IT Compliance Management Maturity Journey 2026

SURECLOUD®

www.surecloud.com

SURECLOUD®

GDPR Compliant

teiss Awards Winner Best Security Compliance Product

Table of Contents

Highlights	4
1. Executive Summary	5
2. Why Compliance Maturity Matters in 2026	6
3. Model Overview: Four Stages of IT Compliance Maturity	7
4. Capabilities & Indicators by Level	10
5. Practical Actions to Advance Maturity	13
6. Measurement & Outcomes – What Success Looks Like	15
7. Case Scenarios	16
8. Common Pitfalls at Each Maturity Stage	18
9. Conclusion and Next Steps	20
References	21

Highlights

- A **four stage maturity model** for assessing current and target IT compliance capability
- **Practical indicators** across governance, evidence, risk, reporting, workflow, and assurance
- **Evidence based guidance** for advancing compliance maturity in a measurable way

Who should read this?

This guide is designed for CISOs, Heads of IT Risk & Compliance, IT audit leaders, technology risk and control owners, and stakeholders evaluating compliance operating models and supporting tooling decisions.

What this guide helps readers do

This guide helps readers assess current compliance maturity, identify the operating model constraints that are holding progress back, and prioritise the next steps most likely to improve consistency, visibility, and decision usefulness.

Practical next step

Use this guide first to identify the maturity stage that best reflects the current operating model. Then use the capability indicators, practical actions, and self assessment prompts to define the next realistic step forward.

1. Executive Summary

1.1 Why compliance maturity matters more now

IT compliance is becoming harder to manage because the environment around it has changed. PwC's 2025 compliance survey points to growing pressure on visibility, reporting, and response across compliance functions. [4] NIST CSF 2.0 also reflects a broader shift away from isolated control activity and toward governance, profiles, and measurable improvement. [2] NIST's enterprise risk management quick start guide reinforces that direction by treating cybersecurity information as an input to wider enterprise risk decisions rather than a separate reporting stream. [3]

1.2 The real challenge behind compliance pressure

For many organisations, the deeper challenge is not effort alone. It is the maturity of the operating model behind compliance. Controls may exist, policies may be documented, and reviews may happen on schedule, but fragmented evidence, manual workflows, and slow reporting still make compliance difficult to scale. [4] That is why passing an audit can still feel like success even when the wider model is under strain.

This guide treats IT compliance not as a checklist exercise, but as an organisational capability that sits across governance, risk, assurance, and operational execution. The stronger that capability becomes, the easier it is to absorb regulatory change, reduce evidence burden, and give leadership a more reliable view of risk. [3]

1.3 What this maturity model is designed to do

This maturity model sets out four stages of development, defines the capabilities that distinguish them, and shows what progress looks like in practical terms. The aim is to help organisations understand where they are now, what is holding them back, and which next steps are most likely to strengthen compliance performance in a measurable way. [6]

2. Why Compliance Maturity Matters in 2026

2.1 Regulatory and operating pressure are rising together

This conversation feels more urgent now because the regulatory landscape is broader and the pace of change is faster. NIS2 expanded cybersecurity risk management expectations across a wider range of organisations. [8] DORA raised the bar for ICT risk management and operational resilience in financial services. [9] The AI Act added another layer of governance and accountability pressure for organisations using AI systems. [10] The European Commission's implementation timeline also makes clear that the AI Act entered into force on 1 August 2024, is fully applicable from 2 August 2026, and includes some exceptions, including an extended transition period for certain high risk AI systems until 2 August 2027. [21]

Together, these developments reinforce a wider expectation that organisations should not only have controls in place, but also be able to show that governance is effective, responsibilities are clear, and evidence can stand up under scrutiny.

2.2 Manual and fragmented models are harder to sustain

That has practical consequences. Many organisations are still trying to manage modern compliance demands through fragmented processes, duplicated evidence requests, and disconnected reporting. PwC's 2025 compliance survey suggests that stronger use of technology and data improves visibility, response, and reporting in compliance functions. [4] That makes manual and fragmented approaches harder to justify as compliance demands continue to expand.

