Days 86–100)

Day 86–87: Hands-on with GRC platforms (open-source or trial tools)

Day 88–89: Automating compliance with cloud services

Day 90–91: Incident & Breach Response process

Day 92–93: Metrics & KPIs for GRC performance

Day 94–95: GRC in DevSecOps

Day 96–97: Emerging risks: AI, IoT, Cybersecurity

Day 98–99: Mock GRC audit (self-assessment)

Day 100: Final project: Create a full GRC roadmap for an organization

■ **Congratulations! Completing this 100-day challenge will give you a strong foundation in Governance, Risk, and Compliance (GRC).**