SELF-ASSESSMENT TOOL

The GRCForce Maturity Model Self-Assessment Tool

Diagnose Your GRC Operating Model in 30 Minutes

GRCForce | Practical GRC for Modern Organisations

Resource landing page: Open the resource page

Related article: The GRCForce Maturity Model

How to Use This Tool

This self-assessment is designed to give you an honest baseline — not where your policies say you are, but where your operating model actually performs.

Work through each of the five dimensions. Read each stage description carefully and select the one that most accurately describes your current state. If you are between stages, choose the lower stage. Honesty here is not a sign of weakness — it is the prerequisite for building a roadmap that actually moves you forward.

At the end of each dimension, record your score. Divide the total by five to get your overall GRCForce Maturity Score.

Time required: 30 minutes

Recommended participants: GRC lead, CISO, Head of Compliance, or Risk Manager

Part 1 — The GRCForce Maturity Model Canvas

Score each dimension from 1 (Reactive) to 5 (Continuous). Use the descriptions to guide your honest assessment.

Dimension 1: Governance Structures

Governance structures define decision rights, escalation paths, and accountability. A mature governance structure is one where every important decision has a clear owner, a clear process, and a clear escalation route — documented and tested, not assumed.

Stage	Label	What It Looks Like	GRCForce Diagnostic Marker
1	Reactive	No formal governance committees. Decisions made informally and ad-hoc.	Nobody can name who has authority to approve a risk exception.
2	Defined	Committees exist but terms of reference are vague. Authority is unclear.	Committees meet, but decisions still escalate to the same senior individual every time.
3	Managed	Clear decision rights. Escalation paths documented. Committees have defined authority.	A risk exception can be approved by the right committee without involving the board.
4	Integrated	Governance is embedded in strategy and business planning.	New joiners understand the governance structure within their first two weeks.
5	Continuous	Governance structures are reviewed and improved continuously based on effectiveness data.	The organisation proactively updates governance design ahead of regulatory or business change.

Your score for Governance Structures: ___

Dimension 2: Risk Management Integration

Risk management integration measures how well risk information flows across functions and how consistently it informs decisions. A mature integration means the risk team, compliance team, and security team share a common language, common evidence, and a common view of the organisation's risk posture.

Stage	Label	What It Looks Like	GRCForce Diagnostic Marker
1	Reactive	Risk is only assessed after an incident or audit finding. No formal process.	The risk register is rebuilt every time an audit approaches.
2	Defined	Formal risk process exists. Assessments are regular. But risk, compliance and security operate separately.	Three separate risk registers exist with no common entries.
3	Managed	Risk management integrated across functions. Common control matrix. Single view of risk.	One risk assessment satisfies ISO, GDPR, and client assurance requirements simultaneously.
4	Integrated	Risk management embedded in strategic and commercial decisions. Risk appetite defined and used.	Risk appetite is referenced in business case approvals, not just in board reports.
5	Continuous	Predictive risk management. Continuous monitoring. Data-driven decisions.	The organisation identifies emerging risks before they appear in audit findings or regulatory guidance.

Your score for Risk Management Integration: ___

Dimension 3: Control Ownership and Accountability

Control ownership measures the clarity and reliability of accountability across your control framework. A mature ownership model means every important control has a named individual responsible for operation, evidence, review, and escalation — and that individual understands their accountability.

Stage	Label	What It Looks Like	GRCForce Diagnostic Marker
1	Reactive	Control ownership is unclear or assigned to generic functions.	Controls are owned by "IT" or "Compliance" with no named individual.
2	Defined	Ownership is formally assigned. But owners do not always understand their responsibilities.	Owners are named in the register but cannot describe what their control requires in practice.
3	Managed	Named owners with clear accountability. Evidence produced by owners as part of normal operations.	Owners update their own evidence without being prompted by the GRC team.
4	Integrated	Owners drive continuous improvement of their controls. Backup owners are designated.	If the primary owner is absent, the backup can operate the control and produce evidence without interruption.
5	Continuous	Control owners proactively identify gaps and propose improvements.	Control owners raise maturity concerns to the governance committee before audits surface them.

Your score for Control Ownership and Accountability: ___

Dimension 4: Evidence Management

Evidence management measures how reliably and efficiently your organisation captures, stores, and retrieves proof that controls are operating. A mature evidence model means evidence is a by-product of operations — created automatically, stored consistently, and retrievable in minutes, not days.

