Buyer's Guide 2026:

Choosing the Right GRC Platform

SURECLOUD®

www.surecloud.com

SURECLOUD®

GDPR Compliant

teiss Awards Winner Best Security Compliance Product

Buyers Guide Contents

Highlights

- A 2026 buyer framework for choosing a GRC platform that supports defensible reporting and assurance confidence
- Practical evaluation criteria and a scoring checklist to reduce buying risk and avoid shortlists that fail after go live
- Guidance on success measures, adoption, and implementation fundamentals so the platform becomes a trusted system of record

Who should read this?

This guide is designed for senior stakeholders involved in GRC tooling decisions, including:

- Security leaders and CISOs
- Risk leaders and ERM owners
- Compliance and operational resilience owners
- Internal audit and assurance leaders
- Procurement and vendor governance stakeholders
- IT and transformation leaders responsible for delivery and integration

1. Executive Summary

1.1 What has changed in GRC buying

GRC is no longer treated as a set of isolated compliance activities. In practice, many organisations now need one connected view of governance, risk, and compliance to support decision making, assurance, and audit readiness. The Open Compliance and Ethics Group defines GRC as an integrated collection of capabilities that help organisations achieve objectives, address uncertainty, and act with integrity.[1] Many buyers also treat 'GRC platforms' as a distinct category, reflecting a broader shift from point tools toward connected platforms that support governance, risk, and assurance.

At the same time, regulatory expectations continue to expand across sectors and domains. The European Commission describes NIS2 as a unified legal framework to strengthen cybersecurity across critical sectors, which increases the need for consistent governance and evidence across teams.[2]

In the financial sector, DORA sets expectations for digital operational resilience, including ICT risk management and oversight, which pushes many organisations to improve how they manage controls, issues, and reporting.[3]

AI is adding a further layer of governance and assurance expectations. According to NIST's AI Risk Management Framework, AI risk management should be treated as a structured discipline that helps organisations manage risks and promote trustworthy development and use of AI systems.[4]

1.2 What this guide helps buyers do

This guide is designed for senior stakeholders involved in GRC tooling decisions, including security, risk, compliance, audit, and procurement.

It helps buyers:

- Clarify what outcomes the platform must support, before comparing features
- Evaluate platforms using practical criteria that stand up to scrutiny from leadership, auditors, and regulators
- Avoid common buying mistakes that slow adoption and delay value
- Build a shortlist that can scale as requirements expand across cyber, operational resilience, third party risk, and AI governance

1.3 The practical next step

If the organisation is replacing a legacy tool, expanding beyond spreadsheets, or consolidating fragmented workflows, the fastest way to make progress is to start with the end in mind.

Define the reporting and assurance outputs leaders need, then work backwards to required workflows, evidence, and ownership. Use the evaluation checklist in this guide to translate those needs into buying criteria. Run a proof of value focused on evidence quality, reporting, and adoption, not feature demonstrations.

2. The GRC Landscape in 2026

2.1 Regulatory expansion and overlap

The regulatory environment is expanding in scope and becoming harder to manage in separate streams. The European Commission describes NIS2 as a unified EU framework to strengthen cybersecurity across critical sectors, increasing the need for consistent governance and evidence across teams.[2]

In parallel, sector specific resilience rules are raising expectations for structured oversight and consistent control evidence. DORA sets requirements for digital operational resilience in the financial sector, reinforcing the need for traceable ICT risk management practices, testing, and third party oversight.[3]

For many buyers, the practical issue is overlap. Controls, policies, and evidence often need to satisfy multiple requirements at the same time. When governance artefacts live in separate tools or teams, duplication grows, reporting becomes slower, and assurance confidence drops.

2.2 Board level accountability and assurance expectations

Boards and executive stakeholders are under increasing pressure to understand risk posture, not just compliance status. The Global Internal Audit Standards set expectations for internal audit work that evaluates and contributes to effective governance, risk management, and control processes, reinforcing the broader shift towards decision useful assurance.[5]

In buying terms, this shifts what “good” looks like in a platform. It is less about whether a team can record risks, and more about whether leadership can see clear ownership, trend lines, remediation progress, and confidence in the underlying data.