2.3 Compliance maturity is now part of enterprise risk capability

Compliance maturity also matters because cyber and compliance are no longer easy to separate. NIST's enterprise risk management guidance makes clear that cybersecurity information should feed broader enterprise risk decisions rather than sit in a separate reporting stream. [3] Forrester's 2024 reflections on European cybersecurity point to a broader shift from technical security delivery toward more strategic leadership expectations. [5] In that sense, compliance maturity is no longer a back office concern. It is increasingly part of how organisations manage enterprise risk, absorb change, and maintain confidence in their control environment as expectations continue to rise. [1]

3. Model Overview: Four Stages of IT Compliance Maturity

3.1 Why maturity should be understood as progression

Most organisations do not move from reactive compliance to strategic compliance in one step. They tend to progress in stages. ISACA's capability and maturity guidance supports the idea that organisations move from less consistent and less repeatable activity toward more defined and managed practice, while NIST CSF 2.0 supports a staged view of improvement through its emphasis on current state, target state, and governance driven progress. [7] [2] ISO 27005 reinforces the need for a structured approach to risk management rather than an improvised one. [12]

In practical terms, that progression usually starts with structure. It then moves into greater consistency, lower manual effort, and better visibility. Only after that does compliance information begin to play a more strategic role in prioritisation and decision making. That matters because the goal is not to jump straight to optimisation. The goal is to identify the next credible stage of maturity and build toward it with the right operating model, the right level of standardisation, and the right degree of measurement.

3.2 The four stages

This guide uses four stages:

1. Ad Hoc/Reactive
2. Managed/Operational
3. Integrated & Automated
4. Optimised & Strategic

Each stage reflects a different level of organisational capability. Each also brings different business benefits, different constraints, and different risks if progress stalls.

3.3 At a glance: maturity summary

Stage	Operating reality	Evidence model	Reporting quality	Main risk if stuck
Ad Hoc/Reactive	Work is driven by immediate pressure	Manual and fragmented	Late and incomplete	Effort is mistaken for control
Managed/ Operational	Processes are clearer and more repeatable	More structured, but still manual	More consistent, but limited	Order is mistaken for scalability
Integrated & Automated	Controls, evidence, issues, and risk begin to connect	More reusable and workflow supported	Better visibility and audit readiness	Automation scales confusion if foundations are weak
Optimised & Strategic	Compliance informs prioritisation and decision making	Stable, reliable, and embedded	Decision relevant and trend based	Polished reporting creates false confidence

3.4 Ad Hoc/Reactive

At the first stage, compliance activity is largely shaped by immediate pressure. A request arrives, an audit approaches, an issue escalates, and teams respond. ISACA's maturity guidance supports the view that this kind of inconsistent, person dependent activity reflects a low level of process capability. [7] NIST CSF 2.0 also makes clear that without a defined view of current and target state, improvement remains difficult to manage. [2]

Work gets done, but it is difficult to do consistently and even harder to do efficiently. The organisation depends heavily on individuals, evidence is assembled manually, and there is limited confidence in how complete or current the underlying picture really is. From the outside, this can look like an organisation that is coping. From the inside, it often feels very different. The same evidence is requested multiple times, responsibilities are assumed rather than clearly defined, and reporting arrives late and says less than leadership needs.

Key capabilities at this stage are basic obligation awareness, local control activity, and informal coordination. Typical behaviours include evidence chasing through email, spreadsheet led tracking, local workarounds, and late escalation. The risks of remaining here are clear. Obligations can be missed, assurance becomes disruptive, and resilience depends too much on particular people knowing where things are and what needs to happen next.

3.5 Managed/Operational

The second stage is where organisations begin to create order. Ownership becomes clearer, core processes are documented, review cycles are more predictable, and control activity is easier to explain and repeat. ISACA's capability language is useful here because it distinguishes more repeatable and managed practice from purely reactive activity, while The IIA's risk management guidance points to clearer governance, more systematic assessment, and more consistent oversight as markers of stronger practice. [7] [13]

In practical terms, this is the point where compliance starts to feel less improvised and more manageable. That said, many organisations stay in this stage for a long time because it feels like progress, and in many ways it is. Audits are less chaotic, teams know more clearly what is expected, and standard templates and recurring forums create a greater sense of control. But this stage still comes with a hidden cost. Much of the work remains manual, reporting often relies on coordination across disconnected sources, and evidence overhead can still be high.