Stage	Label	What It Looks Like	GRCForce Diagnostic Marker
1	Reactive	Evidence is assembled specifically for audits. Not maintained between audits.	The team spends two to four weeks assembling evidence before every annual audit.
2	Defined	Evidence exists and is mostly current. But stored inconsistently across teams and tools.	Evidence is in shared drives, email threads, and spreadsheets with no consistent structure.
3	Managed	Evidence accumulates as a by-product of normal operations. Stored consistently. Retrievable within hours.	An auditor requesting evidence from any quarter in the past two years receives it within one working day.
4	Integrated	Evidence is automatically captured and timestamped by operational tools. GRC platform integration in place.	Audit preparation time is measured in hours, not weeks. Evidence is never assembled manually.
5	Continuous	Evidence drives continuous improvement decisions. Patterns analysed to identify emerging control weaknesses.	Evidence data surfaces control degradation before it becomes an audit finding or an incident.

Your score for Evidence Management: ___

Dimension 5: Governance Culture

Governance culture measures the behavioural norms around risk, escalation, ownership, and transparency. A mature governance culture is one where bad news travels upward quickly, ownership is taken rather than avoided, and compliance is a norm rather than an obligation.

Stage	Label	What It Looks Like	GRCForce Diagnostic Marker
1	Reactive	Issues are hidden or minimised. Governance is seen as a compliance obligation, not a business value.	Staff are reluctant to report issues because they fear blame or extra work.
2	Defined	Issues are reported, but escalation is slow and dependent on individuals with the confidence to raise concerns.	Escalation requires personal courage rather than being expected as standard behaviour.
3	Managed	Transparent escalation is normal. Leaders model good governance behaviour visibly.	A junior team member can raise a risk concern directly to the governance committee without social risk.
4	Integrated	Governance culture is actively developed. Training, leadership behaviour, and incentives align.	Staff in non-GRC roles understand their governance responsibilities and can describe them clearly.
5	Continuous	Staff proactively identify improvement opportunities and act on them.	Governance improvement ideas originate from operational roles, not just the GRC function.

Your score for Governance Culture: ___

Part 2 — Scoring Your Assessment

Overall Maturity Score

Dimension	Your Score (1-5)
Governance Structures	___
Risk Management Integration	___
Control Ownership and Accountability	___
Evidence Management	___
Governance Culture	___
Total	___
Overall Score (Total divided by 5)	___

What Your Score Means

Score Range	GRCForce Stage	Interpretation	Immediate Priority
1.0 - 1.9	Stage 1 — Reactive	Governance is ad-hoc and dependent on individual effort. Audit and incident risk is high.	Establish formal ownership and a basic governance rhythm immediately.
2.0 - 2.9	Stage 2 — Defined	Foundation exists but is fragmented. Functions operate in silos. Most organisations sit here.	Prioritise integration of risk, compliance and security under one control framework.
3.0 - 3.9	Stage 3 — Managed	Operating model is functioning. Evidence accumulates naturally. Audits are manageable.	Focus on resilience: can the model survive a key personnel departure?
4.0 - 4.9	Stage 4 — Integrated	Strong, scalable operating model. GRC supports commercial confidence.	Focus on continuous improvement and predictive capability.
5.0	Stage 5 — Continuous	GRC is a competitive differentiator. The organisation anticipates risk.	Your model is a benchmark. Share it. Others can learn from it.

Dimension Gap Analysis

Review your scores by dimension. Any dimension scoring two or more stages below your highest-scoring dimension represents a structural gap that will limit your overall maturity regardless of strength elsewhere.

Common gap pattern: Organisations frequently score Stage 3 on governance structures and risk management but Stage 1 or Stage 2 on evidence management and culture. This produces an operating model that looks strong in design but fails under audit pressure or personnel change.

Part 3 — Twelve-Month Improvement Roadmap

Use this roadmap to plan from your current overall score toward your target state. Select the phase that corresponds to your current stage.

Phase A: Reactive to Defined (Stage 1 to Stage 2)

Estimated duration: 3-6 months

Priority	Action	Responsible	Evidence of Completion
1	Establish a governance committee with documented terms of reference and clear decision authority	Senior Sponsor + GRC Lead	Signed terms of reference, first meeting minutes
2	Build a formal risk management process with a maintained risk register	GRC Lead	Risk register reviewed at first committee meeting
3	Assign named control owners to all critical controls	Control Owners	Control owner list published and signed off
4	Establish a basic evidence storage structure with consistent naming and access controls	GRC Lead + IT	Evidence location documented and owners briefed
5	Communicate governance responsibilities to all staff	HR + GRC Lead	Completion record from awareness communication

Phase B: Defined to Managed (Stage 2 to Stage 3)

Estimated duration: 3-6 months. This is the highest-value transition for most organisations.

