INRY

# Five Use Cases For ServiceNow GRC

Governance, Risk and Compliance (GRC) is an important area of focus for several organizations. Companies want a robust GRC program in place to help manage compliance with regulations and internal policies; enhance information security practices and streamline audits and remediation activities.

If you are considering ServiceNow® as a potential tool for GRC and are researching its capabilities, you may have a few questions about the various ways in which the tool can be used. While our clients typically start with compliance management, they like to consider risk management and audit as well. However, most clients are surprised that they can leverage ServiceNow GRC for Vendor Risk Assessments and Business Continuity Planning / Disaster Recovery (BCP/DR). In this Perspectives article, we will describe how ServiceNow GRC can be leveraged to address all these common GRC use cases.

## Use Case #1:

### Compliance Management

## Use Case #2:

### IT Risk Management

## Use Case #3:

### Audit Management

## Use Case #4:

### Vendor Risk Management

## Use Case #5:

### Business Continuity Planning / Disaster Recovery

### Monitoring & Reporting Compliance against Regulations, control frameworks and internal policies

ServiceNow integrates with Unified Compliance Framework (UCF) and acts as a **central repository for all your authority documents**, whether they are regulations like SOX or PCI; industry frameworks like COBIT; or internal policies, standards and standard operating procedures.

This makes it easier to support and maintain publicly available control frameworks; manage the lifecycle of your internal policies, procedures and standard operating procedures; and enable alerts and notifications for periodic reviews of content. By creating relationships between multiple regulatory frameworks, internal controls, and policies you can take advantage of a "Test Once, Comply Many" philosophy.

The biggest differentiator between ServiceNow and other tools in the marketplace is its ability to **automate evidence collection**. It does this through automated control testing, attestations, surveys, data certification, and support policy exception processes. By integrating Compliance Management with Service Management, you can embed your IT general controls into IT service management activities within your organization.

ServiceNow's Risk Management application has evolved significantly over prior versions. It assists in the continuous monitoring of risks that can negatively impact business operations; and it provides structured workflows for the management of risk assessments, risk indicators, and risk issues.

ServiceNow's Risk Management application provides ways to organize categories of risks to normalize risk scores across the organization; consistently assess risks using a best practice workflows; and reports on financial and statistical impacts of risk to the organization.

There are two built-in risk scoring methods - qualitative (Impact / Likelihood) or quantitative: Single Loss Expectancy (SLE), Annualized Rate of Occurrence (ARO) and Annualized Loss Expectancy (ALE). Depending on the maturity of your current risk management practices and the availability of metrics and data, you can choose either method for scoring.

Risks can also be integrated with compliance management. For more information regarding Integrhythm's Risk Management implementation approach using ServiceNow GRC, please read our whitepaper, "Perspectives: Six Steps to Risk Management Implementation Using ServiceNow GRC" or contact us at info@inry.com

ServiceNow GRC application can be used by internal audit teams to document and track phases of the audit cycle — audit planning, audit risk assessment, audit project management, time management, issue tracking, audit work paper management, audit evidence management, and reporting.

Like Compliance Management, Audit Management also provides a centralized repository and process for Internal Audit teams to automate the complete audit life cycle. You can maintain all test templates and test plans in a single repository, "connect" your audit tasks to controls within the application and configure indicators to collect audit evidence. Issues can be automatically created from indicator results. Observations and deficiencies can be set up as "tasks", assigned to people or groups, and tracked via workflows, SLAs, alerts and notifications.

An audit workbench provides a timeline view of all audit engagements; from which you can select an audit engagement to view details or create a new engagement. Project driven audits allow auditors to quickly scope engagements, develop audit plans, conduct fieldwork, collect control evidence, and track audit observations. The "My Audit Approvals" feature enables supervisors to view audit documents awaiting approvals.

The application provides an executive view into audit results, engagement breakdowns by task, and allows areas of concern to be identified quickly. If you've previously spent hours building reports for management and leadership; or been a leader frustrated by lack of granularity in your reports; you will appreciate the reporting and dashboarding capabilities this tool provides.

If you need to perform periodic security assessments for third parties that have access to your applications and data, you're probably aware of how time consuming and challenging the process can be. For most organizations, the vendor relationship office sends out the assessments as Excel based questionnaires and requests evidence, example SSAE 16 or SOC reports. Usually, there are multiple iterations of the process before the assessment is completed and a report generated. If you are dealing with multiple regulations (ISO 27002, NIST, HIPAA-HITRUST, PCI-DSS, GLBA etc.), you may be customizing your security assessment by vendor, which can be frustrating and error-prone.

ServiceNow GRC can also be used for management, measurement, and reporting against vendor and third party related risk. Leveraging the Vendor and GRC applications, a Vendor Risk Assessment process can be configured using assessments and workflows. The responses to the assessments can be validated and scored. Dashboards and reports can be leveraged for both transactional reports (ex. number of assessments by status, region, etc.) or analytics based reports (ex. which areas are most vulnerable, vendors with high to low compliance metrics etc.). INRY has developed a robust Vendor Security Assessment application which works with the GRC application to automate assessments and reporting.

This use case is often the most overlooked for GRC. ServiceNow can automate most aspects of ongoing Business Continuity Planning & Disaster Recovery (BCP /DR), because it is a natural extension of both Service Management and Governance, Risk, and Compliance.

ServiceNow's Business Service Maps can generate relationships between business services and the Configuration Items that make up those services. CMDB enables rapid identification of upstream and downstream impacts as infrastructure changes occur. Adding in ServiceNow Discovery enables real-time updates to DR planning and documentation. Workflows for planning, review, and testing activities helps organizations reduce cost and save time. Alerts / Notifications enable organizations to remind service and application owners to update business continuity plans.

Using ServiceNow Knowledge Base and automated testing capabilities, organizations can minimize impact and prevent serious disruptions to their business. Since ServiceNow is a cloud based application, it is not impacted by your downtimes. Greater visibility into all aspects of BCP/DR allows for faster and more effective responses.

One of the most tedious aspects of BCP/DR is ensuring the plans exist for all high-risk applications, and monitoring periodic updates of the plans. This requires tracking, following up with application owners (IT and business), seeking approvals, and uploading documentation to a secure site. A significant portion of this effort can be automated by workflows, SLAs, alerts, and notifications.

While your organization may not require all five use cases currently, it is always good practice to evaluate which other pain points in the organization can be alleviated using tools you either already own, or are in the process of purchasing.

If you have any questions; are looking for more INRY Perspectives related to ServiceNow GRC; or would like more informationabout Integrhythm's implementation approach for ServiceNow GRC, please contact us at info@inry.com

2022 GLOBAL PARTNER Award Winner servicenow

**Fastest Growing Company**

FT FINANCIAL TIMES

Inc. 5000

**Certified & Secure**

AICPA SOC 2

SOC 2 TYPE II CERTIFIED