Key capabilities include documented processes, named owners, standard templates, routine review cycles, and basic management reporting. Typical behaviours include scheduled testing, structured control reviews, periodic forums, and recurring evidence requests managed in a more orderly way. The main risk of remaining here is that operational discipline gets mistaken for scalability. A managed model can support the business well up to a point. Beyond that point, the manual burden starts to slow everything down.

3.6 Integrated & Automated

The third stage is where maturity becomes much more visible in day to day operations. Controls, evidence, issues, and risk data begin to connect. Repeat activities are supported by clearer workflow, evidence becomes more reusable, and reporting becomes more coherent. NIST's enterprise risk management guidance supports the need to connect control information more clearly to broader risk decisions. [3] ISACA's automated compliance guidance supports a move toward more continuous and design led compliance activity. [14] PwC's 2025 survey also suggests that stronger technology and data use can improve visibility, response, and reporting. [4]

This is often the point where audits and assessments become less disruptive. The practical benefit is not just efficiency, although efficiency matters. It is also confidence. Leaders get a stronger view of control performance, teams spend less time chasing information, and issues can be tracked through to remediation more consistently. What this means in practice is that compliance starts to operate as a joined capability rather than a series of parallel tasks.

Key capabilities include a common compliance taxonomy, connected records, more reusable evidence, structured workflow, and clearer cross functional reporting. Typical behaviours include fewer duplicate evidence requests, stronger audit readiness, more consistent remediation tracking, and better visibility from control issues to business exposure. The risk at this stage is not underinvestment. It is misalignment. If organisations automate before they clarify ownership, taxonomy, and process expectations, they can scale confusion instead of reducing it. [20]

3.7 Optimised & Strategic

At the highest stage, compliance is no longer managed mainly as an assurance burden. It becomes part of how the organisation prioritises, decides, and adapts. Leadership reporting is shorter, clearer, and more decision relevant. Measures are used to assess progress, not just activity. Compliance teams are involved earlier in significant change, and target states are refreshed as conditions evolve. NIST SP 800 55 Volume 2 supports the need for a structured measurement programme rather than isolated indicators. [6] McKinsey's risk and resilience research supports the broader move toward more strategic and decision relevant risk functions. [15]

At this stage, maturity can begin to create more visible strategic value. Compliance effort is more closely aligned to business exposure, reporting helps leadership make choices, and improvement becomes more deliberate and less reactive. In practical terms, compliance stops sitting at the edge of important decisions and starts informing them.

Key capabilities include risk aligned metrics, stronger executive reporting, earlier compliance involvement in change, and a more deliberate target state review cycle. Typical behaviours include concise leadership dashboards, more confident prioritisation, stronger links to enterprise risk, and ongoing refinement of the model. Strategic maturity still needs discipline. Without regular recalibration, even advanced programmes can drift into over confidence or produce polished reporting that is less useful than it appears.

4. Capabilities & Indicators by Level

4.1 Why capability matters more than labels

The stage labels are useful, but they are not the most important part of the model. What matters more is the capability behind them. Two organisations can both describe themselves as operationally sound, yet one may still rely on fragmented evidence, disconnected reporting, and manual coordination, while the other has a more joined up way of working that makes compliance easier to manage and easier to trust. NIST CSF 2.0, ISO 27005, The IIA's risk guidance, and ICO accountability guidance support a more capability based view of governance, risk, and compliance practice. [2] [12] [13] [16]

The real test is whether the operating model is strong enough to support the outcomes the organisation needs. Can governance hold under pressure. Can evidence be produced without disruption. Can compliance information support decisions rather than simply document activity. The capability areas below reflect the themes that standards and professional guidance return to most often.

