INTEGRATION OF XACTA AND MICROSOFT AZURE

Accelerating Security Compliance and Operational Approval

Abstract

As cyber threats continue to multiply, the enterprise IT staff face is required to prove systems under their control are safe to operate. In this paper, we explain how Microsoft and Telos are working together to streamline security compliance in Microsoft Azure.

Telos®

INTEGRATION OF XACTA AND MICROSOFT AZURE

Accelerating Security Compliance and Operational Approval

In the age of constantly increasing cyber threats, computing environments are subject to greater scrutiny than ever before. It is a significant challenge for IT staff to put in place the security controls necessary to prove the system is – and that it remains – safe and ready for operation.

In this paper, we explain how Microsoft and Telos are working together to leverage the Xacta® cyber risk management platform to automate and streamline security compliance in Microsoft Azure.

1. We begin with a brief look at the backstory behind IT security compliance, including the burden of reaching operational approval through cumbersome security rubrics.

2. We then consider how the cloud has complicated that effort while at the same time bringing with it the potential for collaborative compliance through the shared responsibility model of cloud security.

3. Finally, we examine how that potential is realized in deployments of Xacta that operationalize Azure features such as Azure Policy and Azure Blueprints with capabilities such as controls inheritance, control mapping, and recommended controls implementations (RCIs).

The goal of the Azure / Xacta integration is to compress the extensive amount of time it normally takes to achieve compliance by extracting busywork from the process, so systems can be authorized faster and customers can start gaining the benefits of the cloud sooner.

THE LONG ROAD TO AUTHORIZATION

The U.S. federal government calls it Authorization to Operate (ATO). In other industries and organizations, it may be referred to as operational approval, or simply security compliance. But whatever security regulation, framework, or standard you are beholden to, it all boils down to fundamentally the same thing – the need to provide a body of evidence to demonstrate compliance with defined information assurance (IA) controls.

The periodic assessment and authorization (A&A) required of U.S. federal government IT systems is well defined in NIST Special Publication 800-37 rev 2, which provides the roadmap for the Risk Management Framework (RMF). The federal government has also standardized on the IA control catalog from NIST Special Publication 800-53 Rev5, which expands the catalog to just over a thousand controls. That number may seem overwhelming, but the controls are well organized into logical categories. With the right

guidance, implementing the RMF is not only doable, but very beneficial, regardless of industry. SP 800-53 Rev 5 also offers new guidance for security of cloud-based systems and serverless architectures.

The government's ATO process was originally intended to be a check on security due diligence, required before any system processed live data. Unfortunately, as originally implemented years ago, this compliance check would be the last gate before a system went live, so system operators would have to work backwards to explain what they had done from a security perspective in standing up the system. This process typically took from six months to two years, causing huge delays in system deployments.

The Xacta cyber risk management solution turns that process on its head by automating much of the compliance process. Teaming with cloud providers such as Microsoft Azure takes this concept to the next level.

COMMERCIAL SYSTEM OPERATORS SEE THE LIGHT

Many organizations beyond the federal government have come to recognize the need for rigorous internal security audits and system approvals, and the government and commercial processes bear many similarities. Whether based on NIST publications or some other standard or framework for commercial environments, from financial services to the field of medicine, the baseline is relatively the same. The system operator needs to establish that:

- They've done the due diligence of establishing a security profile and a secure system build;
- A qualified entity has performed a rigorous evaluation;
- The evaluation has been sufficiently documented;
- Security methodologies and the security practices and best principles within the system architecture are well defined and established; and
- The system's operations follow through with the defined security processes and procedures.

That's what it takes to get from assessment to authorization, and thus to an operational environment that supports the real work the system was intended for.

ENTER THE CLOUD

It can be extremely difficult to garner documentation from the internal operations of a cloud provider. Such compliance documentation must be maintained to keep it relevant in an ever-changing hyperscale elastic cloud, where updates, patches, and operations are taking place in near real time. **Security too must be a real-time activity**.

Taking a security snapshot during an assessment is no longer good enough. Rather, a system provider must build a secure architecture so that when the time comes to perform an assessment, that baseline of security is already in place. And operationally, that same baseline should be leveraged to build the security rigor – the policies, the procedures, and the architecture – necessary for continuous monitoring.

Microsoft Azure is gearing its infrastructure to have continuous assessments, continuous monitoring, and continuous risk evaluation, with that information displayed in an ongoing fashion to those who do the evaluation, maintain the systems, and perform the assessments – everyone from the security engineer to the IT security officer to the authorizing official. The paradigm is shifting from the old school pound-of-paper snapshot in time – a single assessment with yearly reassessments – to a living process that's better suited to the scalability and elasticity of the cloud.

