Telos and Amazon Web Services (AWS):

Accelerating Secure and Compliant Cloud Deployments

Telos Corporation
19886 Ashburn Road
Ashburn, VA 24445
www.telos.com

Introduction

Telos Corporation and Amazon Web Services (AWS) have partnered to expedite security compliance of systems in the cloud through automation. Enabling the Xacta® solution suite to inherit security controls from the AWS Enterprise Accelerator for Compliance allows enterprises to automate compliance and the generation of associated documentation, which streamlines their ability to demonstrate that they meet the standards that apply in their industries.

This paper will highlight the challenges involved in cloud-based compliance and how Telos' relationship with AWS addresses these challenges, using their work together for agencies of the U.S. Intelligence Community as a case study. The benefits that are resulting from this partnership can be extended to public and commercial enterprises that want to move to the cloud while also ensuring they can demonstrate compliance with security standards.

Situation Overview

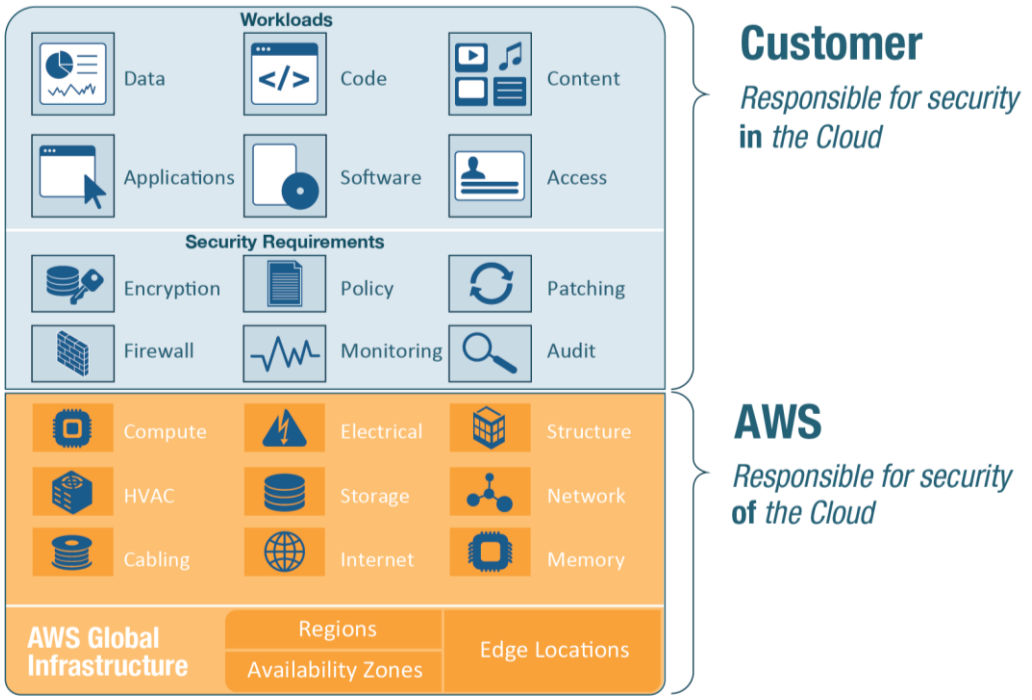
Enterprises in both the private and public sectors are embracing the cloud as a flexible, cost-effective IT resource that can help them achieve their missions faster. Security concerns were once a barrier to cloud adoption, but that's changing. A 2016 survey conducted by the Cloud Security Alliance found that two in three IT leaders think the cloud is as secure as or even more secure than on-premises software.[1]

This growing trust is due in large part to the security that cloud service providers (CSPs) build into their infrastructures. A leader in this initiative is AWS, where cloud security is the highest priority. AWS customers benefit from a data center and network architecture built to meet the requirements of the most security-sensitive organizations. Any system using AWS workloads should be able to leverage (inherit) some or all of the controls implemented by AWS as defined in the applicable standard.