4.2 Governance and Leadership Accountability

Governance is often where the difference between lower and higher maturity becomes most obvious. At earlier stages, responsibilities may exist on paper, but they are not always clear in day to day operation. Escalation happens late, decisions are pushed into informal conversations, and accountability depends too much on local judgement or individual effort. NIST CSF 2.0 places governance at the front of the framework and makes clear that roles, responsibilities, and oversight are central to cybersecurity outcomes. [2]

As maturity improves, ownership becomes more visible and more consistent. Major controls and obligations have named owners, governance forums become more purposeful, and review activity is more clearly structured. Leadership receives a better quality view of what needs attention and why. ICO guidance on accountability reinforces the need to assign responsibility clearly and to be able to demonstrate governance in practice. [16]

At the strongest level, governance is no longer just about oversight. It begins to support better prioritisation and earlier involvement in business change. The IIA's Three Lines Model supports that progression by distinguishing management action, oversight, and assurance responsibilities more clearly. [17]

4.3 Process Standardisation

Process standardisation is what turns compliance from a collection of local habits into a more reliable operating model. At lower maturity, similar activities are handled in different ways across teams. Reviews happen, but not always on the same cadence or with the same expectations. Evidence is requested differently depending on who asks, and issue handling may depend more on custom and local judgement than on a defined process. ISO 27005 supports a structured approach to risk related activity rather than an improvised one. [12]

As maturity improves, core compliance processes become more repeatable. Review cycles are defined, control activities are easier to explain, and escalation paths are clearer. The organisation becomes less dependent on individual memory and more dependent on shared process. The benefit is not only consistency. It is also predictability. That matters because predictable process is what makes improvement, assurance, and measurement possible at scale.

4.4 Evidence Automation

Evidence handling is one of the clearest practical tests of compliance maturity. At lower maturity, evidence is collected manually, stored in multiple places, and repeatedly requested under time pressure. Teams may know how to respond, but the effort has to be recreated each time. ISACA's guidance on automated compliance supports the move away from reactive evidence collection toward more continuous and design led approaches. [14]

As maturity improves, recurring evidence becomes easier to reuse, collection points become clearer, and the organisation starts to reduce manual chasing for information that should already be available. Over time, evidence automation helps move compliance from periodic scramble to more stable readiness. PwC's 2025 survey suggests that stronger use of technology and data improves visibility, response, and reporting across compliance functions. [4]

At a stronger level of maturity, evidence handling stops being a recurring source of disruption. It becomes part of the normal operating model, with better trust, clearer lineage, and greater readiness for assurance activity.

4.5 Risk Integration

One of the clearest signs of weaker maturity is that compliance and risk still live in separate conversations. Control failures, audit findings, issue status, and business exposure may all be discussed, but not in a way that creates one coherent picture. Teams can be busy and responsible, yet leadership still struggles to understand what matters most and where action should be focused. NIST's enterprise risk management quick start guide makes clear that cybersecurity information should inform wider enterprise risk decisions rather than sit in a separate reporting stream. [3]

As maturity develops, those views start to come together. Compliance issues are easier to interpret through a risk lens, control exceptions are not treated as isolated administrative items, and reporting becomes more useful because it speaks more directly to exposure and consequence. The IIA's risk management guidance supports stronger linkage between governance, risk appetite, and the use of risk information in oversight. [13]

At the highest level, compliance priorities can be linked more deliberately to enterprise risk and tolerance decisions. That is when the function becomes more strategically useful.

4.6 Metrics and Reporting

Reporting is another area where maturity reveals itself quickly. At lower maturity, reporting is often narrow, operational, and assembled late. It may contain a great deal of detail, but still leave leadership unsure about what is improving, what is deteriorating, and where attention is most needed. NIST SP 800 55 Volume 2 supports a structured approach to measurement rather than reliance on isolated indicators or status updates. [6]

As organisations become more mature, reporting becomes more structured and more consistent. Measures begin to show trend movement rather than isolated activity, and leadership gets a clearer view of progress, exposure, and areas that require intervention. At stronger maturity, reporting becomes shorter, clearer, and more decision relevant. The point is not to report more. The point is to report what matters in a way that supports better judgement.

