GRC STARTER KIT:

Governance, Risk

Management & Compliance

Practical Resources to Build and Strengthen Your GRC Program

1. GRC Fundamentals

Before diving into checklists and templates, it helps to ground the kit in a shared understanding of what GRC actually means. GRC stands for Governance, Risk Management, and Compliance — three disciplines that are often run separately in an organization but work best when they are connected and speak the same language.

What Is GRC?

GRC is an integrated approach to managing an organization's overall governance, enterprise risk management, and compliance with regulations. Rather than treating governance, risk, and compliance as three unrelated departments filling out separate spreadsheets, a mature GRC program links them so that decisions about strategy, risk appetite, and regulatory obligations reinforce one another instead of working at cross purposes.

> ***Example:*** *A bank's compliance team tracks a new data-privacy regulation, its risk team scores the exposure of non-compliance as "high impact, medium likelihood," and its governance committee approves budget for a remediation project — all using the same risk register and the same set of definitions, instead of three disconnected trackers.*

The Three Pillars of GRC

- **Governance:** the structures, policies, and decision rights that direct and control the organization — board oversight, corporate policy, delegation of authority, and the tone set from the top.
- **Risk Management:** the discipline of identifying, assessing, treating, and monitoring the events that could prevent the organization from achieving its objectives.
- **Compliance:** the processes that ensure the organization meets its legal, regulatory, contractual, and internal policy obligations, and can demonstrate that it does so.

How GRC Supports Business Objectives

GRC is not a compliance-only exercise bolted onto "real" business activity — it exists to protect and enable the organization's objectives. A well-run program gives leadership the confidence to pursue growth, enter new markets, or adopt new technology because risks are understood and controlled rather than hidden or ignored.

> ***Example:*** *A healthcare provider wants to launch a new patient portal. Its GRC program identifies the relevant privacy regulations early, builds the required controls into the design phase, and lets the launch proceed on schedule instead of being delayed by a late-stage compliance review.*

GRC Program Objectives Checklist

Use this quick checklist to confirm your program's objectives are clearly defined before you go further:

☐ Business objectives the GRC program exists to support are documented

☐ Risk appetite and tolerance levels are defined and approved by leadership

☐ Applicable laws, regulations, and standards are identified

☐ Roles and decision rights for governance, risk, and compliance are clear

☐ Success metrics for the GRC program are agreed and tracked

2. GRC Framework Selection Checklist

Most organizations don't need to invent a GRC approach from scratch — established frameworks like NIST CSF, ISO/IEC 27001, COBIT, and COSO already provide proven structures. The challenge is choosing the framework (or combination of frameworks) that fits your industry, size, regulatory footprint, and maturity level. This checklist walks through the groundwork needed to make that decision with confidence.

☐ Business objectives identified

☐ Key risks identified

☐ Applicable regulations reviewed

☐ Existing controls assessed

☐ Framework requirements mapped

☐ Gaps identified

☐ Ownership assigned

☐ Automation requirements defined

Work through the items in order. Each one builds on the last: you cannot meaningfully map framework requirements until you know your regulatory obligations, and you cannot identify gaps until you know what controls already exist.

> ***Example:*** *A mid-size SaaS company reviews this checklist and realizes it has never formally assessed its existing controls. Rather than jumping straight to a framework, it spends two weeks documenting current controls first — which makes the later gap analysis far more accurate.*

3. GRC Risk Assessment Worksheet

A risk assessment worksheet turns abstract risk conversations into a structured, comparable record. Use one row per identified risk, and revisit the worksheet on a regular cadence — quarterly at minimum, or whenever a significant change occurs (a new system, a new regulation, a new market).