Still, this built-in cloud security only covers the infrastructure and associated security controls provided by AWS — "from the concrete to the hypervisor," to use Chris Hoff's phrase. Under the AWS Shared Responsibility Model, each customer still needs to ensure that the workloads and resources they move to the cloud comply with relevant security standards.

In the commercial sector, these standards include ISO, COBIT, PCI-DSS, the NIST Cyber Security Framework, and others. In the U.S. federal government, various adaptations of the NIST Risk Management Framework (RMF) are used by civilian agencies, the military, and the Intelligence Community (IC).

[1] "The Cloud Balancing Act for IT: Between Promise and Peril"



The AWS Shared Responsibility Model. *While AWS manages security* **of** *the cloud, security* **in** *the cloud is the responsibility of the customer. Customers retain control of what security they choose to implement to protect their own content, platform, applications, systems and networks, no differently than they would for applications in an on-site data center.*

The Challenge: Simplifying Security Compliance Options to Meet Controls.

The shared responsibility model of compliance leaves customers with a large number of decisions to be made to ensure a secure environment.

For example, federal IT systems must go through the NIST RMF process, which demands that the entire cloud-based ecosystem — including the customer's workloads and the AWS services they use — demonstrate that sets of applicable controls have been appropriately implemented.

The control sets vary for each system and the test plan for validating the implementation of the controls is unique for each system. A single agency might need to map hundreds of NIST 800-53 security controls to dozens of AWS services — an error-prone, time-consuming process.

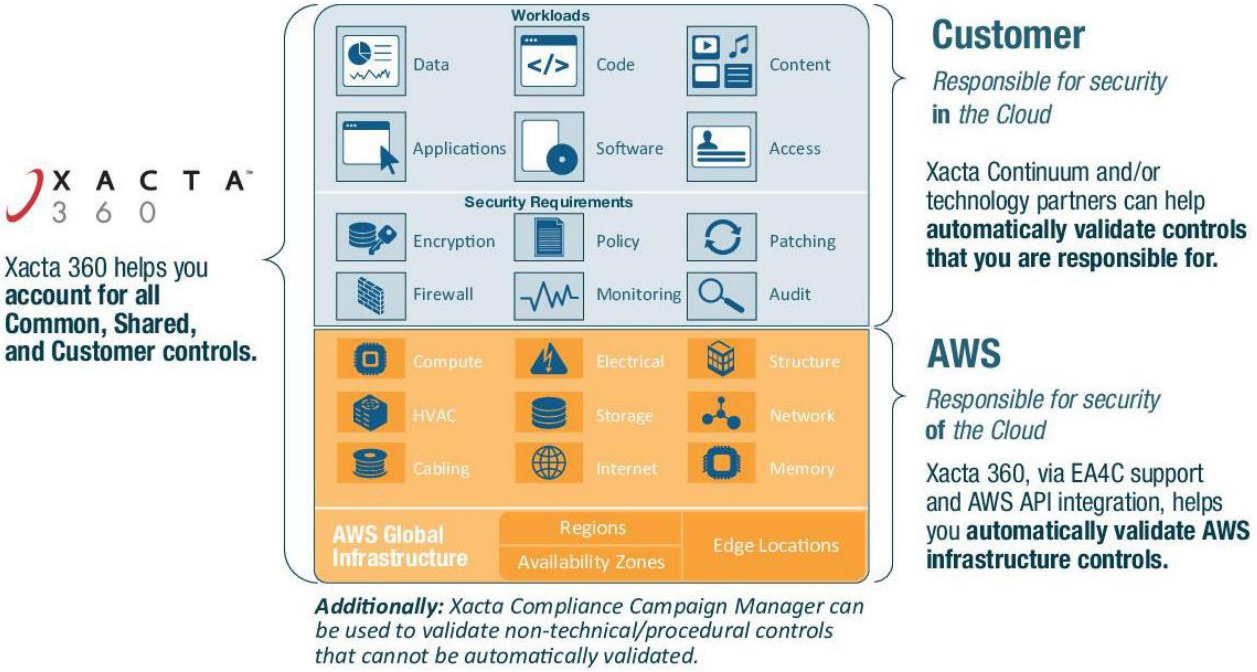
Furthermore, having gone through the NIST RMF, the entire cloud-based ecosystem must receive an ATO (Authority to Operate) from that organization's AO (Authorizing Official) before the customer workloads can become operational.