2.3 Technology driven risk acceleration

Technology change cycles are faster, environments are more connected, and third party dependence is deeper. As complexity rises, manual ways of working tend to break first: evidence collection, control mapping, and reporting cadence.

This is one reason many organisations move away from fragmented processes. When risk and compliance data is spread across spreadsheets, ticketing tools, and shared drives, it becomes difficult to prove who changed what, when it changed, and what the current state actually is.

2.4 AI governance and assurance requirements

AI is now a mainstream governance topic, not a specialist side project. The EU AI Act lays down harmonised rules for AI in the EU, increasing the need for documented governance, risk assessment, and ongoing oversight.[6]

Alongside regulation, NIST’s AI Risk Management Framework is designed to help organisations manage AI risks and incorporate trustworthiness considerations across design, development, use, and evaluation.[4]

For GRC tooling decisions, the key is whether the platform can support AI governance in a defensible way: clear accountability, documented decisions, review checkpoints, and evidence trails that hold up when questioned.

3. Why Organisations Are Replacing Legacy GRC Tools

3.1 Manual evidence collection and audit fatigue

Many GRC programmes still rely on manual evidence collection across shared drives, email threads, and spreadsheets. Over time, this creates predictable friction: repeated requests for the same artefacts, inconsistent versions of the truth, and long lead times to assemble audit ready evidence.

Cost pressure is a common trigger for change. Deloitte's analysis of regulatory productivity describes compliance as a heavy burden for many firms and notes significant increases in compliance operating costs over time, reinforcing why buyers increasingly look for process improvement and technology enabled efficiency.[7]

In practice, organisations replace legacy tools when the effort to maintain evidence, answer questions, and produce defensible reporting becomes too slow, too manual, or too dependent on a small number of people.

3.2 Disconnected systems and inconsistent controls

Another common driver is fragmentation. Risk registers, control libraries, audits, issues, incidents, and third party assessments often sit in separate tools owned by different teams. That separation makes it harder to maintain consistent control definitions, map requirements reliably, and track remediation in a way leaders trust.

As a result, organisations can end up testing similar controls multiple times, reporting different answers depending on the audience, and spending more time reconciling data than reducing risk.

3.3 Reporting limitations and slow decision making

Legacy tooling frequently struggles when reporting needs become more demanding. Leaders want a view that is current, consistent, and easy to interpret, including clear ownership and progress. When reporting depends on manual consolidation, it tends to be out of date by the time it reaches decision makers.

This is also where buying decisions often shift from "a place to record risks" to "a platform that supports governance and assurance." Buyers start prioritising data quality, traceability, and reporting confidence over feature lists.

3.4 Spreadsheet based approaches and data integrity risk

Spreadsheets are a common starting point for early stage GRC work because they are accessible and flexible. The risk appears when the organisation scales. As scope expands, spreadsheets become harder to govern, harder to secure, and harder to validate.

Research on spreadsheet errors consistently finds that errors are common, which becomes a serious operational risk as spreadsheets grow in size and importance. Panko's research discusses how spreadsheet errors occur at meaningful rates and why, in large spreadsheets, the issue becomes how many errors exist rather than whether an error exists.[8]

A literature review by Powell, Baker, and Lawson summarises research showing spreadsheet error risk is persistent and difficult to control without formal approaches, which is one reason organisations move away from spreadsheet led GRC once reporting and assurance expectations increase.[9]

For many buyers, this is the tipping point: when the organisation can no longer confidently prove data lineage, changes, and approvals, spreadsheets stop being a workable system of record for governance, risk, and compliance.

4. What a Modern GRC Platform Must Deliver

4.1 Integrated risk and compliance

A modern platform should support a single, connected approach to governance, risk, and compliance so that risks, controls, obligations, issues, and remediation actions do not live in separate systems. The Open Compliance and Ethics Group defines GRC as an integrated collection of capabilities that help organisations achieve objectives, address uncertainty, and act with integrity.[1]

In practical terms, integration means one control library that maps consistently across requirements, one set of owners and accountability, and one place to see testing status, exceptions, and remediation progress. This reduces duplication and helps leadership rely on the data without constant reconciliation.

4.2 Automation and workflow orchestration

As scope grows, manual coordination becomes the bottleneck. A modern platform should reduce reliance on email chains and spreadsheets by supporting structured workflows for evidence requests, approvals, reviews, attestations, testing cycles, and remediation tracking, with a clear audit trail for decisions and changes.

