ServiceNow
Governance, Risk, and Compliance

The business and IT challenge

Managing risk and compliance with a manual, siloed and reactive work model is no longer effective as the global regulatory environment continuous to evolve, forcing changes across your organization. Changes driven by the need to: adopt new business models, establish new partner relationships, deploy new technologies, and address the increasing number of threats and cyber risks. Many enterprises have discovered that without an integrated view of risk it is virtually impossible to quickly assess the impact on their existing compliance obligations and risk posture of these changes.

Respond to business risks in real-time with ServiceNow

ServiceNow Governance, Risk, and Compliance (GRC) helps transform inefficient processes across your extended enterprise into an integrated risk program. Through continuous monitoring and automation ServiceNow delivers a real-time view of compliance and risk, improves decision making, and increases performance across your organization and with vendors. Only ServiceNow can connect the business, security, and IT with an integrated risk framework that transforms manual, siloed, and inefficient processes into a unified program built on a single platform.

- **Risk management** - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise, and respond to critical changes in risk posture

- **Policy and compliance management** - Automate best practice lifecycles, unify compliance processes, and provide assurances around their effectiveness

- **Audit management** - Scope and prioritize audit engagements using risk data and profile information to eliminate recurring audit findings, enhance audit assurance, and optimize resources around internal audits

- **Vendor risk management** - Institute a standardized and transparent process to manage the lifecycle for risks assessments, due diligence, and risk response with business partners and vendors

Risk

Compliance

Audit

Vendor

Identify risks in real-time

Configure real-time business and IT service performance data, and identify vendor requirements to enable automated controls testing. Define thresholds as indicators for continuous monitoring of your extended enterprise

Increase performance

The Now platform CMDB, process designer, service mapping, and consistent and cross-functional workflow automation simplifies GRC processes and eliminates errors

Optimize internal audit productivity

Use of risk data and issues management enables effective audit project scoping, planning, and reporting while optimizing internal audit and compliance resources

Improve strategic planning and decision making

Fine-grained business impact analysis, task management, and contextual alignment with the CMDB on a single platform provides cross-functional visibility to identify, prioritize, and appropriately respond to risks

Automate third-party risk

Formalized vendor risk assessment and tiering process, improved visibility, and transparency save time and reduce vendor risk.

Extend your Servicenow investment

The single platform of engagement offers orchestration, easy integration, and data ingest and publication capabilities

GRC use cases

Compressing the time to identify, prioritize, and respond to changes in your risk and compliance posture is imperative. To do so you need to continuously monitor data across your extended enterprise to speed detection of emerging risks. Automating the appropriate remediation and risk treatment actions across business and IT processes breaks down the silos and ensures a rapid response.

The Now platform collaboration engine and issues management capabilities work across GRC applications and with the Vendor Portal to create a shared understanding and facilitate timely decisions.

Define a governance framework and test compliance controls

ServiceNow GRC helps manage your governance framework, including policies, laws and regulations, and best practices in one system, and maps them to controls. Once defined, you can automate repetitive processes, even across functional groups.

Through ServiceNow GRC you can identify relevant business, risk and IT owners, and systems, and automate the manual cross-functional processes for policy lifecycle management and compliance testing to identify non-compliant controls, respond to issues, or effectively scope a GRC engagement. The unique capabilities of our platform eliminate errors and inefficiencies associated with emails, phone calls, and in-person meetings.

Additionally, using the built-in GRC Attestation Designer, you can create and execute tests and attestations that are specific to a policy statement. This eliminates errors during evidence

data collection and mitigates the need to manually reconcile test results and metrics.

Create a risk register and automate risk assessments

ServiceNow GRC helps identify and manage risks in a single register. Self-assessments can be scheduled to collect information about existing and emerging risks, and the accuracy of controls.

GRC combines asset and process-centric risk methodologies to determine qualitative and quantitative risk scores, which are informed by service performance data with the business impact derived from the configuration management database (CMDB). This allows you to accurately gauge your risk exposure in real time. There is a consistent process for automatically creating and responding to issues, reducing remediation time from weeks to only minutes.

Implement real-time monitoring

ServiceNow GRC identifies non-compliant controls, monitors high-risk areas, and manages the Key Risk Indicator (KRI) and Key Performance Indicator (KPI) library with automated data validation and evidence gathering.

To complement existing GRC capabilities, we provide out-of-the-box integration with Performance Analytics (PA) for GRC, which uses PA indicators and thresholds as another means to detect failing critical controls between assessments.

Interactive real-time dashboards provide overviews of your risk and compliance posture and audit activities. The role-based dashboards in the GRC Workbench allow you to view status updates, priorities, and tasks associated with GRC engagements. Dependency

modeling uses CMDB information to show upstream and downstream relationships across entities, so you can visualize the business impact of a control failure throughout the enterprise.

Assess vendor risk

ServiceNow GRC provides the ability to more easily manage and assess vendors, saving time and reducing vendor risk.

Portfolio management capabilities allow you to consolidate vendors into a single vendor catalog. Through the assessment designer and built-in questionnaires, you can more easily monitor vendors and obtain better quality data, to more accurately track changes over time.

The first step in a vendor risk management program is to appropriately tier your vendors. A formal tiering process, including tiering assessments and automatically generated tiering scores help you categorize vendors into levels or tiers. Expand the knowledge of the risk posed by your vendors through integration with third-party security score provides, allowing you to adjust vendor tier scores.

Vendors risk is based on risk scores, which are dynamically generated based on vendor questionnaires, updated in real time, and stored in the vendor catalog.

The vendor portal consolidates communication and enables collaboration with your vendor and between your vendor and their response team—replacing email and phone calls. Scheduled assessments and automated notifications and escalations ensure you stay on top of activities.

Learn more at

www.servicenow.com/risk

servicenow.