Risk	Likelihood	Impact	Risk Level	Existing Controls	Treatment	Owner

Unpatched servers exposed to internet	Medium	High	High	Quarterly patch cycle	Accelerate patch cadence	IT Security
Vendor lacks SOC 2 report	High	Medium	Medium	Annual vendor review	Request report; add contract clause	Procurement

Guidance for completing each column:

- Risk identification — describe the event or condition that could affect objectives, stated specifically enough to be actionable (not just "cybersecurity risk," but "unpatched external-facing servers").
- Risk evaluation — score likelihood and impact using a consistent scale (e.g., Low / Medium / High) so risks across the organization can be compared fairly.
- Risk prioritization — combine likelihood and impact into an overall risk level to decide what gets attention first.
- Risk treatment — choose to accept, mitigate, transfer, or avoid the risk, and state the specific action being taken.

- Risk ownership — assign a single named owner accountable for the treatment action; a risk with no owner rarely gets addressed.

4. GRC Controls Mapping Template

Controls mapping connects the dots between what your organization is required to do (regulations, standards, contracts) and what it is actually doing (controls) — with evidence to prove it. This is the template auditors and regulators will effectively be reading whether or not you hand it to them directly, because it is the backbone of every audit response.

Business Objective	Risk	Requirement/Regulation	Control	Control Owner	Evidence Required	Testing Frequency	Status
Protect customer data	Data breach	GDPR Art. 32	Encryption at rest & in transit	IT Security	Encryption config export	Quarterly	Effective
Maintain financial	Unauthorized	SOX 404	Segregation of	Finance Ops	Access review log	Monthly	Gap identified

integrity	journal entries		duties in ERP				

When a control shows a gap, capture it and the remediation plan alongside the mapping so the two are never separated:

- Identified Gap — state precisely what is missing (e.g., "segregation of duties not enforced for journal entry approval").
- Remediation Action — the specific fix, with an owner and target date.

Example: *The Finance Ops example above shows a gap in segregation of duties. The remediation action might read: "Restrict journal-entry approval role to a second approver in the ERP by end of Q3 — Owner: Controller."*

5. GRC Implementation Roadmap

Building or maturing a GRC program is easier to manage as a sequence of concrete stages rather than one large, undifferentiated project. The seven steps below turn the roadmap into a working checklist your team can move through step by step.

Step 1 — Define Business Objectives

Start with what the organization is trying to achieve, not with a list of regulations. Every subsequent step should trace back to protecting one of these objectives.

Step 2 — Identify Requirements

Catalog the laws, regulations, industry standards, and contractual obligations that apply to your organization, and note which business units or systems each one touches.

Step 3 — Assess Current Risks

Use the Risk Assessment Worksheet from Section 3 to build (or refresh) the risk register, scoring each risk for likelihood and impact.

Step 4 — Define Controls

For each significant risk and requirement, define the control that addresses it, using the Controls Mapping Template from Section 4.

Step 5 — Assign Roles & Responsibilities

Name an accountable owner for every control, risk, and requirement — use the Roles & Responsibilities Matrix in Section 6 as a starting point.

Step 6 — Implement GRC Technology

Select and configure tooling to support the program at scale — see the Technology Checklist in Section 7 for the capabilities worth evaluating.

Step 7 — Monitor and Improve

Treat GRC as a continuous cycle rather than a one-time project. Revisit the Continuous Monitoring Checklist in Section 9 on a recurring basis.

Example: *A logistics company works through Steps 1–4 over one quarter to build its first formal risk register and control map, then spends the following quarter on Steps 5–7 to operationalize ownership, select a GRC platform, and set a monthly monitoring cadence.*

6. GRC Roles & Responsibilities Matrix

Clear ownership is what separates a GRC program that actually runs from one that exists only on paper. Use this matrix as a starting point and adapt titles to match your organization's structure.

