Advancing your risk management maturity

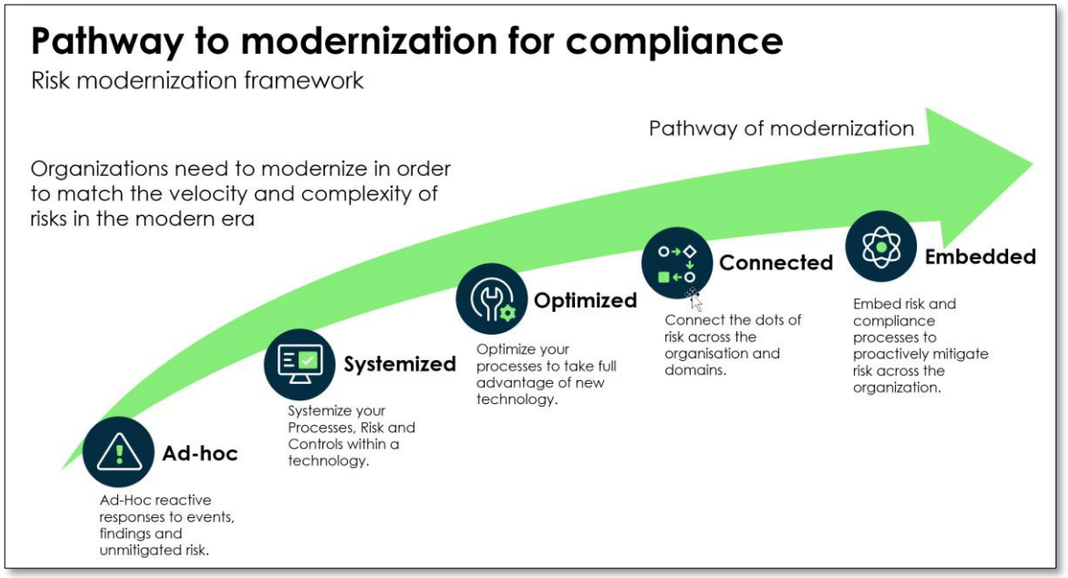
A roadmap to effective governance and increased resilience

servicenow

Introduction: a marathon not a sprint

Organizations begin to think about risk and compliance for many different reasons. Whatever your reason, taking a phased approach to growing your risk and compliance maturity is critical. If you just visualize the end state and try to get there in one step, it's like running a marathon without any previous training. You're going to fail, and there's a good chance you're going to hurt yourself. On the other hand, if you move forward in discrete steps, you build organizational capabilities that propel you from stage to stage—increasing your chances of success and accelerating time to value by realizing benefits throughout your risk and compliance journey.

In this ebook, we look at five key stages of risk and compliance maturity and provide guidance on how you can move from one stage to the next.



Reasons organizations embark on a risk or compliance journey

- Government entities and companies in highly regulated industries such as financial services or healthcare often face an ever-expanding set of regulations and standards they need to comply with.
- Other organizations want to improve their operational risk, security, or privacy posture by adopting common frameworks such as Basel III, GDPR, ISO, NIST, or CIS.
- The pandemic has made black swan events a reality, many organizations have reacted by ramping up their risk management capabilities.
- Those embarking on digital transformation initiatives—such as moving to the cloud or digitizing critical processes—realize that they face increased risks due to potential breaches or human error.

Stage 1: Ad hoc processes

This is the starting point for many organizations. You spend most of your time reacting to new risks and audit findings when they're reported. You track risks and compliance posture using spreadsheets, and your processes are fueled by emails. This means you have poor risk visibility and can't anticipate risks, let alone respond quickly and effectively. That leaves your business exposed, even though you're spending an increasing amount of time and resources trying to keep up.

What to do

- Develop an executive champion for risk and compliance. This sets the stage for success by building support and a common language across executive stakeholders, frontline employees, and your board.
- Identify the key regulations and risk frameworks you have to comply with.
- Pick one of these regulations or frameworks to start your journey. Don't try to tackle everything at once. Document your existing processes and policies in this area.
- Many organizations start with Sarbanes-Oxley (SOX), while others that have data privacy concerns focus on GDPR. On the other hand, if your overriding issue is your operational risk posture consider picking Basel III or for security, look at ISO, CIS, or NIST.
- Identify critical services that are vital to the success of your business, these will need business continuity and disaster recovery plans.

servicenow

Stage 2: Systemized

You now have a baseline understanding of one key regulation or framework, along with your current policies and processes. It's time to start systemizing how you manage risk and compliance for this regulation or framework.