4.7 Tool Enablement and Workflow Orchestration

Tooling only improves maturity when it supports a clearer operating model. At lower maturity, workflow is often held together by email, spreadsheets, local trackers, and manual follow up. That makes repeat activity harder to manage and assurance more disruptive than it needs to be. ISACA's automated compliance guidance supports the idea that workflow and automation deliver more value when they are built into clearer, more preventive operating practices. [14]

As maturity improves, workflow becomes more structured. Reviews, attestations, remediation actions, and approvals are easier to track. The organisation spends less time coordinating compliance activity manually and more time acting on what the information shows. The risk here is easy to miss. Tooling can amplify confusion if ownership, process, and taxonomy are not already clear enough to support it. Forrester's 2025 writing on disconnected systems and weak foundations reinforces that technology alone is a poor substitute for strong process design. [20]

4.8 Assurance and Audit Readiness

Assurance readiness is one of the most visible outcomes of maturity. At lower maturity, audits and assessments create disruption because evidence is hard to find, responsibilities are unclear, and teams have to rebuild the same picture each time. That creates fatigue and makes the organisation look less in control than it may actually be. The IIA's risk management guidance supports the value of more systematic and disciplined approaches to assessment and assurance. [13]

As maturity improves, audits become less chaotic. Evidence is easier to locate, control ownership is clearer, and issues can be tracked more consistently from identification through to remediation. ISACA's guidance on cyber assurance supports stronger readiness through better structure, reporting, and coordination. [18]

At stronger maturity, assurance readiness becomes less of a scramble and more of a by product of normal operating discipline. That is one of the clearest signs that compliance is moving from reactive effort to a more mature capability.

5. Practical Actions to Advance Maturity

5.1 Why practical next steps matter

A maturity model is only useful if it helps organisations decide what to do next. That is why the actions in this guide are framed around stage transitions rather than long lists of generic good practice. Most organisations do not need more theory. They need a clearer view of which next changes will reduce pressure, strengthen consistency, and create better visibility. The most helpful actions are usually the ones that strengthen the operating model first.

5.2 Transition 1: Ad Hoc/Reactive to Managed/Operational

At this stage, the organisation usually does not need a large transformation programme. It needs structure. The first priority is to make accountability visible. Major obligations and controls need clear ownership, escalation routes need to be defined, and core compliance activity needs to be repeatable rather than dependent on local memory or individual workarounds. NIST CSF 2.0 supports the importance of defined governance, roles, and current state understanding as foundations for improvement. [2]

A practical first step is to adopt a documented control framework that gives teams a shared point of reference. ISO 27005 also supports the value of structured risk related processes rather than improvised ones. [12] From there, organisations should standardise the main evidence, review, and issue handling processes. The goal is not to make everything complex. It is to make core activity consistent enough that it can be repeated, measured, and improved. The IIA's risk management guidance points to the value of more systematic oversight and more clearly defined governance responsibilities. [13]

A small operational measurement set is usually enough at this stage. That might include review completion, overdue actions, and the time needed to assemble evidence for a defined request. The real objective is to create the foundations for stronger discipline, not to build a heavy reporting model too early.

5.3 Transition 2: Managed/Operational to Integrated & Automated

Once the basics are in place, the main constraint is usually not a lack of discipline. It is the friction created by duplication, disconnected records, and manual coordination. This is the point where organisations benefit from a more joined up operating model. A common compliance taxonomy helps teams speak the same language, rationalising duplicate records improves trust, and better workflow reduces the effort required to manage repeat activity. PwC's 2025 survey suggests that stronger use of technology and data can improve visibility, response, and reporting in compliance functions. [4]

Automation becomes useful when it is applied to recurring evidence and well understood processes, not as a substitute for clarity. ISACA's automated compliance guidance supports the move toward more continuous and design led compliance activity rather than periodic manual effort. [14] In practical terms, organisations at this stage should focus on centralising key compliance data, reducing duplicate evidence requests, and connecting control activity more clearly to issue and risk records. Workflow should support recurring tasks such as reviews, attestations, approvals, and remediation tracking. The aim is not simply to work faster. It is to reduce friction and improve confidence at the same time.