In short, a federal agency cannot actually go production on a commercial cloud such as AWS unless its workloads on those cloud services are also compliant.

Introducing Xacta: Automating Compliance in the Cloud.

Now, Telos is streamlining compliance in the cloud by enabling Xacta to automatically inherit security controls from the AWS Enterprise Accelerator for Compliance. Xacta can now automate the compliance testing and verification of workloads on the cloud architecture according to the most common security standards and guidelines.

This will allow organizations to seamlessly automate compliance as they stand up their data, information, and applications in the cloud. The solution queries the user as to which regulations apply to them, generate and auto-populate a compliance package specific to their cloud environment, and then walk them through to completion with a wizard-based application.



Leverage the AWS Shared Responsibility Model for faster cloud compliance and deployment.
Xacta inherits the AWS security controls while enabling you to implement and manage security compliance for your own data, content, platform, applications, systems, and networks.

The AWS Enterprise Accelerator for Compliance is a security-focused, standardized architecture solution to help managed service providers (MSPs), cloud provisioning teams, developers, integrators, and information security teams adhere to strict security, compliance and risk management controls.

The Xacta solution suite meets the complex challenges of managing IT risk with continuous compliance monitoring, security assessment, and ongoing authorization.

Deployed at more than 100 customer locations and used by agencies of the Intelligence Community for their risk management requirements, Xacta enables IT security personnel to continuously manage risk and security compliance as well as automatically manage key elements of the NIST assessment and authorization process.

Xacta 360 automatically inherits common security controls from AWS workloads, continuously validates their compliance with leading standards and frameworks, and automates key compliance processes to maintain risk posture in the face of rapidly changing IT environments. It also integrates with AWS EC2 to accommodate workload fluctuations.

Xacta Continuum™ correlates scan results from multiple security products into a single view and maps them to the relevant controls for security and risk management, such as NIST 800-53, CNSS 1253, DoDi 8500.2, ISO, and others. These results can be used to create reports for continuous security assessment and to understand trending security issues in the environment.

> *"The two things organizations are demanding in GRC related solutions are ease of use as well as relevant analytics and reporting. Organizations need 360° situational awareness of their risks in a context that is meaningful and relevant. Xacta is delivering this ease of use and situational awareness."*
> *- Michael Rasmussen, GRC 20/20*

Xacta Compliance Campaign Manager streamlines and simplifies IT policy compliance by letting organizations create and distribute OCIL-based surveys and questionnaires for manual security checks, enforce controls for leading government and commercial standards, and crosswalk controls from different frameworks for greater efficiency and less redundancy.

Xacta SmartView™ is a fully customizable visualization and reporting module that brings together data sets to create an executive view of an organization's security and compliance posture. The intuitive and user-friendly dashboard makes it easy for CISOs and other security decision-makers to pull reports, see what items need attention, and gain actionable insights into risk and compliance.

Working in combination, the AWS Enterprise Accelerator for Compliance and Xacta will enable enterprises to leverage a standardize-and-repeat model for efficiency and less redundant or manual effort. The combination supports the creation of reference implementations of typical use cases as standardized baseline architectures. Enterprises can then pre-populate and endorse security controls implementation details within Xacta as well as automate NIST RMF processes and deployments.

The Intelligence Community: First to Benefit from Xacta's Inheritance of Security Controls from the AWS Enterprise Accelerator for Compliance

Growing confidence in cloud security has given members of the U.S. Intelligence Community the confidence to move sensitive data and applications into AWS Cloud Regions such as GovCloud and C2S, which have been purpose-built for the IC's stringent security requirements.