Forrester's commentary on the GRC platform market highlights the importance of improvements to workflow and the overall analyst experience to reduce friction and scale.[10]

The goal is not automation for its own sake. The goal is to make governance repeatable, reduce rework, and keep reporting current without forcing teams into constant manual follow up.

4.3 AI with human oversight

AI can support GRC work when it is applied in controlled, reviewable ways, such as helping triage issues, summarise evidence, suggest mappings, or identify anomalies. What matters is that AI outputs are transparent, reviewable, and governed with clear accountability.

NIST's Generative AI Profile, published as part of the AI Risk Management Framework, is designed to help organisations manage generative AI risks and implement trustworthy risk management practices, which reinforces why oversight and governance must be built into AI enabled workflows.[11]

In buying terms, assess whether the platform supports review checkpoints, clear ownership, documented rationale, and traceable evidence for any AI assisted outputs that influence risk or compliance decisions.

4.4 Executive visibility and reporting

A platform is only as useful as the decisions it supports. Modern GRC reporting should help leaders see what matters without waiting for manual consolidation: risk trends, control coverage, overdue actions, remediation progress, and confidence indicators such as data freshness and completion status.

The Global Internal Audit Standards reinforce the importance of reliable evaluation and communication around governance, risk management, and controls, which supports the expectation that reporting should be decision useful, not just a record of activity.[5]

Buyers should look for reporting that is board ready by design, with drill down that connects headline metrics to underlying evidence and ownership.

4.5 Scalability and configurability

A platform should scale as requirements expand across cyber risk, operational resilience, third party risk, privacy, and AI governance, without forcing a rebuild each time scope changes. Configurability matters because it affects time to value, maintainability, and the organisation's ability to evolve workflows as governance maturity increases.

Forrester's market view notes that differentiated vendors support vast requirements while also providing a degree of pre configured applications, content, and best practices to meet customers at different levels of maturity.[10]

In evaluation, focus on whether the platform can adapt safely through configuration, support controlled change management, and maintain clear audit trails as processes and control sets evolve.

5. Buyer Evaluation Framework and Checklist

5.1 Strategic alignment

Start by defining the outcomes the organisation needs from a GRC platform in the next 12 to 24 months, then pressure test whether the platform supports the operating model required to achieve them.

Key questions

- What decisions should the platform support at board and executive level
- Which risk and compliance domains must be in scope now, and which are likely to be added next
- What is the target level of standardisation across teams, versus local flexibility
- What evidence outputs must be produced regularly, and for whom

Risk governance principle to anchor the approach

GRC should be treated as an integrated capability that supports objectives and uncertainty management, not as disconnected tooling for separate functions.[1]

5.2 Functional depth

Functional depth is about whether the platform can support your real workflows end to end, not whether it has a long feature list.

Focus areas to validate in demonstrations

- **Risk lifecycle:** identification, assessment, treatment, monitoring, review
- **Control lifecycle:** control library, mapping, testing, exceptions, remediation, evidence
- **Obligations and requirements:** structured obligations, mapping, tracking, change handling
- **Audit and assurance:** planning, testing, evidence collection, findings, actions, reporting
- **Third party workflows:** onboarding, assessments, issues, ongoing monitoring, reporting

If AI is in scope, treat it as a governed capability, not a novelty

- Clear ownership for AI assisted outputs
- Review checkpoints before outputs become records or decisions
- Traceability from output back to inputs and rationale

NIST provides a cross sector framework for managing AI risks and promoting trustworthy AI, which supports the need for governance and oversight in AI enabled workflows.[4]

5.3 Data integrity

A platform can only improve decisions if it improves data confidence.

What to evaluate

- **Data model clarity:** consistent definitions for risks, controls, issues, owners, status
- **Change traceability:** who changed what, when, and why
- **Evidence lineage:** where evidence came from, what it supports, how current it is
- **Reuse:** ability to reuse controls, evidence, and assessments across requirements
- **Reporting trust:** confidence indicators such as completion, freshness, and approvals

Spreadsheet led approaches struggle here at scale because errors are common and difficult to eliminate in large spreadsheets used for operational records.[8]

5.4 Security and privacy

Treat the platform as part of your risk surface, because it will store sensitive governance data.

