March 2017

Telos® Xacta®

Accelerating Compliance of IT Security Controls

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.

Telos® Xacta®

Accelerating Compliance of IT Security Controls

Complexities of the Cloud Hinders Organizations

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 as an insignificant risk in one area can have profound impact on other risks and cause compliance issues. Understanding and managing IT governance, risk management, and compliance (IT GRC) in today's environment requires a new paradigm in managing these interconnections and relationships. This is particularly true of cloud environments in which there is shared responsibility for security, risk, compliance, and control between the organization and the cloud hosting environment.

IT security departments are scrambling to keep up with multiple initiatives that demand greater oversight of risk and compliance across the cloud, infrastructure, identities, processes, and information. Most organizations approach these issues reactively — putting out fires of security and compliance wherever the flames are hottest. As these pressures mount, IT security often fails to think strategically as it is too busy reacting to issues. Organizations need to step back and think strategically; to figure out how to streamline resources and use technology efficiently, effectively, and agilely to manage and monitor cloud environments.

A reactive approach to cloud security and compliance is not sustainable in an environment of growing pressures, and is a recipe for disaster that leads to:

Higher cost, from . . .

- **Wasted and/or inefficient use of resources.** Silos of reaction to IT security needs and issues lead to wasted resources. Instead of leveraging controls and resources to meet a range of risks and compliance requirements, controls are developed haphazardly to address specific pain with no thought for leverage across pains. Organizations often try to relieve the symptoms instead of thinking how to address the root cause. IT security ends up with different internal processes, systems, controls, and technologies 'in play' to meet individual risk and compliance needs.

- **Unnecessary complexity.** Multiple IT security and compliance approaches introduce complexity which in turn adds overhead, cost and increases inherent risk. Controls are impossible to streamline and manage consistently, introducing more opportunities for controls to fail or go unmonitored. Inconsistent controls

also produce inconsistent documentation, which further confuses IT security, regulators, and the line of business.

Inability to align with the business, resulting in . . .

- **Lack of agility.** Complexity drives inflexibility. Cloud security and control becomes so wrapped up in spinning individual risk and compliance plates and reacting to cloud deployments that support of the business is degraded. IT security staff along with the business is bewildered by a maze of varying methodologies and control requirements that are not designed with any consistency or logic, and struggle to apply and assess this in cloud environments.

- **Vulnerability and exposure.** A reactive approach leads to more exposure and vulnerability. Complexity means departments are focused on their own silo of risk, and no one sees the big picture in cloud exposure. No one looks at cloud security and control holistically or contextually, with regard for what is good for the business in the long run. Varying and independent efforts around the cloud lead to difficulty demonstrating control with a result in confusing audits and assessments.

Not only does a reactive approach to cloud security and control lead to greater vulnerability and exposure, it also means higher costs for the business. Addressing cloud security, compliance, and control across a series of disconnected projects and assessments leads to inefficiency in management and operations, wasted spending on redundant approaches, and a greater burden to the business.

The bottom line: When organizations approach cloud security, compliance, and control in scattered documents and disconnected solutions and processes there is no possibility to be intelligent about cloud security and control decisions that impact the broader organization, its operations, and compliance to regulations. Organizations need an integrated cloud security architecture that delivers 360° contextual intelligence on cloud security, compliance, and control.

Telos Xacta

Accelerating Compliance of IT Security Controls

Telos Xacta (Xacta) is an IT GRC management solution that GRC 20/20 has researched and evaluated, that can manage IT security, risk, compliance, and controls in complex, distributed, and dynamic business environments, particularly cloud environments. Xacta delivers a cloud security control management solution to identify, asses, and mitigate risk in cloud environments.

Xacta has a partnership with Amazon Web Services (AWS). As part of this partnership Xacta integrates with AWS' Enterprise Accelerators for Compliance (EA4C) and specific AWS services to enable controls compliance validation of AWS infrastructure to be continuous in a dynamic and changing cloud and business environment, as well as thoroughly documented to satisfy regulators, stakeholders, and other third parties.

GRC 20/20 finds that the Xacta solution enables organizations to be efficient, effective, and agile in their cloud management strategy and processes. Xacta is well suited for use across industries and organizations from small to large to manage cloud security and control.

GRC 20/20's evaluation of Xacta reveals that it:

- ***Automates*** continuous compliance processes in the cloud
- ***Provides*** an intuitive and easy to use interface
- ***Documents*** controls and requirements to satisfy regulators and stakeholders

What Xacta Does

GRC 20/20 has evaluated the capabilities of the Xacta solution and finds that it delivers an intuitive and robust security and control management solution to manage on-premises and cloud environments, like AWS, in context of today's demanding requirements and dynamic environments. Xacta automates what were once labor intensive tasks associated with managing IT risk and compliance. This functionality has now been optimized for use in cloud environments. This functionality is essential for managing a maze of manual processes, documents, spreadsheets, email, and narrow point solutions.