5.4 Transition 3: Integrated & Automated to Optimised & Strategic

At the more advanced stages, the question changes again. The challenge is no longer just to reduce manual work. It is to make compliance more useful to the business. That means building a more deliberate measurement model, aligning priorities more clearly to business exposure, and improving the decision value of executive reporting. NIST SP 800 55 Volume 2 supports the need for a structured measurement programme that links measures to organisational objectives. [6]

This stage also requires compliance to be involved earlier in important technology, supplier, and change decisions. McKinsey's risk and resilience research supports the broader shift toward more strategic and decision relevant risk functions. [15] In practical terms, organisations should refine leadership reporting so that it highlights trend movement, business significance, and areas that require action. They should also review whether compliance activity is aligned to the areas of greatest exposure rather than distributed evenly across everything. The strongest organisations use compliance information not only to demonstrate control, but also to support better judgement.

6. Measurement & Outcomes – What Success Looks Like

6.1 What a stronger measurement model should show

A stronger compliance model should produce visible operating benefits. It should take less effort to produce evidence, shorten the path to audit readiness, give leadership a clearer view of what matters, and make it easier to connect compliance activity to business exposure and follow through to action. NIST SP 800 55 Volume 2 is especially useful here because it treats measurement as a structured programme rather than a loose collection of metrics. [6]

That matters because maturity can otherwise become too abstract. Organisations may talk about optimisation or automation without being able to show what has materially changed. A stronger measurement approach helps distinguish maturity that looks good on paper from maturity that actually improves the operating model.

6.2 Four groups of useful indicators

The most useful indicators usually fall into four groups. The first group measures efficiency. Examples include the reduction in manual evidence production, the time needed to assemble evidence for a defined audit scope, and the number of duplicate evidence requests avoided. The second group measures execution quality. Examples include remediation timeliness, control review completion, and the proportion of overdue actions. The third group measures visibility and integration. Examples include the frequency and quality of integrated risk reporting, the consistency of control to risk mapping, and the ability to view issues, controls, and exposure together. NIST's enterprise risk management guidance supports the value of connecting control information more clearly to enterprise risk decisions. [3]

The fourth group measures decision value. These indicators show whether reporting is becoming more useful to leadership. Examples include the regularity of executive reporting, the clarity of trend reporting, and the degree to which reporting supports prioritisation rather than simple status tracking.

6.3 Benchmark context and measurement discipline

Public cross industry benchmarks remain uneven in this area. That makes internal baselines and trend measurement more reliable for most organisations than trying to force universal target numbers. PwC's 2025 compliance survey is useful for directional context because it shows where organisations are seeing value from stronger technology and data use in compliance, including visibility, response, and reporting improvements. [4] Deloitte's 2024 Future of Controls benchmarking survey contains data and insights from more than 500 global organisations and identifies common governance, operating model, technology, and monitoring patterns associated with stronger controls maturity. [22]

The practical lesson is simple. Measure what changes the operating experience. If evidence is still hard to produce, readiness is still slow, and leadership still lacks decision useful reporting, maturity has not advanced as far as it may appear.

7. Case Scenarios

7.1 Why composite scenarios are useful

Composite scenarios are useful because they show how maturity works in practice without turning the whitepaper into a product story. The examples below are not based on one organisation. They combine common patterns seen in compliance functions that are trying to move from reactive effort to a more structured and strategic operating model.

7.2 Case Scenario 1: Moving from Managed/Operational to Integrated & Automated

A global manufacturing group has grown through acquisition. It has named control owners, standard policies, and a routine review cycle. On paper, it looks reasonably mature. In practice, evidence still sits in different places, audit requests trigger repeated manual effort, and reporting takes too long to assemble. What this shows is that a degree of control does not automatically mean a high degree of maturity. The organisation has improved discipline, but it has not yet reduced enough friction in the operating model.

PwC's 2025 compliance survey helps explain why that matters. It suggests that stronger use of technology and data improves visibility, response, and reporting in compliance functions. [4] The group responds by simplifying before scaling. It defines a common taxonomy, reduces duplicate records, focuses first on automating repeat evidence in the control areas that create the most recurring effort, and introduces clearer workflow for remediation and attestation. ISACA's automated compliance guidance supports this kind of move toward more continuous and design led compliance activity. [14]

The lesson is straightforward. Stronger maturity does not always begin with a full technology redesign. It often begins with clearer structure, more consistent language, and a better view of where effort is being wasted.

Likely maturity movement: from Managed/Operational to Integrated & Automated.

