ServiceNow IT Governance, Risk and Compliance

Benefits

- **Reduce Compliance Complexity**
  Ensure continuous visibility and control with a single platform for authoritative sources, policies, risks, controls, IT data and the automation of regularly scheduled control tests.
- **Streamline Audits**
  Establish a set process for validating controls using audit definitions and reduce the time and effort required to gather compliance evidence by automating defined control tests on a scheduled basis.
- **Mitigate Risks**
  Evaluate risks and determine mitigation strategy through automated controls of data already in the ServiceNow platform or pulled in through easily built integrations.

The IT Challenge

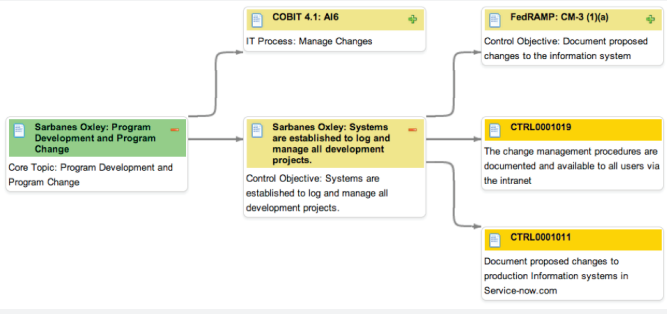
Every organization must follow regulations, standards, frameworks and audit guidelines from authoritative sources – especially those enterprises operating in heavily regulated industries. With both internal and external security threats on the rise globally, it is increasingly important that organizations have a solid IT Governance, Risk and Compliance (IT GRC) program in place. Unfortunately, staying compliant can be disruptive, complex and time-consuming. Some organizations use expensive, specialized software that is separate from their IT systems of record while others rely on manual processes.

Consequently, many organizations struggle to get accurate audit information. Disparate data sources, testing evidence, and control objectives make it difficult to consolidate results into a format that can be easily reported and reviewed for audits. More commonly, organizations initiate manual "fire drills" using spreadsheets and email whenever an audit is conducted, requiring significant effort across the business. Further complicating matters, the findings and results of an audit are often poorly communicated and difficult to understand. And tracking progress on observations and remediation efforts is usually a manual process and problematic to manage.

The ServiceNow Solution

ServiceNow® IT Governance, Risk and Compliance is an application that automates the business-critical process of measuring and managing adherence to legislative policies, such as Sarbanes-Oxley (SOX), and industry frameworks like Control Objectives for Information and Related Technology (COBIT). With ServiceNow's IT GRC application, process controls are aligned to organizational risks and corporate policies. This alignment enables IT GRC to automate the audit process by: managing audit controls, assigning control testing tasks, managing evidence collection, and assigning remediation activities. ServiceNow IT GRC provides a central repository for key controls and audit definitions including a history of audit results with the corresponding findings.

The process is straightforward. First, IT GRC is used to document policies specific to the organization, evaluate the risks to comply and to design controls to enforce policies and mitigate risks. IT GRC is then used to schedule control tests to collect compliance evidence and identify failures that need remediation on a regular basis. Finally, information from service management processes is automatically extracted as evidence for compliance audits. This enables simplified reporting to audit committees and reduces compliance reporting costs. Since all IT service management applications are on the same platform, data can also be reused to run tests and increase audit efficiency. Organizations can also leverage existing ServiceNow platform capabilities for notifications, tasking and collaboration.



Visualize authoritative source content relationships

Single Source of Truth

ServiceNow creates a single source of truth that allows processes across IT to execute with uniform information. Since ServiceNow IT GRC runs on the same platform as all other ServiceNow applications, organizations can automatically collect information from across all service management processes in ServiceNow as evidence of compliance. Audit instances with the corresponding results and findings are automatically updated and retained, creating a distinct audit trail. This gives IT visibility across all applications for a comprehensive view of the audit process.

Authoritative Sources

Authoritative sources define the external standards, frameworks and regulations used by the compliance process. Authoritative sources are made up of authoritative source content and policies and each can be related to or from other sections of the content. Organizations can create policies and related controls to ensure that the required company process is followed each and every time. Publishing and version control of policies are managed using document and knowledge management capabilities built into ServiceNow. Policies can be secured so that only specific individuals or groups can update or change them. Custom workflows ensure that all policy changes are routed to the appropriate executives for final approval. All approved organizational policies are published in the knowledge base and available to the business.

Simplify Audits and Improve Efficiency

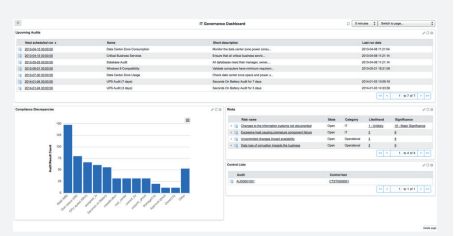
Streamline the audit process by establishing a repeatable process for validating controls and control tests using audit definitions. This also gives organizations the ability to create an audit on-demand; immediately check for compliance; and have ServiceNow automatically assign tasks to the appropriate groups or individuals that need to be performed before, during and after the audit. The audit instances are tracked and recorded as they are created, producing a log of the audit state at a given point in time. The users and groups responsible for the different controls, control tests, remediation tasks and audit instances can easily view the work assigned to them in their work queues. The results can then be provided directly to internal and external audit teams.

Increase Business Agility

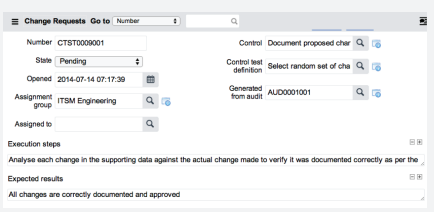
ServiceNow IT GRC gives organizations a tool that can be used to connect policies to evidence, and automatically collect that evidence in real-time – ensuring that accurate audit information is constantly available to business. Any non-compliance and root cause can be identified and corrected to mitigate risk. Furthermore, control tests – based on the data gathered – can automatically assign remediation tasks to the groups or individuals responsible for that area, leading to continuous control of the IT environment. This means that IT can report compliance status with confidence.

Assess and Manage Risks

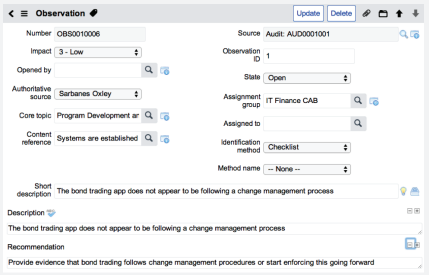
Risks are assessed based upon both frequency and impact to the organization – providing a risk strategy for the company. Risks requiring immediate or ongoing mitigation can be prevented or controlled using organizational-defined controls and related control tests. The control test definition list defines how and when the control tests are performed including execution steps, expected results and the owner of the task. And, test information can be gathered from ServiceNow incident, problem, change, release and configuration applications. Respond to control test failures and audit observations as they happen by automatically creating remediation tasks, which are assigned to either a remediation group or individual within the organization. And, report assessment results and remediation activities through ServiceNow dashboards – the same ones used for service automation.



Define risks and rank the business significance and likelihood of it occurring



Define tests to verify controls are followed to reduce risk and ensure compliance



Audit observations with ability to assign remediation tasks to follow-up

servicenow

www.servicenow.com