Xacta for Cloud Compliance

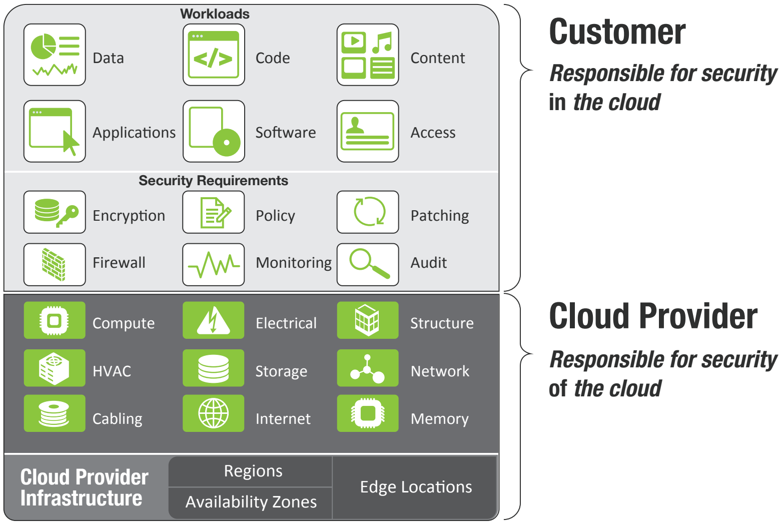
Compliance and Control in the Cloud

How automated cloud compliance helps enterprises manage regulatory risk without inhibiting innovation.

In the past, IT leaders in highly regulated industries were cautious about embracing the cloud. Now, a tipping point has been reached and cloud adoption is no longer optional. It's a business essential. And as security and compliance automation have become more sophisticated and powerful, moving to the cloud can help solve some of the toughest compliance challenges your organization is facing today.

Too many controls.

Enterprises have to deal with an enormous number of controls to maintain regulatory compliance, and each control takes an enormous amount of work to establish. The control has to be interpreted in a way that makes sense for the environment, an implementation plan must be developed and executed, and once in place, the control needs to be monitored, maintained, and documented. Keeping audit trails up to date is time-consuming and resource-intensive work.



The Shared Responsibility Model of cloud security. While your cloud provider manages security of the cloud, security in the cloud is your responsibility.

Cloud controls are out of your control.

Cloud providers follow a "shared responsibility model" of cloud security. They manage the security of the cloud – things like disaster recovery, system redundancy, network controls, and physical security of the data center. On the other hand, security in the cloud – of the workloads and systems you manage there – is your responsibility. You need to demonstrate that you've implemented the appropriate security controls for your applications, databases, software, files, and other assets.

What's more, you also have to report on the compliance of the cloud provider's services you use. (They manage the security, but you have to report on it.) For each service, there can be hundreds of security controls you need to account for — just as with an on-premises asset, service, or system. This configuration and documentation process can be tedious, labor intensive, and challenging to customers and will normally delay cloud migrations.

> *86% percent of security personnel reported that cloud compliance is an issue for their organizations.*

Not enough people.

Most businesses are subject to multiple security standards. But few have the expertise on staff to build the workflows or generate the documentation required for each standard, or to change workflows and documents every time a standard is updated. Even if the budget for headcount is available, finding people with the right skills can be a challenge.

Audit fatigue and empty chairs.

Audit preparation is an endless cycle and the people involved can feel like they're fighting a losing battle. Audit fatigue leads to burnout, which leads to unfilled seats in the SOC—and an understaffed security team is a business risk.

Visibility is always just over the horizon.