7.3 Case Scenario 2: Moving from Integrated & Automated to Optimised & Strategic

A financial services firm has already done much of the hard work of operational improvement. Workflow is more structured, evidence is easier to locate, and most reviews can be supported without major disruption. Even so, leadership remains dissatisfied with reporting. There is no shortage of information, but too much of it is operational and not enough of it helps leaders understand changing exposure or make prioritisation choices. That is a common sign that the organisation is approaching the boundary between operational maturity and strategic maturity.

The firm responds by reshaping reporting around business exposure, resilience priorities, and executive decision needs. It also brings compliance into important supplier and technology decisions earlier. DORA reinforces the need for stronger linkage between ICT risk management, resilience, and oversight in financial services. [9] The firm also refreshes its target state using a more formal measurement model. NIST SP 800 55 Volume 2 supports the need for structured measurement that links indicators to organisational objectives and decision making. [6]

The result is not simply more efficient reporting. It is more useful reporting. The organisation becomes better able to connect compliance activity to business significance, which is one of the clearest markers of the most advanced stage. McKinsey's risk and resilience research supports the broader move toward more strategic and decision relevant risk functions. [15]

Likely maturity movement: from Integrated & Automated to Optimised & Strategic.

7.4 What these scenarios show

Both scenarios point to the same underlying lesson. Maturity is not defined by how much activity exists. It is defined by how well the operating model supports control, evidence, visibility, and decision making. That is why maturity improvement should focus less on isolated point fixes and more on the conditions that make compliance scalable, measurable, and useful.

8. Common Pitfalls at Each Maturity Stage

8.1 Why maturity progress often stalls

Every maturity stage has its own traps. Many organisations stay longer than they need to because visible activity can look like progress even when the underlying operating model remains weak.

8.2 Ad Hoc/Reactive

At the earliest stage, the main pitfall is normalising fire fighting. Teams become very good at responding under pressure. Requests get answered, audits are survived, and issues are handled as they arise. But that responsiveness can hide the fact that the underlying model is still fragile. ISACA's maturity guidance helps explain this problem because it distinguishes reactive effort from more consistent and repeatable capability, and NIST CSF 2.0 reinforces the need for defined governance, clear roles, and a clearer view of current state. [7] [2]

The risk is not simply inefficiency. It is that the organisation confuses effort with control.

8.3 Managed/Operational

At the managed stage, the most common pitfall is assuming that documentation equals maturity. Processes are clearer, templates exist, and review cycles are more predictable. That is real progress. But it does not automatically solve duplication, fragmentation, or weak visibility. The IIA's risk management guidance supports the idea that stronger practice depends not only on formal structure, but also on how consistently risk information is used and acted on. [13] PwC's 2025 survey also suggests that stronger use of technology and data improves visibility and reporting, which implies that manually coordinated models still carry significant limits. [4]

The risk at this stage is that organisations mistake better order for real scalability.

8.4 Integrated & Automated

At the integrated stage, the biggest risk is over relying on tooling before the operating model is fully aligned. Automation, workflow, and shared systems are all valuable. But they only improve maturity when ownership, process, and data logic are already clear enough to support them. ISACA's automated compliance guidance supports the move toward more continuous and design led compliance, not automation for its own sake. [14] Forrester's 2025 writing on disconnected systems and weak foundations makes a similar point. Technology does not solve weak process design on its own. [20]

The risk here is subtle. Organisations can accelerate confusion instead of reducing it.

8.5 Optimised & Strategic

At the most advanced stage, the danger shifts again. Reporting can become polished without becoming more useful. Dashboards can look mature while still doing too little to support prioritisation or resource allocation. NIST SP 800 55 Volume 2 is a useful guardrail here because it emphasises measurement discipline, relevance, and alignment to organisational objectives. [6]

The risk at this stage is not lack of information. It is false confidence.

8.6 Cross stage pitfalls

Some blockers show up at every stage. One is leadership sponsorship. McKinsey's risk and resilience research supports the broader point that risk related functions become more effective when leadership engagement is stronger and more strategic. [15] Another is fragmented records and inconsistent data. Gartner's public material on data quality reinforces the importance of shared responsibility, trusted datasets, and disciplined data management. [11] Tool sprawl is another recurring problem. ISACA's 2025 guidance on tool sprawl highlights how too many disconnected tools can make security and compliance environments harder to manage rather than easier. [19]

The practical lesson is simple. Maturity programmes tend to stall when organisations try to scale activity before they strengthen the conditions that make activity reliable.

