Risk and resilience

Risk management and resilience are critical success factors for businesses navigating business uncertainty. Managing risk and resilience in real time is the continuous, proactive process of understanding, identifying risk and opportunities, implementing action plans, and monitoring those plans.

Proactively manage technology and cyber risks and compliance

- Efficiently manage technology risk and compliance through integration and automation across silos.
- Continuously monitor and intelligently respond to evolving cyber risk.
- Understand and manage privacy and data loss risks.

Effectively manage and report on enterprisewide risks and compliance

- Integrate, manage, and monitor operational and enterprise risk.
- Manage and report on corporate compliance and regulatory changes.
- Perform internal audits with high-quality data.

Maintain business continuity and operational resilience

- Build, test, and execute effective business continuity plans informed by business, IT, and external context.
- Mitigate potential IT disasters and disruptions and recover effectively to protect the business.
- Integrate, monitor, and manage operational resilience activities enterprisewide.

Manage third-party and supplier risk

- Reduce digital supply-chain risk as you digitally transform.
- Efficiently assess and manage third-party and supply chain risks.

servicenow

For more, visit the ServiceNow Customer Success Center

Mobilize your ESG strategy

Develop and document formal ESG strategies and workflows. Take these actions to prepare your organization to deliver and support this capability:

Prepare for integrated risk management.

- **Reinforce expectations for collaboration across silos.** ServiceNow provides the enterprise a single place to collect and analyzes risk information and then manage and automate remediation and reporting. Align incentives and workflows across the two functions to ensure they take advantage of these new capabilities.
- **Ensure the accuracy of IT and business information.** Your teams will need accurate configuration items (CIs) in the ServiceNow CMDB to add business context to risks. Similarly, make sure foundational data like organizational structure and user roles are up to date so automated workflows involve the correct people.
- **Consider how to communicate impact.** Everyone in the enterprise is responsible for keeping the organization secure, but business leaders are unlikely to fully understand how technology, cyber, and privacy risks impact them. Business-relevant risk dashboards will ensure impact is understood.

Develop plans for automation and continuous monitoring.

- **Improve vulnerability management processes to enable faster workflows and automation.** ServiceNow lets you to streamline how to assign and manage vulnerability remediation. Make sure to define and document processes for how to assign ownership of remediation and your process for requesting and approving exceptions. Look for opportunities to improve your processes to take advantage of greater data integration and automated workflows.
- **Map out processes for continuous monitoring of cyber risks.** Define roles and responsibilities between risk, security, and IT for identifying risks, surfacing vulnerabilities, patching vulnerabilities, and verifying that risks are resolved. Understand handoffs between teams.

Strive for privacy by design.

- **Incorporate privacy safeguards as early as possible into your product development lifecycle.** Determine when your employees can—and should—access data, and implement controls at that point.
- **Create forward-looking privacy policies and controls.** With the regulatory landscape changing so quickly, it's not efficient—or even possible—to manually change privacy controls in response. Create a simple, intuitive, and automated system for data privacy controls.

Effectively manage and report on enterprisewide risk and compliance

Modernize governance, risk, and compliance in support of digital transformation. Take these actions to prepare your organization to deliver and support this capability:

Prepare to standardize and integrate disparate risk, governance, and compliance processes.	• **Inventory and review risk management processes across your enterprise. It is likely many risk management processes currently operate in siloes.** Prepare to standardize and integrate these processes by understanding the different processes for risk assessments, reporting, and policy exceptions. • **Plan how to manage change and get stakeholder buy-in.** As you standardize into a single integrated risk framework, have plan to ensure adoption of new enterprise-wide processes. • **Build a solid foundation for the risk management program.** There should be strong executive sponsorship, a shared understanding of risk across your enterprise, and clarity on the goals of your risk management program with specific objectives and goals.
Rationalize and consolidate your controls.	• **Update the organizations' controls.** Make sure every control supports your business objectives, that the control is effective, and confirm there isn't another control option that would be more effective, simpler, or more efficient. Aim for a holistic view but, if this is too resource intensive, focus on controls for your highest-risk and most critical business process. • **Unify the enterprise control framework.** Regulatory frameworks (e.g., SOX, HIPAA, GDPR, and PCI) have common, repeated controls. Don't maintain independent sets of the controls. Consolidate controls across multiple frameworks into a single set of controls to simplify control management and testing.
Refresh your policies.	• **Normalize and consolidate your policies before your IRM implementation.** A good integrated risk management (IRM) program is defined by the requirements established in your organization's policies. Also take the opportunity to make sure your policies are written in plain language that everyone can understand.
Help your audit team maximize the value of high-quality data.	• **Invest in data and analytics training for your audit staff.** Help the entire team understand and "speak data as a common language," including audit leadership. • **Update audit planning processes to take advantage of real-time data.** Consider using risk information to make real-time audit plan changes and design a planning process that builds in flexibility to respond to new risk information in the moment.