For IC agencies that use these services, the addition of Xacta has brought the promise of more efficient and streamlined compliance processes. Xacta is already in use as the System of Record and Database of Record enterprise-wide within the Intelligence Community. Together, AWS and Telos are proving the effectiveness of this new approach to cloud compliance automation in their mutual work with intelligence agencies.

Additionally, a capability has been added to Xacta allowing information sharing and persistent inheritance across diverse instances of Xacta. This capability facilitates a master "Xacta instance," capable of providing common or shared controls across multiple organizations or boundaries.

AWS provided the control details to the Telos team for integration into the Xacta solution, making them automatically inheritable (in whole or in part) for any system owner looking to run their workloads on AWS. In addition to these AWS-provided controls, Telos has also captured all the common provider (shared responsibility) controls and made these automatically inheritable.

Xacta: a Groundbreaking History in IT Governance, Risk Management, and Compliance

The Xacta suite from Telos is a fully integrated enterprise risk management solution that provides flexible and comprehensive visualization of compliance-related data.

- Xacta technology and vision influenced the establishment of the commercial IT GRC industry in early 2002.
- Telos launched the industry-first agent-based continuous assessment capability in 2004 which influenced the current continuous monitoring market.
- As an extension to continuous assessment, Telos introduced industry-first continuous remediation management capability in 2005.
- Telos was first to operationalize the NIST Risk Management Framework via software, allowing government agencies to easily migrate from previous certification and accreditation (C&A) processes such as DIACAP and DCID 6/3 to risk-management processes based on the NIST RMF.
- Today, Telos is pioneering new ways to enable organizations transitioning to cloud environments to assess risk, maintain compliance, and continuously monitor the risk posture of their enterprise.

An example of a common provider control might be one or a set of controls that is met when using an agency or community approved Network Access Control or User Access Control configuration. Being able to automatically inherit all these controls within Xacta greatly reduces the time and effort for system owners to get to ATO.

The Business Case for Xacta featuring the AWS Enterprise Accelerator for Compliance

The key to AWS and Xacta saving you time and effort is the ability to inherit common security controls and automate key compliance processes. According to an analysis conducted by Telos:

- The estimated effort for a typical deployment of the NIST Risk Management Framework for a small system is 2,546 labor hours over a six-month period.
- Applying Xacta featuring the AWS Enterprise Accelerator for Compliance would reduce the effort to a conservative estimate of 2,062 hours over 3-4 months, with the potential for additional timeline compression as the organization matures.

- Thus, in addition to the lower cost of cloud, an organization can save a minimum of 20% in labor costs for security compliance activities, and perhaps as high as 90% depending on how many common controls the organization needs to leverage.

- Future savings and improved security visibility can be realized by refocusing the activities of security personnel from tedious RMF processes to development and usage of better continuous monitoring tools.

Integrating the AWS Compliance Architecture into Xacta

AWS and Telos are working together to combine the best practices and generally accepted security configurations with the automation capabilities of AWS and Xacta to develop reference implementations for typical system designs and use cases.

With the release of AWS Enterprise Accelerator for Compliance's Security Controls Matrix (SCM), this automation is available today. The automation provided by AWS to build these environments naturally accelerates deployment with security controls included, and the advent of Infrastructure as Code lends itself to integration into the Xacta suite to pre-populate security documentation:

> "… With proper use of this tool and implementation, up to 70+ controls can be fully implemented / inherited and up to 15+ additional controls achieve partial implementation, requiring only system-specific customization." Veris Group

- Standardized reference implementation artifacts based on pre-defined architectures
- AWS Common Controls inherited by cloud tenants
- System specific security controls within AWS cloud environments

The SCM identifies two sets of controls: Common (fully inheritable) and Shared (system specific or hybrid). This content will be used to create standardize packages in Xacta 360 for each control set, populated with the respective security control implementation details and reference architecture diagrams for automated distribution into the individual projects.

Xacta 360 features can then be leveraged for the NIST RMF workflow and continuous monitoring. The security control configurations can be built into scripts, and then evaluated and approved for use and re-use within each authorizing agency.