Priority	Action	Responsible	Evidence of Completion
1	Consolidate separate risk, compliance and security assessments into a single universal control matrix	GRC Lead + Risk + Security	Single control matrix adopted; duplicate assessments retired
2	Embed evidence production into operational processes so that evidence accumulates as a by-product	Control Owners + IT	Evidence auto-captured for top twenty critical controls
3	Establish predictable governance rhythms: weekly tactical stand-up and monthly risk committee	GRC Lead	Calendar established; first three cycles completed
4	Rewrite governance committee terms of reference to specify decision authority explicitly	Senior Sponsor + GRC Lead	Updated terms of reference approved
5	Designate named backup owners for all critical controls	Control Owners	Backup owner list published and tested

Phase C: Managed to Integrated (Stage 3 to Stage 4)

Estimated duration: 6-12 months

Priority	Action	Responsible	Evidence of Completion
1	Integrate GRC into project governance, procurement approvals and strategic planning	GRC Lead + Business	GRC checkpoints embedded in project methodology
2	Define and board-approve risk appetite with threshold-based decision authorities	Senior Sponsor + Board	Approved risk appetite statement
3	Document the full operating model — every forum, workflow and handover — so it survives staff changes	GRC Lead	Operating model documentation; tested with a new joiner
4	Implement GRC platform integration to eliminate manual evidence assembly	IT + GRC Lead	Audit preparation time below one working day
5	Develop governance awareness programme for non-GRC staff	HR + GRC Lead	Training completion record; culture survey baseline

Phase D: Integrated to Continuous (Stage 4 to Stage 5)

Estimated duration: 12-24 months

Priority	Action	Responsible	Evidence of Completion
1	Implement continuous monitoring dashboard for key controls and risk indicators	GRC Lead + IT	Live monitoring dashboard reviewed in every committee meeting
2	Establish predictive risk process: horizon scanning, regulatory watch, threat intelligence	Risk Lead	Quarterly emerging risk brief to board
3	Conduct annual GRCForce Maturity Model reassessment and present results to board	GRC Lead	Updated maturity scorecard; board presentation
4	Develop GRC as a commercial asset: client assurance packs and supplier due diligence automation	GRC Lead + Commercial	Standard assurance pack available to sales within 24 hours
5	Plan next improvement cycle based on maturity data and audit outcomes	GRC Lead	Next 12-month improvement roadmap approved

Part 4 — Anti-Patterns to Avoid

These patterns consistently prevent organisations from advancing through the GRCForce Maturity Model stages.

Anti-Pattern	What It Looks Like	Stage It Blocks	How to Break It
The Heroic Effort Trap	GRC depends on one or two highly capable individuals. Everything stops when they leave.	Stage 2 to 3	Document the operating model. Build the system, not the person.
The Silo Problem	Risk, compliance and security operate independently with separate processes, evidence and reports.	Stage 2 to 3	Build a universal control matrix. One assessment, multiple outputs.
The Policy Graveyard	Policy library has grown without consolidation. Policies contradict each other or nobody reads them.	Stage 2 to 3	Consolidate. Fewer, clearer, shorter policies with named owners.
The Evidence Scramble	Evidence exists only because someone assembles it before each audit. No systematic accumulation.	Stage 3 to 4	Integrate evidence production into operational tools and workflows.
The Governance Theatre	Committees exist and meet, but decisions still escalate to one senior individual.	Stage 3 to 4	Rewrite terms of reference. Test decision-making in simulation exercises.
The Culture Gap	Governance structures are strong on paper but escalation requires personal courage.	Stage 4 to 5	Leadership behaviour is the only lever. Senior leaders must visibly model and reward transparent escalation.

Next Step

Use the scores from this assessment to identify your current GRCForce Maturity Stage and your single highest-priority improvement action.

If your canvas shows too many dimensions at Stage 1 or Stage 2, or if you are unsure how to sequence the improvements, GRCForce can support a focused GRC Operating Model Review — typically a four to six week engagement that produces a prioritised improvement plan, an updated control framework, and a governance model your team can sustain independently.

The review covers:

- Governance structure and decision rights.
- Risk management integration and control matrix design.
- Control ownership and accountability model.
- Evidence architecture and tool integration.
- Culture and escalation programme.

Start a conversation with GRCForce.