May 2018

ServiceNow Indicator Based Continuous Control Management

Innovation in Automated Control Management

SOLUTION***PERSPECTIVE***

Governance, Risk Management & Compliance Insight

Table of Contents

TALK TO US . . .

We look forward to hearing from you and learning what you think about GRC 20/20 research. GRC 20/20 is eager to answer inquiries from organizations looking to improve GRC related processes and utilize technology to drive GRC efficiency, effectiveness, and agility.

ServiceNow Indicator Based Continuous Control Management

Innovation in Automated Control Management

Agility Required in Control Automation

Organizations operate in a complex environment of risk, compliance requirements, and vulnerabilities that interweave through departments, functions, processes, technologies, roles, and relationships. What may seem to be an insignificant information or technology risk in one area can have profound, cascading, and exponential impact on other risks and significant compliance ramifications. The dependency of organizations on information and technology exacerbates this problem with the interconnectedness of third parties and the Internet of Things (IoT) causing more points of exposure. Understanding and managing governance, risk management, and compliance (GRC) in today's environment requires a new paradigm in managing and measuring these interconnections and relationships of information and technology risk management.

Business is impacted by constant change. Change is the single greatest GRC challenge today. Today's organization is in a continuous state of change with shifting employees, business processes, and technology evolving at a rapid pace. In the context of change, internal controls, regulatory requirements (e.g., SOX), internal and external auditors, and fraud risk put increased pressure on corporations to ensure all business systems and data are secure and control risks are managed across a dynamic and distributed business environment.

Managing controls in manual processes is a losing battle. The challenge of managing controls in a heterogeneous technology environment is burdensome when done with manual and document centric approaches.

Surprisingly, many organizations still use these manual processes to manage controls. This is primarily done through spreadsheets, word processing documents, and email. Not only are these approaches inefficient and ineffective, slowing the business down, but they introduce greater exposure to risk and non-compliance, as it is nearly impossible to keep up with the pace of change in technology and business systems. The inefficient, ineffective, and non-agile organization runs a combination of security and control reports, and compiles information into documents and spreadsheets that are sent out via email (used as an improvised workflow tool) for review and analysis. At the end of the day, significant time is spent running reports and compiling and integrating that information into documents and spreadsheets to send out for review. This ends up costing the organization in wasted resources, errors in manual reporting, and audit time drilling into configurations and testing controls in the technology environment. Organizations often miss things, as there is no structure of accountability with audit trails. This approach is not scalable and becomes unmanageable over time. It leads to a false sense of control due

to reliance on inaccurate and misleading results from errors produced by manual access control processes.

Manual processes and document-centric approaches to internal controls are time-consuming, prone to mistakes and errors, and leave the business exposed. This is further complicated by organizations that choose internal control technologies that only look at part of the environment and not across all of their varying business and technology infrastructure and systems. By automating controls, organizations take a proactive approach to avoiding risk while cutting down the cost and time required to maintain controls, be compliant, and mitigate risk.

The bottom line: To address internal control failures and risk, organizations are establishing an automated internal control strategy with process and technology to build and maintain control automation that balances business agility, control, and security to mitigate risk, reduce loss/exposure, and satisfy auditors and regulators while enabling users to perform their jobs. When evaluating solutions for internal control automation the organization needs solutions that are intuitive, easy to use, and should look for a solution that covers the range of business systems used in their environment.

ServiceNow Indicator Based Continuous Control Management

Innovation in Automated Control Management

ServiceNow is a solution provider in enterprise applications for governance, risk management, and compliance (GRC). The company's flexible, scalable, and integrated suite of cloud applications is used by organizations to automate GRC processes, reduce enterprise risk, and demonstrate regulatory compliance to achieve audit-ready status. The ServiceNow Indicator-Based Continuous Control Management functionality delivers efficiency, effectiveness, and agility to strengthen risk management, security, and compliance for organizations across industries and around the world. Organizations can implement control indicators that can test data on schedule with minimal human intervention. In this context, GRC 20/20 has recognized ServiceNow Indicator-Based Continuous Control management with a 2017 GRC Innovation Award for Automated/ Continuous Control Management.