For more, visit the ServiceNow Customer Success Center

servicenow

Maintain business continuity and operational resilience

Take these actions to prepare your organization to deliver and support your organization's ability to detect, prevent, respond to, recover, and learn from operational disruptions:

Assess your entire lifecycle of resilience—from business impact analysis to crisis response and recovery.

- **Expand plans beyond technology.** Resilience and business continuity plans are often overly focused on systems and tools. Make sure your plans cover not just technology but the suppliers, facilities, and people required to support critical business services.
- **Assess your crisis management plans.** Clearly define the roles and responsibilities assigned to named individuals. You should also have a system and documented processes for communicating and making decisions in the event that your regular lines of communication go down.

Plan to test your business continuity and crisis management plans.

- **Conduct scenario exercises to prepare for a crisis.** Exercises help employees know what needs to be done during a crisis and help identify flaws or gaps in your plans.

Expand your plans for digital transformation to build resilience.

- **Invest in IT modernization.** "Resilience leaders" report that digital technology and solutions are crucial for driving resilience. These investments include workflow automation, data management systems, mobile, machine learning and AI, and real-time risk analysis, cybersecurity, and predictive analytics.

Invest in a culture of resilience.

- **Consider a chief resilience officer role.** For most large organizations, resilience is either the responsibility of the chief risk officer or is made a shared responsibility of the CIO, CHRO, and COO. A dedicated role for resilience provides the the remit and resources to focus on resilience as an enterprisewide priority.
- **Assign business ownership for resilience risks.** A successful resilience posture requires clear lines of authority and clarity about who owns the risk. Business processes are the main priority of operational resilience, so the owners of those processes, not IT, should be the primary decision-makers.
- **Evaluate the business case for hiring resilience specialists.** To bolster their resilience, organizations are hiring specialists in business continuity, disaster recovery, crisis management physical security, and operational risk management. Some organizations are taking it a step further, filling nontraditional roles like auxiliary or remote teams that can respond immediately to emergencies to prevent disruption.

Manage third-party and supplier risk

Formalize vendor risk management, informed by the business context and real-time data and analytics. Take these actions to prepare your organization to deliver and support this capability:

Put vendor risk in context.

- **Align vendor risk reporting to business processes to give stakeholders visibility into potential business disruptions.** Identify the information business leaders who will need to make decisions when managing vendor risks.
- **Incorporate vendor risk information into business resiliency planning.** Your organization's supply chain is a critical element in its ability to run the business. Identify the vendors that are mission critical and make sure the enterprise has a Plan B for the goods and services they provide.

Determine the vendors to manage with ServiceNow.

- **Identify vendors and gather vendor information.** Vendor information can be siloed in different parts of the enterprise, organized in different formats. Make sure there's an owner for each vendor relationship who can provide all the information you'll need to assess the risk.

Plan how you'll use vendor information to improve risk management.

- **Establish vendor tiering criteria.** Classifying vendors by tiers gives you the opportunity to adjust your processes and focus based on the vendor's risk and/or criticality. For example, mission-critical vendors might require far more detailed questionnaires than would be worth the time for low-risk relationships. Tiering criteria typically looks at the business processes and data impacted by the vendor to determine risk and business criticality.
- **Develop early warning signs of vendor risk.** Correlate the responses to vendors' due diligence questions to past incidents and industry data so you can identify the questions and responses that most represent higher risk.

Practitioner insight

Don't make your scope so large that it's difficult to manage. You don't need to include every single vendor. Create a threshold based on the amount you spend with the vendor and the business criticality of the processes the vendor supports. This helps you objectively prioritize which vendors to include, and you can exclude low-risk vendors from your initial implementation.