Once deployed, the Security Controls Assessment need only validate that the operational system matches the original template, and assess any deltas found, reducing time to achieve an authorization decision.

Automating Continuous Monitoring

Since the system architecture can be inspected and described with AWS and other tools programmatically, it accommodates automated continuous monitoring and improved visibility of the network.

Continuous Automated Compliance

- Automated continuous monitoring techniques can report on infrastructure / inventory changes in near real time ("know the network").
- A Remediation Plan is auto-generated in Xacta after an unapproved security-relevant change.
- Xacta HostInfo verifies secure configurations.
- Xacta Continuum automates analysis of technical control details.
- Non-technical control details are managed by Xacta Compliance Campaign Manager.

Areas of Automation within Xacta

- Artifacts: AWS provides artifacts that make up and describe the reference implementation. These artifacts include .json files, the network architecture, data flow diagrams, implementation guides, and others. This is useful to the assessors, engineers, and authorizing officials as it becomes standardized and repetitive, reducing confusion and decreasing the knowledge gathering process of the assessment effort.

- System Interfaces: AWS also provides implementation details regarding the system interfaces and cross-domain solutions that are packaged up in the standardized reference implementation. This is all information that can be staged in the pre-endorsed configuration template within Xacta. The more systems that leverage this particular configuration, the more efficient the assessment of the system.

- System Environment: AWS provides features for users to build their system with redundancy in mind. In Xacta 360, this is recorded as multiple entries in the System Environment. These entries indicate file servers responsible for maintaining data archives, alternate points of presence on the network, and disaster recovery environments.

- System User: Xacta 360 provides features that capture the types of users and groups of users that are responsible for maintaining, administering, and using the information system. As AWS provides features for users to configure their users and groups as well as their list of permissions, this particular information is easily captured in the pre-endorsed configuration as well.

- Customized Test Procedures: Pre-defined test procedures can be developed and documented in Xacta for infrastructure configuration/components.

- Pre-Endorsed Configuration: In addition to the definition of the system boundary, the pre-endorsed configuration can be staged with implementation details of the system-specific controls. The implementation details are provided by AWS according to their recommendations on how each control is met. There are several security components provided by AWS, including User and Network Access Control, Data Flow and Data Protection, Redundancy, Logging and Auditing of the Information System, as well as Boundary protection mechanisms. All of these components are easily notated in the Xacta pre-endorsed configuration in the previous examples, as well as the implementation details of the SCM.

- AWS Common Control Provider: In addition to the pre-endorsed configuration, common control providers can be established in the system based on recommendations from a cloud provider. These packages can be established for inheriting controls to consumers of the service, such as those systems that were created using AWS's standard reference implementation.

Conclusion

The same dynamics that are leading the Intelligence Community to the cloud are also compelling civilian federal agencies, the military, commercial enterprises, and critical infrastructure to move in the same direction.

And, the same model that AWS and Telos have established to support the IC can be replicated to other industries reflecting standards and frameworks that apply to them:

...automated FedRAMP compliance for civilian federal agencies;

...the NIST CSF for critical infrastructure and related industries;

...cross-industry standards like ISO, COBIT, and PCI-DSS;

...industry-specific standards like HIPAA and GLBA.

With Xacta compliance, enterprises have the evidence and artifacts they need to prove their cloud-based IT systems are compliant. By automating compliance in the cloud, Xacta featuring the AWS Enterprise Accelerator for Compliance smooths the way for any enterprise that wants to leverage the power of the cloud while also managing risk and compliance across all components of their cloud-based applications and workloads.

Moving to the cloud means faster to mission for government and faster to revenue for business. And Xacta featuring the AWS Enterprise Accelerator for Compliance means faster to security compliance for both.

AWS + Xacta = A Powerful Solution for Cloud-based Compliance

- Standardize base architectures for typical use cases (Reference Implementations)
- Pre-populate and endorse security controls implementation details within Xacta
- Automate NIST RMF & deployment with AWS and Xacta features