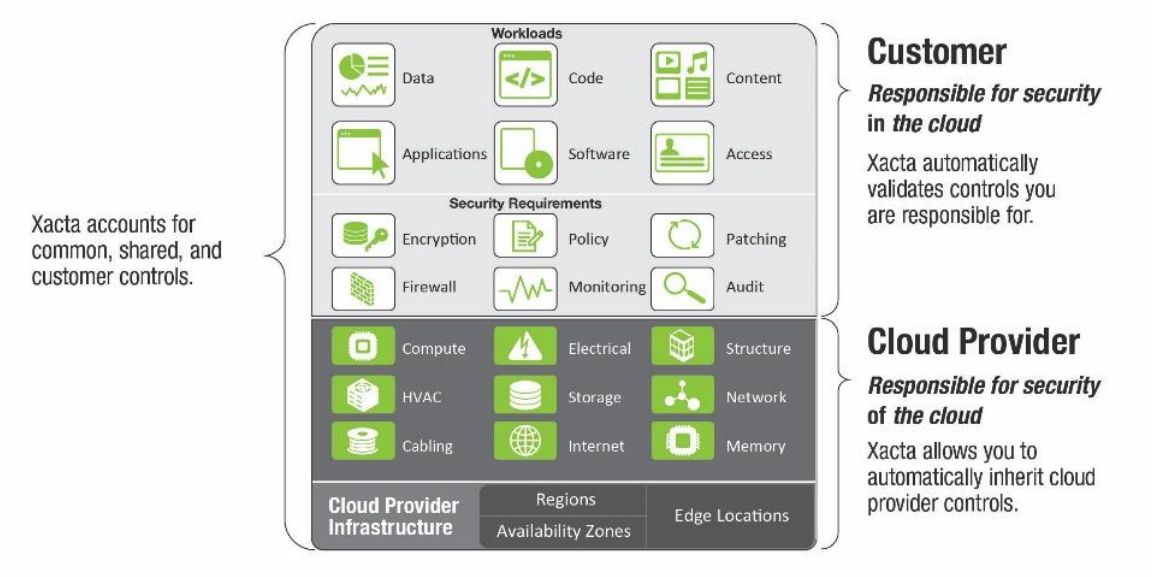
A shortfall of the classic monitoring process has been that the architectures and security controls were written for a client-server or other large-scale network infrastructure that was built and then incrementally upgraded over time. An elastic cloud architecture allows for resources to be provisioned on the fly; systems are stood up and torn down as needed based upon resource allocation and utilization**. A cyber risk management solution that can dynamically expand and contract with the cloud** is a key component to establishing security in the long term. This is the driving force behind the tight integration of Xacta and Azure.

SHARED RESPONSIBILITY FOR CLOUD SECURITY

While a cloud provider such as Microsoft Azure manages security *of* the cloud, security *in* the cloud remains the responsibility of the customer. It is critical not only to understand the difference between what aspects of security the cloud provider handles and which the customer is responsible for, but to have access to resources to meet those responsibilities. The integration of Xacta and Azure ensures this information is documented and available to customers as they roll workloads onto the cloud and that certain controls can be shared or inherited.

When standing up a cloud instance, the customer is faced with a number of configuration decisions. As part of the Xacta / Azure integration, customers receive configuration guidance in order to meet the intent of security controls given their specific requirements. These suggested configurations leverage Azure Policy and Azure Blueprints to provide a clear understanding of responsibilities, which traditionally would have required a deep background in IA controls.

Regardless of regulation or framework concerned – NIST-based, ISO, PCI-DSS, HIPAA, and others – the parties have a clear understanding of the work for which they are responsible. Everyone must understand where the cloud provider's responsibility ends and the customer's begins.



A FRESH APPROACH TO CLOUD SECURITY AND SECURITY COMPLIANCE

The integration of Xacta and Azure is a key component to delivering security capabilities as part of cloud operations so customers can evaluate security controls, establish risk baselines, and monitor the risk of the environment and the individual systems within that environment.

Microsoft has always been a classic technology solution developer, building tools, systems, and software. They apply the same methodology to cloud services provisioning and security requirements. Encryption policy, patching, auditing, monitoring, and boundary protection are built into the software as a service (SaaS) fabric. Microsoft is able to ensure the effective application of those capabilities because the majority of the services that Azure provides are integrated within the architecture.