9. Conclusion and Next Steps

9.1 Why maturity matters

The case for stronger compliance maturity in 2026 is clear. Regulatory expectations are broader, cyber and operational risks are more closely connected, and assurance pressure continues to rise. NIS2, DORA, and the AI Act all reinforce the need for stronger governance, clearer accountability, and more reliable evidence. [8] [9] [10]

What matters now is whether the organisation can respond with an operating model that is structured, repeatable, and decision useful. That is why maturity matters. It helps organisations move the conversation away from pressure, backlog, and fragmented activity. It shifts the focus toward capability, progression, and measurable improvement.

9.2 How to self assess

For most organisations, the next step is not to aim for a fully optimised end state all at once. It is to understand the current state more honestly, identify the constraints creating the most friction, and target the next stage of maturity with practical intent. NIST CSF 2.0 supports that kind of progression by focusing on current state, target state, and governed improvement rather than one time transformation. [2]

A practical self assessment does not need to be complicated. It should begin with a small number of questions that reveal whether the operating model is strong enough to support compliance at scale.

- Can the organisation describe its current compliance state in a way that is consistent across teams
- Are ownership, evidence, and review responsibilities clear enough to hold up under pressure
- Can audits and assessments be supported without repeated disruption
- Is reporting good enough to support prioritisation rather than just status tracking
- Are compliance activities linked clearly enough to business exposure and enterprise risk

9.3 What to do next

The most useful next step is to identify the stage the organisation is in today and focus on the next realistic move forward. For some, that means creating clearer ownership and more repeatable process. For others, it means reducing evidence friction, improving workflow, and connecting compliance activity more clearly to risk. For more advanced organisations, it means strengthening measurement and making reporting more useful to leadership.

The point is not to make compliance look more mature. The point is to make it work better.

9.4 Neutral next steps

- ✔ Download our self assessment template.
- ✔ Contact SureCloud for a maturity workshop.

References

1. **Gartner.** Survey Shows Unsettled Regulatory and Legal Environment Tops Emerging Risks for First Quarter of 2025.
2. **National Institute of Standards and Technology.** The NIST Cybersecurity Framework (CSF) 2.0.
3. **National Institute of Standards and Technology.** NIST Cybersecurity Framework 2.0: Enterprise Risk Management Quick Start Guide.
4. **PwC.** PwC's Global Compliance Survey 2025.
5. **Forrester.** European Cybersecurity Reflections, 2024.
6. **National Institute of Standards and Technology.** NIST SP 800 55 Volume 2: Measurement Guide for Information Security.
7. **ISACA.** Effective Capability and Maturity Assessment Using COBIT 2019.
8. **EUR Lex.** Cybersecurity of Network and Information Systems. Summary of Directive (EU) 2022/2555.
9. **EUR Lex.** Digital Operational Resilience for the Financial Sector.
10. **European Union.** Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence.
11. **Gartner.** Data Quality: Why It Matters and How to Achieve It.
12. **ISO.** ISO/IEC 27005:2022 Information Security, Cybersecurity and Privacy Protection — Guidance on Managing Information Security Risks.
13. **The Institute of Internal Auditors.** Assessing the Risk Management Process, Second Edition.
14. **ISACA.** A Proactive, Continuous Approach to Automated Compliance.
15. **McKinsey & Company.** McKinsey on Risk & Resilience, Number 17.
16. **Information Commissioner's Office.** What Are the Accountability and Governance Implications of AI?
17. **The Institute of Internal Auditors.** The IIA's Three Lines Model: An Update of the Three Lines of Defense.
18. **ISACA.** Proven Strategies to Boost the Effectiveness of Your Cyber Assurance Function.
19. **ISACA.** Tool Sprawl: Why More Cyber Tools Make You Less Secure.
20. **Forrester.** Build Your Foundation First: The Hard Truth About Successful AI Deployments.
21. **European Commission.** AI Act.
22. **Deloitte.** Becoming control intelligent through the future of controls.

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