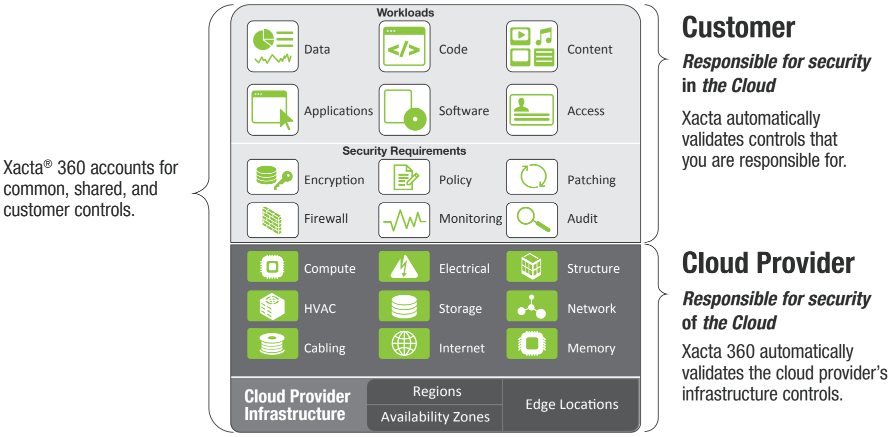
To achieve the visibility needed to protect their infrastructure, enterprises implement a lot of security products, which produce a lot of data... but then security operators have to normalize all that data in order to gain a cohesive and comprehensive view of network activity. Data management becomes the job, when the job *should* be extracting insights to fuel faster decision-making so the business can stay a step ahead of the next wave of threats.

Xacta: The Era of Manual Processes for Cloud Compliance is Over.

Modern multi-cloud and hybrid infrastructures are too big, too complicated, and too dynamic to control with spreadsheets and emails. With **Xacta from Telos Corporation**, you can manage IT risk with continuous compliance monitoring, security assessments, and ongoing authorization.

Xacta delivers the essential capabilities for compliance in the cloud.

Inherited controls for more efficient security compliance reporting. Xacta supports continuous controls inheritance so that your workloads can inherit the regulatory status from the cloud environment they're hosted on. In a cloud environment, that means you can leverage the benefits of your cloud provider's security compliance efforts for your own reporting requirements. This capability takes advantage of the cloud's "shared responsibility model" to reduce the burden on your security team by orders of magnitude.


Xacta® 360 accounts for common, shared, and customer controls.
Workloads
Data
Code
Content
Applications
Software
Access
Security Requirements
Encryption
Policy
Patching
Firewall
Monitoring
Audit
Compute
Electrical
Structure
HVAC
Storage
Network
Cabling
Internet
Memory
Cloud Provider Infrastructure
Regions
Availability Zones
Edge Locations
Customer
Responsible for security in the Cloud
Xacta automatically validates controls that you are responsible for.
Cloud Provider
Responsible for security of the Cloud
Xacta 360 automatically validates the cloud provider's infrastructure controls.

Xacta inherits the cloud provider's security controls while enabling you to implement and manage security compliance for your own data, content, platform, applications, systems, and networks.

Risk-based security management and automated control validation. Xacta aggregates data from across the infrastructure, normalizing scan results from the security stack into a single view, and mapping the results to relevant cloud-specific and other security controls and standards, including FedRAMP, DoD CC SRG, ISO/IEC 27001, and others. Results are associated with actual systems, so a risk that is known to touch critical data can be patched right away.

Continuous assessment to support continuous audit cycles. Xacta automates the security assessment processes that underlie compliance and maintains a central body of evidence that supports today's continuous audit cycles. The same data can be used for real-time analysis to support threat-informed risk decisions about the security of critical assets in multi-cloud, hybrid, and on-premises environments

Predictive control mapping: test once, comply with many standards. Xacta enables you to dynamically map content from various vulnerability schemas to relevant controls in a relationship model. This industry-unique Predictive Mapping™ capability lets you test once and comply with multiple cloud-specific and other security controls. Predictive Mapping automatically detects and plots points of intersection among vulnerabilities, controls, and assets, and the model grows as new sources of information, such as third-party scans, are added.

Xacta: 90 percent

time-savings in compliance and audit tasks – on-premises, in the cloud, and in hybrid / multi-cloud environments.

Cloud compliance doesn't have to be an exercise in frustration.

Xacta's unique capabilities for managing security risk in cloud, multi-cloud, and hybrid environments result in 90 percent time savings in compliance level-of-effort to help you achieve continuous audit readiness. With Xacta, your organization can reduce the number of working days your security team spends each year managing the audit process, free up budget to spend on growth, and acquire the ability to innovate without the risk of falling out of compliance.

Xacta reveals risk in real time and delivers proof of compliance with all major security standards for all types of environments. When you automate your cyber risk management capabilities, you can speed time to compliance and break the cycle of endless audit preparation so you can spend more time on digital transformation and strategic security assurance.

For more information, please contact us.

KTT

Ken Michaels
ken.michaels@kttechnologies.net
https://www.kttechnologies.net

publication number: 5690-0627-B