INTEGRATING XACTA FOR CYBER RISK MANAGEMENT

Such native Microsoft tools have a much greater impact when combined with Xacta, offering a roll-up view of security. A security engineer can see into the operating systems, the storage and compute environments, and the database capabilities, and can influence the adoption of security control-based plans, provisions, and profiles needed to evaluate the risk of the system.

Xacta was launched in 2000, the first web-based risk management and compliance solution on the market. Originally designed for on-premises systems, it has been re-engineered over the last five years to operate in cloud infrastructures, automating elements of the cloud, pulling in resources, and leveraging cloud scalability. In an environment where servers are spun up and retired according to real-time requirements, security boundaries need to adjust quickly, even automatically.

***Policy** – Ability to enforce rules and effects on Azure resources in order to stay in compliance with standards and requirements*

***Blueprints** – Bundle of policies, e.g. NIST 800-53 Blueprint*

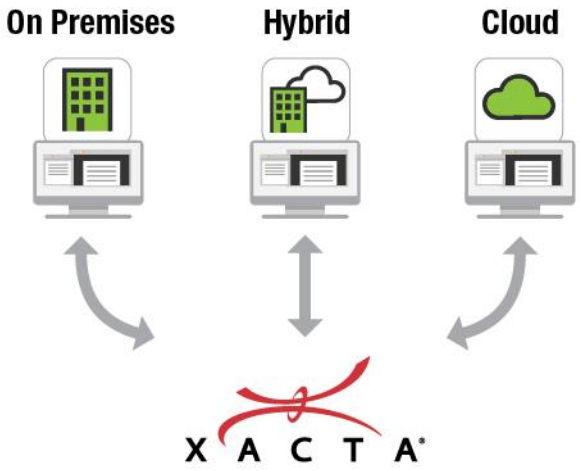
***Azure** executes policy scans to determine if the resources pass or fail policy rules*

***Xacta** queries Azure for policy status, which is in turn translated to test results*

Xacta manages the entire risk and compliance process, pulling data from its HostInfo Agent as well as from third-party software – and now the Azure APIs – at an interval defined by the system owner. It then runs compliance validations in an automated fashion. And, Xacta provides a centralized repository of inventory and compliance data with strict, role-based access control.

EVIDENCE-BASED COMPLIANCE

Xacta also works within Azure to automate the generation of the body of evidence (BoE) necessary to prove compliance. This is particularly valuable for organizations that must comply with multiple security standards, such as the NIST frameworks, PCI-DSS, HIPAA, ISO, and Sarbanes-Oxley. Xacta includes an advanced controls mapping capability that gives organizations the ability to test against the high bar, and then map it automatically against other standards to produce the BoE necessary for each. Such continuous monitoring of the high-bar standard, combined with controls mapping to other standards, greatly simplifies ongoing compliance across the board.

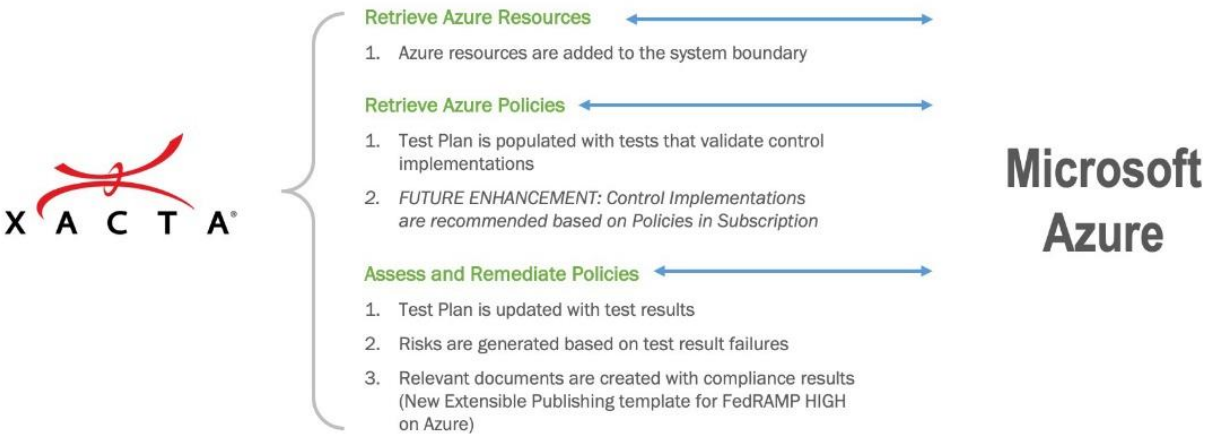


Xacta facilitates a system accreditation not just in a hyperscale cloud configuration; it optimizes for on-premises, hybrid, or multi-cloud environments as well. The goal of the Xacta / Azure integration is to support the customer no matter the requirement. Whether an entire system moves into Azure, there is a portion that needs to operate on-premises, or even a piece that needs to operate in another vendor's cloud, Xacta and Azure security capabilities can be leveraged to feed a risk profile and provide the data for informed risk decisions.