Minimum evaluation areas

- **Access control model**: role based access, segregation of duties, least privilege support
- **Audit logs:** completeness, immutability expectations, retention options
- **Data handling:** encryption, backup, retention, deletion, data residency where required
- **Supplier assurance:** independent security attestations and transparent security posture
- **Privacy controls:** support for privacy obligations where relevant to stored data

If the organisation operates in regulated sectors, confirm how the platform supports evidence and oversight expectations linked to operational resilience requirements.[3]

5.5 Implementation and time to value

Implementation success depends on delivery approach, configurability, and adoption planning.

What to validate

- Time to first usable outcomes, not time to full rollout
- Configuration versus custom development expectations
- Data migration effort and data quality remediation plan
- Integration requirements with core systems, including identity and reporting
- Training, enablement, and the operating model needed after go live

Procurement can strengthen outcomes by benchmarking proposals, simulating true costs, and holding suppliers accountable through structured processes and data driven evaluation.[12]

5.6 Vendor viability

Long term viability is part of risk management. Buyers should evaluate whether the supplier can support the programme as scope grows.

What to assess

- Product direction and investment signals
- Customer support model and response expectations
- Implementation ecosystem and partner support where relevant
- Commercial transparency: licensing model, cost drivers, scaling assumptions
- References and proof: case studies that match your use cases and maturity

Market evaluation research can be useful as a directional signal when it aligns with your needs and is interpreted as one input, not the decision.[10]

5.7 Buyer checklist buyers can use

Use this as a practical scoring tool during shortlisting. Score each line 0, 1, or 2.

0 means not met

1 means partially met or requires workarounds

2 means clearly met with evidence in the demonstration or documentation

Strategic alignment

- ☐ Clear support for the operating model required across risk, compliance, and audit
- ☐ Supports current scope and expected expansion without a redesign
- ☐ Reporting outputs align with leadership needs and assurance expectations

Functional depth

- ☐ End to end risk lifecycle supported in the way your teams actually work
- ☐ End to end control lifecycle with mapping, testing, exceptions, and remediation
- ☐ Obligations tracking and change handling supports regulatory overlap
- ☐ Audit and assurance workflows support repeatable evidence collection
- ☐ Third party workflows support onboarding, assessments, and ongoing oversight

Data integrity

- ☐ Strong ownership model with clear accountability and approvals
- ☐ Full audit trail for changes to risks, controls, issues, and evidence
- ☐ Evidence lineage is clear and reusable across requirements
- ☐ Reporting includes confidence indicators and can be trusted without manual reconciliation

Security and privacy

- ☐ Role based access control supports segregation of duties
- ☐ Audit logs and retention support governance requirements
- ☐ Security posture is transparent and independently validated where required
- ☐ Data handling controls align with organisational privacy obligations

Implementation and time to value

- [ ] Clear path to first usable outcomes in a short timeframe
- [ ] Configurability supports change without heavy custom development
- [ ] Data migration and integration approach is realistic and resourced
- [ ] Training and adoption plan is included, not left as an afterthought

Vendor viability

- [ ] Clear product roadmap and evidence of ongoing investment
- [ ] Support model, service levels, and escalation paths are clear
- [ ] Commercial model is transparent and scales predictably
- [ ] Customer references match your industry, size, and maturity level

6. Common Buying Mistakes and How to Avoid Them

6.1 Buying for one regulation

A common mistake is selecting a tool to solve one urgent regulatory requirement, then discovering it cannot scale when scope expands across cyber risk, operational resilience, third party risk, privacy, and AI governance. NIS2 and DORA show how expectations can cut across governance, risk management, oversight, and evidence in ways that create overlap in control and reporting needs.[2] [3]

How to avoid it

- Define the future scope upfront, including the next two or three risk and compliance domains the organisation is likely to add
- Require a single control library approach with consistent mapping across obligations
- Test reporting for cross requirement questions, not just a single compliance view

6.2 Over weighting features instead of outcomes

Another frequent issue is treating the buying process as a feature comparison exercise. This often produces a shortlist that looks strong in demos but fails when teams try to operationalise workflows, produce evidence, or deliver trusted reporting.