What to do

- Look for accelerators or content packs for your chosen regulation or framework and use this to kickstart your implementation. You'll get up and running faster and avoid unexpected pitfalls.
- Plan your risk and compliance management processes. Use the processes you've already documented as a starting point, but don't just replicate them. Existing processes are typically inefficient and have gaps, so now's your opportunity to streamline them and make them more effective.
- Identify your risk universe by examining areas with high strategic importance or compliance mandates. Use this to build a risk register so you can track issues related to these risks in your risk management system. If you're managing operational risk, now's also the time to think about capturing your risk appetite. At this point, also define the controls you need to support your chosen regulation or framework.
- Assign risk and compliance owners in your risk management system so you can respond to issues quickly. If a risk or control is related to a specific asset, identify the appropriate asset owner as well.
- Define your auditable units (the processes, business entities, and so on that you want to audit), along with your engagement and test plans. These auditable units should line up with your chosen regulation or framework, as well as the controls and control owners you've identified.
- Put your top 15 to 20 assets, services, applications, and vendors into the your CMDB. This acts as an "anchor point" for risk and compliance data, providing context that lets your risk management system automatically calculate the impact of risks so you can prioritize the actions you take. It also lays the groundwork for integrating risk and compliance directly into the operational processes of your system.

Plans should include your extended enterprise and building business resilience

- Identify the vendors and other third parties that are relevant to your chosen regulation or framework. Populate these in your vendor catalog so you can later manage third-party risks holistically alongside other risks.
- Create your select continuity and recovery plans and establish a schedule for testing and updating.

Put your top 15 to 20 assets, services, applications, and vendors into your CMDB. This acts as an "anchor point" for risk and compliance data, providing context that lets your risk management system automatically calculate the impact of risks so you can prioritize the actions you take.

servicenow

Grow your third-party risk program to further support your extended enterprise

Use your risk management system to implement formal onboarding and contract management practices for third parties. This will reduce risk and allow you to embed these relationships into your overall risk and compliance program at a later stage

Now is the time to build on this foundation, implementing additional regulations or frameworks and starting to bring your frontline employees onboard.

Stage 3: Optimized

At this point, you're on your way to having a formalized program with processes and actions in place to improve your risk and compliance stance. You've identified controls for one regulation or framework. You've also identified the risks, have the most important assets, services, applications, and vendors in your CMDB, and have plans to protect your business from disruptive events.

Now is the time to build on this foundation, implementing additional regulations or frameworks and starting to bring your frontline employees on board.

What to do

- Start with other regulations or frameworks that you've identified on your key priority list. Also look for other departments or functional groups that need risk or compliance management, as well as companywide policies you want to manage.
- When supporting a new regulation or framework, identify relevant controls you've already defined and reuse these rather than creating new ones. This reduces initial implementation effort as well as ongoing testing effort. Your risk management system should make it easy to reuse controls. Also look at how you can reuse audit evidence rather than collecting the same evidence multiple times.
- Make it easy for frontline employees to carry out basic tasks such as performing policy acknowledgements or creating exceptions in an employee portal. This lets you fit risk and compliance into the way they already work, increasing acceptance and adoption.
- Map risks to controls. This allows you to easily create issues for noncompliant controls and also lets you to use risk data to decide where to focus your internal audits. Select a few controls where it is easy to automate control testing to put you on the road to continuous controls monitoring.
- Institute an automated policy exception process so you control when exceptions are granted and can track these for audit purposes. This also allows you to set time limits on policy exceptions where appropriate, so you revisit exceptions rather than letting them continue forever.
- If you're managing operational risk, ensure that you're tracking risk events and losses in your risk management system. Also use the tool to provide regular operational risk reports to leadership by rolling up risk data.
- To increase efficiency, analyze how well you're managing issues. Also group similar issues to avoid duplication. Your risk management system should allow you to do both.

servicenow

Stage 4: Connected

Congratulations! You're well on your way to risk and compliance maturity. It's time to take the next step by looking at risks more holistically across your business and automating repetitive and redundant processes. Providing effective oversight of risk processes also becomes more valuable at this stage. For example, think about how quickly you can identify and address issues such as a software vulnerability that hasn't been addressed within an established SLA period, a failed financial control that will lead to regulatory noncompliance, or a new critical service without a continuity plan.

What to do

- Improve your risk and compliance stance by detecting and responding to issues faster. Establish measurable key risk indicators (KRIs) and key compliance indicators (KRIs) in your risk management system so you can model and predict risk and increase visibility by using the platform to schedule quarterly control attestations. Automate issue generation—for instance, when a control isn't compliant—and start to build automated cross-functional workflows on a single platform to orchestrate your responses to issues.

- Simplify external audits by giving auditors read-only access to your risk management system so they can view controls and associated evidence. This reduces the number of questions for control owners and internal audit teams.