Organizations need to move faster, but lack of process and legacy tools hold them back. Every day, thousands of customer requests, IT incidents, and HR cases follow their own paths moving back and forth between people, machines, and departments. Unstructured, undocumented, and unimproved for years. With the ServiceNow System of Action™ an organization can replace unstructured work patterns of the past with intelligent workflows of the future. Rapid changes in the business, technology, and regulatory environments continuously challenge enterprise GRC programs. Relying on point-in-time risk information and semi-automated processes contributes to risk failures, especially in dynamic and abstracted environments. Enterprises are under pressure to continuously detect for failing critical controls, especially in between assessments to accelerate business impact analysis, orchestrate effective remediation, and enhance visibility and stakeholder accountability.

The ServiceNow platform delivers operational efficiencies and enhances GRC efficacy and control by delivering a system of engagement and actionable insights about the enterprises' risk and compliance operations. ServiceNow GRC extends the benefits of a single cloud-based platform into risk management, compliance, and internal audit. With ServiceNow GRC, enterprises utilize real-time service performance data along with security and threat information to effectively operationalize compliance controls, enhance internal audit productivity, and detect changes in the risk posture. ServiceNow Governance Risk and Compliance integrates with security operations, IT operations, and service management processes to accelerate detection, risk mitigation, and orchestrate remediation across functional groups and processes. The overall outcome is real-time visibility and enhanced productivity of security, compliance, and risk management operations.

What Indicator-Based Continuous Control Management Does

Most organizations manage their GRC processes on a quarterly or annual basis: running attestation questionnaires and collecting attached evidence. This process is very often cumbersome and ineffective to track "Business as Usual" deficiencies. Often the reality of the effectiveness of the attested controls would be very different if it was based on real data, rather than on self-attestations. When run in parallel, data-based continuous compliance testing generally shows major gaps compared to the related self-attestations. Identifying deficiencies on a quarterly, if not annually, basis, also leads to very low response from the organization. Continuous control monitoring allows for immediate response and effective remediation.

Because ServiceNow is a Platform, creating a single system of record between many different applications (e.g., ITSM, CMDB, PPM, HR, CSM, Security, and GRC), organizations can implement control indicators that will test data on schedule without human interaction. These control indicators can test data from ANY ServiceNow table and, based on a business rule, collect evidence and pass or fail the related control.

For example, an organization can have a patching control tested every night individually for each critical application which includes testing:

- A random sample of related change requests and test if all those approved actually have a tested backup plan.
- All related critical vulnerabilities aged more than 30 days. The policy states that all critical vulnerabilities must be patched within 30 days.
- If there are any IT or security incidents related to a processed change request.

Organizations can test and validate as many control indicators as needed. The more data the organization has in ServiceNow, the more that can be automated and tested. No interfacing, no integration, no business intelligence database. Direct testing on live production data for accurate results and assurance.

As soon as a control fails, a related issue (e.g., remediation plan) is created, allocated, and notified to a proper issue owner. The issue owner will then create and allocate as many tasks as required to remediate the control failure. Each issue progress is monitored compared to its service level agreement (SLA).

In addition to this control automation, ServiceNow offers the traditional control attestation questionnaires and workflows, which include a drag and drop design of attestation questionnaires.

The main difference, and innovation, from the previous generation of ServiceNow Governance Risk and Compliance is that control indicators are now associated individually to each controlled entity or profile, based on a library of indicator templates. They are also associated to specific internal policy and/or regulatory requirements. ServiceNow Governance Risk and Compliance allows you to profile any entity from the ServiceNow system of record, for instance: regions, companies, departments, business processes, and applications (critical, PCI related, GDPR related, and operational)

Benefits Organizations Receive with Indicator-Based Continuous Control Management

GRC is an integrated capability to reliably achieve objectives [GOVERNANCE], while addressing uncertainty [RISK MANAGEMENT], and acting with integrity [COMPLIANCE].[1] Successful GRC strategies deliver the ability to effectively mitigate risk, meet requirements, satisfy auditors, achieve human and financial efficiency, and meet the demands of a changing business environment. GRC solutions should achieve stronger processes that utilize accurate and reliable information. This enables a better performing, less costly, and more flexible business environment.