GRC platform selection is widely recognised as a cross functional decision that requires collaboration across business, IT, compliance, and audit because success depends on how well the platform supports real operating processes, not just tool capability in isolation.[13]

How to avoid it

- Write outcome led requirements first, anchored in the reports and decisions leaders need
- Ask vendors to demonstrate end to end workflows using your scenarios, your roles, and your cadence
- Score platforms on evidence quality, reporting confidence, and adoption readiness, not the number of modules

6.3 Underestimating change management and adoption

GRC tooling changes behaviour. If ownership, incentives, communications, and reinforcement are not planned, the platform may go live but fail to become the system of record.

Prosci research links strong change management to higher rates of meeting or exceeding project objectives, and shows a large gap between outcomes for excellent change management versus poor change management. This is a practical warning for GRC programmes where success depends on consistent use across multiple teams.[14]

How to avoid it

- Make adoption part of the buying criteria, including role based training, workflow design, and leadership sponsorship
- Confirm how accountability will work after go live: who owns the control library, who owns reporting, who owns remediation follow up
- Pilot with the teams that will carry the workload, then expand based on what was learned

6.4 Treating implementation as a one time project

Many buyers plan implementation as a single delivery event, then underestimate what happens next: ongoing changes to obligations, evolving reporting needs, and continuous improvement expectations. That gap can lead to a platform that is technically deployed but operationally brittle.

Transformation work often fails when organisations overlook execution fundamentals and do not manage the practical work of embedding change across teams. McKinsey highlights common pitfalls that undermine transformation success, which maps closely to system implementations where sustained adoption is required.[15]

How to avoid it

- Plan for phased delivery with clear success measures for each phase, starting with one or two high value workflows
- Build a sustainment model: reporting cadence, data quality checks, ownership of updates, and governance for configuration changes
- Treat the platform as a living capability that must evolve with risk and regulatory expectations, not a static system that is finished at go live

7. Real World Use Cases

7.1 Enterprise risk management

Enterprise risk management becomes difficult when risk registers are disconnected from controls, issues, and remediation. The result is often a list of risks with limited visibility into what is being done, whether it is working, and what has changed since the last review.

What good looks like in a platform

- A consistent risk model that supports ownership, assessment, treatment planning, and review cadence
- Links between risks, controls, issues, and actions so reporting reflects reality, not assumptions
- Reporting that supports leadership decisions, including trend movement, top drivers, and residual risk confidence

A practical test in evaluation

Ask vendors to demonstrate a quarterly risk review workflow end to end, including how changes are approved, how actions are tracked, and how the board view is generated from underlying evidence.

7.2 Third party risk management

Third party risk is often where tools and processes break down because it spans onboarding, assurance, contracts, security reviews, ongoing monitoring, and incident response. Requirements in DORA reinforce the need for structured third party oversight and resilience expectations in the financial sector, which is a useful benchmark for what good governance looks like even outside regulated industries.[3]

What good looks like in a platform

- A central inventory of third parties with clear ownership and tiering
- Standardised assessments aligned to risk level and service criticality
- Findings linked to remediation actions, deadlines, and evidence
- Ongoing review schedules with traceable outcomes over time

A practical test in evaluation

Ask vendors to demonstrate how a critical supplier is assessed, how issues are raised and tracked, and how leadership reporting shows current risk and remediation progress without manual consolidation.

7.3 Control automation and continuous control monitoring

Control programmes struggle when control definitions are inconsistent, testing is not repeatable, and evidence collection is manual. This is where buyers start looking for workflow support and automation that improves consistency and reduces rework.

What good looks like in a platform

- One control library that maps across obligations and standards
- Testing schedules and evidence requests that run on a cadence with clear ownership
- Automated reminders, approvals, and audit trails that show completion and exceptions
- A clear view of control coverage and gaps across requirements

A practical test in evaluation

Ask vendors to demonstrate one control across multiple obligations, then show how evidence is collected, reviewed, approved, and reused without duplicating effort.