- Proactively plan for regulatory changes by integrating feeds that give you visibility of the regulatory horizon.

- Further engage frontline employees by making it easy to create compliance cases or risk events using your employee portal. Build in privacy, security, and compliance by design so employees proactively engage with risk and compliance teams.

- Kick off scenario planning and analysis to help predict where the gaps or weaknesses may lie in your continuity or recovery plans.

Create connections into your extended enterprise

Leverage your risk management system to integrate third-party risks into your overall risk and compliance program. Schedule recurring third-party assessments, using the third party's tier to determine the frequency. Ensure these assessments look at all key risk areas, including security, financial, operational, ESG, and others. Augment these assessments by integrating objective risk intelligence feeds from BitSight, Interos, and other providers into your risk management system . Extend coverage to fourth parties and beyond wherever possible. Define controls and risks to manage third-party failures—such as failures to return assessments or follow mandatory policies—and tie these to your overall enterprise risks.

Embed risk and compliance into everyday workflows

- Leverage audit integration with your project portfolio management system to track projects, resources, costs, and timesheets.
- Integrate compliance management into your development processes using your DevOps program, enforcing policies such as requiring test results and detecting code and configuration noncompliance.
- Reduce risk and increase compliance in your HR services by ensuring policies are acknowledged through integration with your HR service delivery system.
- Better manage risks due to software vulnerabilities by easily creating risk events in a vulnerability response tool

servicenow

Stage 5: Embedded

At this point in your journey to maturity, you're integrating risk management and compliance into everyday workflows and familiar user experiences. This allows you to proactively manage risk across your enterprise. Your leadership should also be actively monitoring risk across your organization. Ideally, you should have a single platform and data repository that not only houses the most current information but also provides this information in real time to frontline employees, risk and compliance teams, and internal audit to streamline operations. And by integrating with third-party tools, you're continually feeding this single source of truth with new insights.

Now you're ready to achieve full maturity by proactively monitoring and responding to risks, and by leveraging out-of-the-box integrations with other applications that run on a single platform

What to do

- Implement continuous risk and control monitoring to provide a real-time view of issues as they emerge. Your risk management system should allow you to automatically do this by tracking evolving operational data housed in the platform as well as data it collects from other systems. You can also dynamically update risk scores by automating the collection of data for risk assessments.
- Now that you have real-time visibility, you can also use dynamically calculated KRI and KCIs to proactively notify risk owners of potential problems before an incident occurs.
- Make use of virtual chatbots and mobile interfaces to increase frontline employee engagement and give risk and control owners access to risk and compliance information and capabilities anytime and anywhere.
- Automate processes using AI/ML in the form of bots to fill in forms or collect information to drive efficiencies
- Create rules to identify if risk intelligence scores for your third parties deviate by a percentage from established thresholds and automate responses.

servicenow

Conclusion: prepare for the marathon

Every organization has unique needs and approaches risk and compliance in its own way. Don't expect your journey to look like that of your peers. However, successful journeys share common characteristics: sufficient time for upfront planning, a well-thought-out roadmap, executive sponsorship, a risk-conscious culture, and a common language to define and measure risk. And while some organizations tackle risk and compliance on their own, most seek out a trusted partner, whether that's ServiceNow Expert Services or an experienced implementation partner.

If you set realistic expectations and take a phased approach to growing your risk and compliance maturity—rather than setting out on a marathon unprepared—you'll maximize your chances of success and increase the benefits you realize.

Want proof?

Here are some typical benefits of transforming risk and compliance with solutions from ServiceNow:

22%

faster risk identification[1]

40%

less time responding to risks[1]

70%

faster risk and compliance reporting[1]

40%

reduction in annual penalty payments from failed audit findings[1]

Minutes not months

to report compliance[2]

50%

reduction in time by automating control testing[3]

To find out more about ServiceNow risk and resilience products, visit us at www.servicenow.com/resilience

Ready to start your journey to risk and compliance maturity?

Ebook: 5 stages of security automation maturity

Webinar: Transforming IT and finance processes with RPA

Ebook: Operationalizing the ESG business imperative

References:

1. Forrester Total Economic Impact™ (TEI) of ServiceNow—Validated Financial Model Data, a commissioned study conducted by Forrester Consulting on behalf of ServiceNow, February 2022
2. Avanade case study
3. ServiceNow case study

About ServiceNow

ServiceNow (NYSE: NOW) makes the world work better for everyone. Our cloud-based platform and solutions help digitize and unify organizations so that they can find smarter, faster, better ways to make work flow. So employees and customers can be more connected, more innovative, and more agile. And we can all create the future we imagine. The world works with ServiceNow™. For more information, visit: www.servicenow.com.