Role	Key Responsibilities	Accountability
Board & Executives	Set direction, define risk appetite, provide oversight	Strategic
GRC Manager	Coordinate the program and report to leadership	Program
GRC Analyst	Perform assessments, maintain controls, support audits	Operational
Risk Manager	Identify and treat risks across the organization	Risk

Compliance Team	Track regulatory requirements and run assessments	Compliance
Internal Audit	Independently evaluate the effectiveness of controls	Assurance
IT/Security Teams	Implement and maintain technical controls	Technical

A practical tip: for every control in your mapping template, name exactly one person from this matrix as the control owner. Shared ownership across a whole team tends to mean no one is truly accountable when an audit finding comes in.

7. GRC Technology Checklist

Spreadsheets can support a GRC program in its earliest stages, but most organizations eventually outgrow them. Use this checklist to evaluate whether a dedicated GRC platform — and which capabilities within it — would meaningfully reduce manual effort and risk of error.

☐ Risk register

☐ Policy management

☐ Compliance tracking

☐ Control management

☐ Audit management

☐ Third-party risk management

☐ Evidence collection

☐ Issue/remediation tracking

☐ Regulatory monitoring

☐ Dashboards & reporting

Example: *A company preparing for its first SOC 2 audit prioritizes evidence collection and control management first, since manually chasing screenshots from a dozen system owners was the single biggest time drain in a self-run pilot audit.*

8. GRC Audit Readiness Checklist

Audit readiness is not something to build in the two weeks before an auditor arrives — it is the natural output of a GRC program that is already running well. Use this checklist as a pre-audit gut check, and treat any unchecked item as an action item with an owner and a date.

☐ Policies documented

☐ Controls mapped

☐ Control owners assigned

☐ Evidence centralized

☐ Risk assessments updated

☐ Compliance requirements reviewed

☐ Open issues tracked

☐ Remediation activities documented

☐ Audit responsibilities assigned

9. GRC Continuous Monitoring Checklist

GRC is not a project with an end date — regulations change, new threats emerge, vendors come and go, and controls that were effective last year can quietly become ineffective. Build a recurring review (monthly or quarterly, depending on your risk profile) around the items below.

- Regulatory changes — new or amended laws and standards that apply to the organization
- Technology changes — new systems, migrations, or decommissioned tools that affect the control environment
- Emerging threats — new attack techniques or fraud patterns relevant to your industry
- Vendor/third-party changes — new vendors, ownership changes, or lapsed certifications

- Control effectiveness — whether existing controls are still operating as designed
- Risk levels — whether likelihood or impact scores have shifted since the last review
- Compliance gaps — new gaps surfaced through testing or self-assessment
- Remediation progress — status of open remediation actions against their target dates

Treating GRC as a continuous cycle, rather than a one-time exercise, is what keeps the program credible with both leadership and auditors over time.

10. GRC Program Self-Assessment

Score your program honestly against each dimension below using a 1–5 maturity scale. This is most valuable when repeated annually — the trend line matters more than any single score.

Maturity scale: *1 = Initial 2 = Developing 3 = Defined 4 = Managed 5 = Optimized*

Dimension	Score (1-5)			
Governance				
Risk Management				

Compliance				
Controls				
Technology				
Ownership				
Monitoring				
Reporting				
Audit Readiness				

Note: the four blank columns to the right of each score are intentional — they give you room to circle or write in a number by hand, or to track the same dimension across four review cycles side by side.

> ***Example:*** *An organization scores "Governance" a 4 (Managed) but "Monitoring" only a 2 (Developing). That gap is itself useful data: it suggests the program is well-directed from the top but not yet consistently tracked day to day — a natural next investment.*

11. 30-60-90 Day GRC Action Plan

Whether you are starting a GRC program from scratch or picking up ownership of an existing one, a 30-60-90 day plan gives you a manageable pace: understand and stabilize first, then build, then operationalize.