7.4 Audit readiness and assurance reporting

Audit readiness fails when evidence is scattered, versions are unclear, and teams cannot explain what changed since the last audit. The Global Internal Audit Standards reinforce expectations for internal audit activity that evaluates and contributes to effective governance, risk management, and control processes, which supports the need for reliable evidence and decision useful reporting.[5]

What good looks like in a platform

- Structured audit planning and fieldwork support, including scope, testing, and evidence collection
- Findings linked to actions with clear owners and deadlines
- Reporting that can be produced quickly and trusted because it is built on current workflow data
- Traceability that supports who did what, when, and why, across the audit trail

A practical test in evaluation

Ask vendors to demonstrate how an audit report is produced and how each statement can be traced back to controls, testing outcomes, evidence, and approvals.

7.5 AI risk governance

AI governance is moving from policy statements to operational assurance. The EU AI Act introduces harmonised rules for AI and increases expectations for documented governance, risk assessment, and oversight, particularly for higher risk use cases.[6]

NIST's AI Risk Management Framework provides a structured approach to managing AI risks and promoting trustworthy AI, which is useful when defining what evidence and accountability should look like in practice.[4]

What good looks like in a platform

- A clear inventory of AI systems and use cases with owners and accountability
- Risk assessments and approvals that are documented, reviewable, and repeatable
- Controls and monitoring activities that produce evidence over time
- A governance workflow that supports periodic review and change management as models, data, and use cases evolve

A practical test in evaluation

Ask vendors to demonstrate how an AI use case is approved, how risks are assessed and reviewed, and how ongoing monitoring evidence is captured and reported in a way that holds up under scrutiny.

8. Measuring GRC Success

8.1 Outcome based metrics that matter

Measuring success starts with clarity on what the GRC programme is meant to improve. Metrics should show whether risk is being reduced, assurance confidence is increasing, and the organisation can respond faster when priorities change. COSO's ERM guidance places risk alongside strategy and performance, which supports measuring not only activity, but whether risk management is helping the organisation achieve objectives.[16]

A practical way to structure measurement is to separate three metric types:

- **Outcome metrics:** These show whether risk exposure is trending in the right direction and whether the programme is improving decision making. Examples include risk reduction over time for top risks, reduction in repeat findings, or improvement in control effectiveness ratings.
- **Performance metrics:** These show whether key processes are working efficiently. ISACA describes how KRIs and KPIs can be integrated in technology risk management, which supports using a mix of indicators to track both exposure and execution.[17]
- **Confidence metrics:** These show whether leaders can trust the reporting. Examples include evidence freshness, completion rates, approval coverage, and the percentage of controls with clear ownership.

If AI governance is in scope, add AI risk metrics deliberately. NIST's AI Risk Management Framework includes a Measure function focused on selecting and applying appropriate methods and metrics for AI risks, which reinforces the need for defined indicators and ongoing monitoring.[4]

8.2 Example KPI set for year one

Below is a pragmatic year one set that works across most organisations. It avoids vanity metrics and focuses on visibility, accountability, and reduced rework.

Risk and control outcomes

- Percentage of top risks with a current treatment plan and named owner
- Percentage of key controls rated effective, and trend over time
- Number of repeat findings by theme and trend over time
- Reduction in open high severity issues beyond agreed due dates

Operational performance

- Median time to collect, review, and approve evidence for key controls
- Percentage of scheduled control tests completed on time
- Median time to remediate audit findings by severity
- Percentage of third party assessments completed to schedule for critical suppliers

Reporting confidence

- Percentage of controls with current evidence within the defined validity window
- Percentage of key records with complete ownership and approval metadata
- Percentage of high impact reports produced without manual consolidation outside the platform

AI governance measures, if relevant

- Percentage of AI use cases with documented approval and ownership
- Percentage of in scope AI systems with defined monitoring metrics and review cadence
- Number of material model changes assessed through governance workflow and completed on time
- To keep the set realistic, start with a small number of measures that leadership will actually review, then expand once reporting is stable and trusted

8.3 Reporting cadence and ownership

Metrics only improve outcomes when they are reviewed consistently and owned clearly. The Global Internal Audit Standards include expectations around communicating results and supporting effective governance, which aligns with establishing a reliable reporting cadence and clear accountability for what gets reported and acted on.[5]

A practical cadence model

- **Monthly operational review for risk and compliance owners:** Focus on overdue actions, evidence coverage, control testing progress, and emerging issues.
- **Quarterly executive review:** Focus on top risk movement, control effectiveness trends, repeat findings, and remediation performance.
- **Periodic assurance reporting:** produce a consistent pack that links conclusions to evidence and ownership.[18]

Ownership model

- Assign a named owner for each metric, not just each risk or control
- Define who approves the reporting pack and who is accountable for follow up actions
- Treat metric definitions as controlled content so they do not drift over time

9. Implementation and Adoption Considerations

9.1 Phased deployment approach

A phased rollout tied to clear outcomes reduces change load, limits data migration risk, and helps teams build confidence in reporting before scope expands.