Xacta is a suite of products that provide specific IT GRC capabilities as follows:

- **Xacta 360.** The core of the Xacta solution-suite operationalizes IT risk and compliance frameworks (e.g., NIST, ISO). This is an established component of the Xacta suite since 2000. Most recently this component has been optimized for cloud deployments in which Xacta integrates with AWS to allow for automated scalability to accommodate spikes in usage. Xacta 360 integrates with AWS infrastructure via EA4C and specific AWS services to automate AWS resource scanning and control compliance validation. Xacta 360 can be deployed on premise or in the cloud. Either deployment option will allow users to manage AWS workloads.
- **Xacta Continuum.** The component of Xacta that operationalizes continuous monitoring of the IT risk, control, and compliance environment. Xacta Continuum can be deployed on-premises or in the cloud. On premise, Xacta Continuum allows the organization to manage risk and compliance of on-premises assets. When deployed in the cloud, Xacta Continuum is used to manage controls and compliance of cloud-based resources such as those in the AWS infrastructure (e.g., operating systems).
- **Xacta Campaign Compliance Manager (CCM).** Xacta CCM is used to validate non-technical controls through questionnaires and surveys. Non-technical/ administrative controls often represent approximately 70% of the total number of IT security controls many organizations are responsible for evaluating.

Automated control validation is critical, but other validation methods such as surveys and questionnaires are essential for IT compliance.

Xacta Enables Cloud Security & Control Lifecycle

Xacta effectively and efficiently enables an organization's end-to-end cloud security and control management strategy by providing a platform to manage the lifecycle of control in cloud environments. This lifecycle that Xacta automates, includes:

- **Defining scope and requirements.** Xacta integrates with the AWS Enterprise Accelerator for Compliance to provide a thorough and robust framework of control for compliance. This is cross-referenced to show compliance to a range of regulations and standards, such as NIST standards, PCI DSS, ISO 27000, and HIPAA. Organizations can also add their own specific controls and requirements in context of the framework provided.

- **Assessment.** Utilizing the scope of requirements, the organization can then do the initial assessment of their cloud application against the requirements to validate and document compliance and control.

- **Ongoing continuous monitoring.** Assessment is not a one-time effort with Xacta, it is something that is done continuously. Xacta can be used to continuously reassess cloud implementations to ensure they are always compliant. This is critical in today's dynamic technology and business environments.

- **Issue resolution.** When issues are discovered, Xacta is used to define workflow and tasks to ensure they are remediated.

- **Documentation & reporting.** Xacta streamlines the documentation and reporting on cloud control and compliance. This saves significant time for staff that had to manually reconcile and validate controls in scattered processes, documents, and emails.

Foundational Capabilities in Xacta

While Xacta can manage specific cloud security and control processes, it can also be used for managing security, compliance, and control across the range of internal systems organizations have in their data centers, not just in the cloud. Specific capabilities Xacta delivers that enable organizations in IT security management, no matter the scope are:

- **Configurability.** Xacta is designed to be highly agile and adaptable to the unique requirements of organizations. The solution is able to evolve to accommodate the dynamic nature of IT security, compliance, and control as well as changing business and regulatory requirements.

- **Content integration.** Xacta has integrated and mapped a broad array of regulations and standards for controls so organizations can assess once and comply with many.

- **Analytics.** Xacta delivers contextual risk and control analytics that is intelligent through the triangulation of collected information across systems and initiates workflow issue resolution when red flags occur.

- **Risk modeling.** Xacta enables organization to provide a standardized objective calculation of risk in IT environments to determine.

- **Notifications.** Xacta provides notification through emails to notify stakeholders and others of programs and expectations with embedded links to online questionnaires and tasks.

- **Workflow and task management.** The Xacta solution provides a full range of capabilities to flexibly build workflow and tasks. This includes the ability for both linear and parallel workflows, alerts on pending tasks that are soon due, and escalation of missed tasks.

- **Questionnaires, self-assessments, and surveys.** The Xacta solution delivers a full range of survey capabilities to gather information from stakeholders with embedded instructions and validations to help ensure completeness and accuracy.

Benefits Organizations Can Expect with Xacta

Organizations are most likely to move to the Xacta platform because they found that their manual document centric approaches took too many resources to administer, only addressed specific areas of control, and found things slipping through the cracks because of the continuous barrage of change. Some organizations choose Xacta because their existing IT GRC management solution was too narrow and could not address all their needs (e.g., AWS) or was too costly in the complexity, licensing, and administration of the system.

Specific benefits organizations can expect from implementing the Xacta solution are:

- *Data integrity* with Xacta being the system of record for all cloud security, compliance, and control information.

- *Reduction in errors* by automating the validation of compliance and control removing errors from manual processes and reconciliation that was incomplete or incorrectly entered.

- *Significant efficiencies in time* through automation of workflow and tasks as well as reporting. Specifically, the time it took to build reports from documents and spreadsheets now is just a matter of seconds.

- *Collaboration and synergies by providing a single platform* with a consistent interface to manage cloud security, compliance, and control information and interactions across departments instead of different departments doing similar things in different formats and processes.

- *Consistency and accuracy of information* as all internal stakeholders have to conform to consistent processes and information collection. A single solution with a uniformed and integrated process and information architecture.

- *Accountability with full audit trails* of who did what and when; this particularly has delivers value in fewer things slipping through the cracks.

Considerations in Context of Xacta

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 Xacta to enable organizations in the consistent control management and monitoring of cloud environments — readers should not see this as a complete and unquestionable endorsement of Xacta or Telos.

Overall, organizations should have a high degree of satisfaction with their use and implementation of Xacta. The solution's adaptability and ease of use, as well as the ease of integration into the broader IT environment is of a particular benefit to organizations. The solution is agile by allowing distributed internal stakeholders to get what they need while providing consistency across functions involved in cloud management.

GRC 20/20 finds that Xacta provides value in managing the lifecycle of cloud security, compliance, and control across departments and functions. As many organizations respond to growing regulatory requirements in cloud environments and risk exposure they often enter a fire-fighting reactive mode to deploy a solution for specific purposes where the need for automation has been the greatest given regulatory and audit pressures upon the organization.

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