First 30 Days — Understand

☐ Define objectives

☐ Identify stakeholders

☐ Document requirements

☐ Establish baseline risks

Days 31–60 — Build

☐ Map controls

☐ Assign ownership

☐ Identify gaps

☐ Prioritize remediation

Days 61–90 — Operationalize

☐ Implement improvements

☐ Centralize evidence

☐ Establish monitoring

☐ Create management reporting

12. Quick Reference: GRC Frameworks

A short, at-a-glance comparison of five commonly used frameworks. This is intentionally brief — use it to decide which framework(s) merit a closer look, not as a substitute for reading the source material.

Framework	Primary Focus	Best Fit For
NIST CSF	Cybersecurity risk management, organized around Identify, Protect, Detect, Respond, Recover	Organizations of any size building a cybersecurity risk program
NIST RMF	Structured, step-by-step process for applying security controls to information systems	Government agencies and contractors with formal system authorization requirements
ISO/IEC 27001	International standard for information security management systems, certifiable by an accredited auditor	Organizations that need a certifiable, internationally recognized standard
COBIT	Governance and management of enterprise IT, aligning IT goals with business goals	Organizations focused on IT governance and value delivery

COSO	Internal control and enterprise risk management framework, widely used in financial reporting	Organizations with financial reporting and internal control obligations (e.g., SOX)

13. Final Checklist: Are You GRC Ready?

This one-page checklist pulls together the single most important action from every section of the kit. If you can check every box, your program has the essentials in place; any unchecked box points you back to the relevant section for the detail you need.

☐ Program objectives and risk appetite are documented (Section 1)

☐ A framework has been selected and requirements mapped (Section 2)

☐ A live risk register exists and is scored consistently (Section 3)

☐ Controls are mapped to risks and requirements with evidence defined (Section 4)

☐ An implementation roadmap is underway (Section 5)

☐ Every control and risk has a named, accountable owner (Section 6)

☐ Technology needs have been assessed against program scale (Section 7)

☐ The organization could pass an audit readiness check today (Section 8)

☐ A continuous monitoring cadence is scheduled, not ad hoc (Section 9)

☐ The program has been self-assessed on the maturity scale in the last 12 months (Section 10)

14. About GSDC + Certification

The Global Skill Development Council (GSDC) offers certification programs designed to build practical, job-ready expertise across governance, risk, and compliance disciplines. A certification is a useful complement to a kit like this one: the kit gives your team a working toolset, while certification deepens the underlying knowledge of frameworks, control design, and organizational resilience behind it.

Build Practical GRC Expertise

Explore the GSDC GRC certification to strengthen your knowledge of governance, risk management, compliance, controls, and organizational resilience.

GSDC
Global Skill Development Council

CERTIFIED AI GRC PROFESSIONAL

THE AI GOVERNANCE, RISK & COMPLIANCE (AI GRC) CERTIFICATION PROGRAM IS GLOBALLY DESIGNED TO STRENGTHEN AI GOVERNANCE, RISK MANAGEMENT, REGULATORY COMPLIANCE, AND RESPONSIBLE AI IMPLEMENTATION SKILLS, ENABLING PROFESSIONALS TO ESTABLISH TRUSTWORTHY, SECURE, AND COMPLIANT AI SYSTEMS WHILE ALIGNING INNOVATION WITH ORGANIZATIONAL AND REGULATORY REQUIREMENTS.

ABOUT GSDC CERTIFICATION

EBOOK

Extensive and exclusive Ebook created by world's experts to help you with understanding core concepts.

EBOOK

Extensive and exclusive Ebook created by world's experts to help you with understanding core concepts.

CREATED BY EXPERTS

GSDC certifications are created and authored by world's leading experts in the field.

LEARNING MATERIALS

Get access to learning materials such as videos, ebooks, templates, and practice exams, which will help you clear the certification exam.

LEARNING OBJECTIVE

- Prove your knowledge of responsible AI principles including fairness, transparency, explainability, and human oversight in AI systems
- Understand how to design and implement AI security controls, manage adversarial risks, and build trustworthy AI programs across the organization

Enroll now with the code **LEARN20** To avail **20%** discount

Enroll Now

www.gsdcouncil.org