A practical phased approach

- **Phase 1: Establish the core data model and reporting outputs**

  Agree definitions for risks, controls, issues, actions, owners, and status. Build the first executive level reporting pack from live platform data, not spreadsheets.
- **Phase 2: Embed one or two high value workflows**

  Common starting points are control testing and evidence collection, audit actions tracking, or third party assessment workflows.
- **Phase 3: Scale across domains**

  Expand to additional obligations, teams, and workflows once the first set is stable and trusted.

This aligns with the principle that buyers should start less complex and evolve as governance maturity increases, rather than loading everything on day one.

9.2 Governance ownership model

A GRC platform only becomes a system of record when ownership is explicit. Define who owns the control library, who approves changes, who owns reporting, and who is accountable for follow up on actions.

Minimum ownership decisions to lock early

- Control library ownership and change approvals
- Risk taxonomy ownership and review cadence
- Evidence standards, including what counts as acceptable evidence and validity periods
- Reporting ownership, including who signs off on executive packs
- Issue and remediation ownership, including escalation paths when deadlines slip

Internal audit standards reinforce the need for effective governance, risk management, and control processes, which supports formalising ownership and

accountability for how GRC information is maintained and reported.[5]

9.3 Stakeholder adoption plan

Adoption is not a training event. It is a change programme that needs sponsorship, clear expectations, and reinforcement. Prosci's research links strong change management with higher rates of meeting or exceeding project objectives, which is a relevant warning for GRC programmes that depend on consistent participation across teams.[14]

A practical adoption plan should include

- A stakeholder map that identifies who will use the platform, who will supply evidence, and who will consume reporting
- Role based workflows that match how teams actually work
- A communications plan that explains what is changing, why it matters, and what success looks like
- Reinforcement mechanisms, including reporting cadence, accountability routines, and leadership visibility

McKinsey's work on transformation pitfalls highlights how execution often fails when organisations do not manage the practical work of embedding change, which applies directly to GRC platform rollouts that require sustained use.[15]

9.4 Data quality and migration realities

Data is usually the hardest part. Legacy tools and spreadsheets often contain inconsistent definitions, missing ownership, duplicated records, and outdated status fields. If those issues are migrated without remediation, the platform can go live with unreliable reporting, which undermines trust and adoption.

A realistic approach

- Start with the minimum dataset needed to support Phase 1 reporting
- Clean and standardise definitions before importing, especially for control names, risk ratings, ownership, and status
- Define what historical data must be migrated versus archived
- Establish data governance routines early, including periodic reviews and rules for required fields

Spreadsheet risk is well established, and error risk increases as spreadsheets grow and become operational records, which is a key reason to treat migration as a quality programme rather than a technical transfer.[8]

10. Conclusion and Next Steps

10.1 How to shortlist

A strong shortlist process reduces risk by making decision criteria explicit and repeatable. Start by converting the evaluation framework in Section 5 into a weighted scorecard, then limit the shortlist to vendors that can demonstrate end to end workflows using your scenarios.

A practical shortlist method

- **Step 1: lock the top outcomes**

  Confirm what the organisation must improve in the next 12 to 24 months, such as evidence quality, reporting confidence, remediation speed, or cross requirement control consistency.
- **Step 2: define non negotiables**

  Examples include a single control library approach, full audit trail, role based access control, and board ready reporting.
- **Step 3: score against your operating reality**

  Require demonstrations that show your workflows, your roles, your cadence, and your reporting outputs.
- **Step 4: keep the shortlist small**

  Two or three vendors is usually enough for a proof of value, and reduces evaluation fatigue.

Treat GRC as an integrated capability when designing the shortlist criteria, not as disconnected tooling requirements across different functions.