GRC 20/20 measures the value of GRC initiatives around the elements of efficiency, effectiveness, and agility. Organizations looking to achieve GRC value will find that the results are:

- **GRC Efficiency.** GRC provides efficiency and savings in human and financial capital resources by reduction in operational costs through automating processes, particularly those that take a lot of time consolidating and reconciling information in order to manage and mitigate risk and meet compliance requirements. GRC achieves efficiency when there is a measurable reduction in human and financial capital resources needed to address GRC in the context of business operations.

- **GRC Effectiveness.** GRC achieves effectiveness in risk, control, compliance, IT, audit, and other GRC processes. This is delivered through greater assurance of the design and operational effectiveness of GRC processes to mitigate risk, protect integrity of the organization, and meet regulatory requirements. GRC effectiveness is validated when business processes are operating within the

1 *This is the official definition of GRC found in the GRC Capability Model and other work by OCEG at www.OCEG.org.*

controls and policies set by the organization and provide greater reliability of information to auditors and regulators.

- **GRC Agility.** GRC delivers business agility when organizations can rapidly respond to changes in the internal business environment (e.g. employees, business relationships, operational risks, mergers, and acquisitions) as well as the external environment (e.g. external risks, industry developments, market and economic factors, and changing laws and regulations). GRC achieves agility when organizations can identify and react quickly to issues, failures, non-compliance, and adverse events in a timely manner so that action can be taken to contain these and keep them from growing.

GRC 20/20 has identified that the business benefits and value of ServiceNow's Indicator-Based Continuous Control Management to be:

- *Maximize flexibility*, by leveraging the applicability of control indicators to specific controls and specific profiles (entities).
- *Increase performance* in running those control indicators, as they run against individual controls and against specific profiles (entities), they do not affect the global performance of the ServiceNow Platform.
- *Enhance detection and response* by providing control evidence on a daily / weekly basis and by launching related remediation plans (Issues) immediately. The organization has an up-to-date view of compliance at any time.

Considerations in Context of Indicator-Based Continuous Control Management

Every solution has its strengths and weaknesses and may not be the ideal fit for all organizations in all situations. While GRC 20/20 has identified many positive attributes of ServiceNow and Indicator-Based Continuous Control Management to enable organizations to achieve efficient, effective, and agile GRC management processes, readers should not see this as a complete and unquestionable endorsement of ServiceNow.

The previous architecture of ServiceNow Governance, Risk, and Compliance allowed direct control testing on ServiceNow data, but scoping by profiles was not available. However, the addition of Profile Management in the Helsinki release (2016) has made it easier for organizations to scope controls by profiles, which are created on existing records in ServiceNow tables. This makes the adoption of the continuous control monitoring easier. ServiceNow automates this process providing greater assurance to the organization and its stakeholders that controls are effective. Other GRC solution providers do not offer this level of control automation as they do not provide a full IT Service Management Platform, with direct access to the data needed to test, as ServiceNow does.

About GRC 20/20 Research, LLC

GRC 20/20 Research, LLC (GRC 20/20) provides clarity of insight into governance, risk management, and compliance (GRC) solutions and strategies through objective market research, benchmarking, training, and analysis. We provide objective insight into GRC market dynamics; technology trends; competitive landscape; market sizing; expenditure priorities; and mergers and acquisitions. GRC 20/20 advises the entire ecosystem of GRC solution buyers, professional service firms, and solution providers. Our research clarity is delivered through analysts with real-world expertise, independence, creativity, and objectivity that understand GRC challenges and how to solve them practically and not just theoretically. Our clients include Fortune 1000 companies, major professional service firms, and the breadth of GRC solution providers.

Research Methodology

GRC 20/20 research reports are written by experienced analysts with experience selecting and implementing GRC solutions. GRC 20/20 evaluates all GRC solution providers using consistent and objective criteria, regardless of whether or not they are a GRC 20/20 client. The findings and analysis in GRC 20/20 research reports reflect analyst experience, opinions, research into market trends, participants, expenditure patterns, and best practices. Research facts and representations are verified with client references to validate accuracy. GRC solution providers are given the opportunity to correct factual errors, but cannot influence GRC 20/20 opinion.

GRC 20/20 Research, LLC
4948 Bayfield Drive
Waterford, WI 53185 USA
+1.888.365.4560
info@GRC2020.com
www.GRC2020.com