How the Azure / Xacta integration works

Azure Subscriptions are accounts that hold all resources used by the Azure customer. Xacta queries the subscription and retrieves Azure resources via the Azure Resource Manager API. Azure resources are added to the system boundary based on user selection.

The Azure Policy API, called Azure Policy Insights, is queried to return all policies tied to the subscription and resources. The policies contain all of the tests, mapped controls, and test results associated with each resource. The test plan is populated with tests that validate control implementation and updated with test results. Risks are generated based on test results.



Xacta maintains an inventory of subscription resources and collects cloud resource information from Azure. Through the Azure API, Xacta is able to scan a subscription and see all of its resources. As resources scale up or down, the system owner is made aware of the changes being made inside of the subscription. They then have the ability to add them to a system or security boundary or choose not to.

Xacta is also able to retrieve policies to automatically populate test plans. Xacta provides control implementations as a function of the policies selected in a subscription. Azure provides configuration guidance and suggestions, giving the customer the ability to run their workloads in a configured manner that meets the intent of the control.

When resources are synched, Xacta makes a call to Azure's Policy Insights API to pull back all currently running resources in the selected Azure subscriptions. The user can select which resources should be included in the system boundary and include them for testing. Users can also assign resource roles in order to execute certain cloud tests against those resources.

The test plan is updated not only with control implementations, but actual test results. As those policies are validated in Azure, Xacta pulls that data in, showing automatic test passes and fails in the Xacta instance, making it clearly visible whether a system is running in a compliant manner or not.

A TEAM APPROACH TO SHARED RESPONSIBILITY

Although it's important that the cloud provider and customer understand who owns responsibility for which controls, the authorization process is truly an integrated team effort. Microsoft has assumed a forward-leaning approach to this, assuming responsibility for any control that can be addressed within the cloud and providing recommendations about best practices, policies, and procedures to help answer the remaining requirements. The objective is to ensure the customer can achieve their security goals.

> *"One of our core tenets at Microsoft is our customer focus. If the customer has a stop gap or a roadblock that needs to be overcome, then the compliance team works with the customer interface team to get it taken care of... We will work with anyone anywhere to solve their accreditation problems."*
>
> *- Richard Scher*
> *CISO for High Security Clouds, Microsoft*

Addressing encryption controls, for example, depends on how encryption is handled in the infrastructure, in the fabric, and on the trunk lines. Azure makes recommendations for services, best practices, and procedures that leverage those encryption security standards and capabilities for cloud-based systems. This is key to helping customers get faster adoption and faster authorizations.

This is where Azure Policy and Azure Blueprints are so effective. If a system owner is implementing the NIST RMF and struggling with the Prepare, Categorize, Select, or Implement steps, a blueprint will help define what the system's control sets are going to be. A manager of a tenancy or the manager of an enterprise cloud migration can leverage policies and blueprints to set guardrails, identifying, for example, what systems are allowed to be launched and how the systems are configured. These Azure resources are being mapped into Xacta so that a capability provided in Azure can be consumed by Xacta, thus giving the customer access not only to the service, but to the accreditation process for that service as well.

Xacta's recommended controls implementations (RCIs) provide a rich understanding of controls and how they need to be configured. They help the system owner interpret this information and apply it to numerous compliance hurdles.

The intent is to make it as simple as possible for the end user by selecting the appropriate blueprint and associated policies. Xacta scans an Azure subscription to identify resources for the boundaries. Azure common control providers (CCPs) satisfy many controls. But the RCIs are the game changer – suggesting an appropriate way to configure to meet the full intent of the controls.

Software engineers and developers can spend months and even years building a system in the cloud and working on its assessment and authorization, all without gaining the benefits of actually using the system for its intended purpose. The goal of the Azure / Xacta integration is to drive that timeline down so that the time between initiating cloud services and getting utility out of those services is as short as possible. Microsoft and Telos, in a combined effort, are shrinking those timelines for customer adoption of the cloud and the authorization to begin productive work.

To learn more information and to discuss how Xacta and Azure can work together to accelerate the benefits of the cloud for your, please visit **www.telos.com/azure** or contact Telos at 703.724.3800.

Version 1.0
November 2020