10.2 How to run a proof of value

A proof of value should focus on whether the platform can produce defensible reporting and reduce manual work in a way teams will adopt. It should not be a feature tour.

A practical proof of value structure

- **Scope: one or two workflows with high business value**

  Common choices are control testing and evidence collection, audit findings and remediation tracking, or third party assessment workflows.
- **Inputs: your data, not vendor sample data**

  Use a subset of real controls, obligations, suppliers, and reporting needs so results are meaningful.
- **Outputs: board and executive reporting pack**

  Require the vendor to generate leadership reporting from live workflow data, including ownership, progress, exceptions, and evidence links.
- **Success measures: define them upfront**

  Examples include reduction in manual consolidation, evidence collection cycle time, reporting freshness, and completeness of audit trails.

Where AI is involved, require governance controls. NIST's AI Risk Management Framework provides a structured approach to managing AI risks and promoting trustworthy AI, which supports setting clear oversight expectations for AI assisted outputs.

10.3 What to ask vendors

Use these questions to test whether the platform will hold up in real governance conditions, not just in demonstrations.

Data integrity and audit trail

- How does the platform record who changed what, when, and why for risks, controls, issues, and evidence
- Can audit trails be filtered and exported for assurance purposes without manual work
- How does the platform handle versioning for policies, controls, and evidence

Control and obligations management

- How does the platform support one control library mapped across multiple obligations and standards
- How are changes to obligations managed, including updates to mappings, testing, and reporting

Workflow and adoption

- How are evidence requests, approvals, attestations, and remediation actions managed end to end
- What role based experiences exist for contributors versus approvers versus leadership
- What adoption support is included beyond initial training

Security and privacy

- What access control options exist, including segregation of duties and least privilege
- What security attestations and security documentation can be provided
- What data residency, encryption, retention, and deletion controls are available

Operational resilience and third party oversight, where relevant

- How does the platform support third party oversight workflows, including assessments, issues, and reporting
- How can the organisation evidence governance and oversight expectations aligned with operational resilience requirements such as DORA, where applicable

AI governance, where relevant

- What AI features exist and what is the governance model for their outputs
- What review checkpoints and approval controls exist for AI assisted recommendations
- How does the platform produce traceable evidence for AI governance decisions aligned to recognised frameworks such as NIST AI RMF

References:

1. OCEG. What Is GRC?
2. European Commission. NIS2 Directive
3. EUR Lex. Regulation (EU) 2022/2554 (DORA)
4. NIST. AI Risk Management Framework (AI RMF 1.0)
5. The Institute of Internal Auditors. Global Internal Audit Standards
6. EUR Lex. Regulation (EU) 2024/1689 (EU AI Act)
7. Deloitte. Cost of Compliance and Regulatory Productivity
8. Raymond Panko. What We Know About Spreadsheet Errors
9. Powell, Baker, and Lawson. A Critical Review of the Literature on Spreadsheet Errors
10. Forrester. Announcing The Forrester Wave: Governance, Risk, and Compliance Platforms, Q4 2023
11. NIST. AI 600-1: AI Risk Management Framework Generative AI Profile
12. McKinsey. Reaching excellence in software procurement
13. ISACA. Criteria and Methodology for GRC Platform Selection
14. Prosci. The Correlation Between Change Management and Project Success
15. McKinsey. Common pitfalls in transformations
16. COSO. Enterprise Risk Management Guidance
17. ISACA. Integrating KRIs and KPIs for Effective Technology Risk Management
18. The Institute of Internal Auditors. Communicating Results of Internal Audit Services

For more information on how SureCloud can assist your organization, visit us online at **www.surecloud.com**, or email **sales@surecloud.com**

SureCloud Summary

SureCloud Ltd. has two decades of experience as a leading provider of Governance, Risk, and Compliance (GRC) solutions since its founding in 2006. Headquartered in the UK, with offices in the US, SureCloud supports a global portfolio of organisations with its holistic and intelligent GRC platform. Whether addressing cyber risk, data privacy, third parties, or compliance demands, SureCloud has a proven record of empowering organisations to continuously identify, manage and automate their risk and regulatory alignment.

Corporate Headquarters 1 Sherwood Street, London, W1D 7HR