ALERT LOGIC®

# COMPLIANCE CHECKLIST
## WHEN USING MICROSOFT AZURE

Compliance workloads are often kept on-premises as they are perceived as too difficult to deploy in, or migrate to, the cloud. However, we at Alert Logic have seen several SaaS and eCommerce customers with compliance requirements who have made the leap to the cloud without much difficulty, and are now benefiting from the investments the cloud platform providers are making, and the new controls they are putting in place.

Microsoft Azure has secured multiple attestations for compliance frameworks across industry groups, regulatory organizations, and even sovereign requirements, such as data residency. This checklist can help you understand how using Microsoft Azure can help you meet your requirements, and scope your regulated workload to the cloud.

### 1 STEP 1: UNDERSTAND HOW MICROSOFT AZURE SERVICES MAP TO VARIOUS COMPLIANCE FRAMEWORKS AND CONTROLS

First, identify all of the Azure services your application or service will use. This includes VMs and Storage Services, but may also include Azure SQL, HDInsight, or Event Hubs depending on how you ingest, store, and analyze sensitive information as part of your application. If you are using App Services, where Microsoft manages your underlying VMs and network, you will have to rely on Microsoft to meet any requirements that are tied to those components. This is one of the major differences between Platform-as-a-Service (PaaS) deployments and traditional Infrastructure-as-a-Service (IaaS) deployments. For IaaS, you have more control, but you also have increased responsibility for managing those assets.

Once you have identified the services, you can use Microsoft's Trust Center to build out the compliance worksheet, and clarify which controls you are responsible for and which ones are addressed by Microsoft. You can read more about this service by visiting: https://azure.microsoft.com/en-us/blog/microsoft-common-controls-hub-provides-uncommon-convenience/

### 2 STEP 2: REDUCE THE COMPLIANCE FOOTPRINT AND SEPARATE THOSE SERVICES FROM THE REST

Once you understand how the various Azure services map to compliance requirements and controls, you can start looking for ways to minimize the services touching sensitive data and maximize the benefit of using those services based on the attestations Microsoft has already secured.

The next step is to separate the compliance related services and infrastructure from the rest of your application and implement controls only for those specific assets. You can read more about how Microsoft IT aligned security controls for ISO 27001 by visit this link

In addition to implementing additional security controls, you should implement role-based access control and implement more granular access control policies to these resources. This helps ensure the configurations are safe from accidental changes and protected if an employee's or contractor's credentials are compromised.

## 3 STEP 3: EVALUATE SECURITY VENDORS AND OFFLOAD RESPONSIBILITIES WHEN POSSIBLE

Check to see if your security solution providers have their own attestations or reporting capabilities to simplify audit processes. Offloading this work helps reduce overhead on your teams, streamline your audit processes, and save you money.

## 4 STEP 4: REVISE YOUR METRICS

By leveraging the capabilities provided by your cloud platform service provider and security partners, your team can focus on the remaining requirements not included as part of their platform. This includes business processes and implementing other controls and security solutions. By focusing on fewer requirements, your team can implement a more proactive auditing strategy to ensure these environments are protected and the sensitive information is secure.

Many teams focus on getting through their scheduled audits before measuring their efficiency. However, there are several capabilities available in the cloud that enable better security and improved visibility into what is happening in their environment. For example, the Azure Activity Logs capture every API call made to the Azure Resource Manager (ARM), enabling your team to review every action and configuration setting for your environment. There are also several tools to help monitor your environment and alert on changes, making it easier to identify suspicious activity. These capabilities are not necessarily available in on-premises environments where most of the security initiatives focus on the perimeter.

*Here are some metrics you may want to start tracking:*

- Time to complete an audit
- Time to identify a compromise or attack
- Time to complete analysis of data access to determine whether sensitive data was accessed or exfiltrated

## CONCLUSION

Cloud platform service providers can not only help your organization lower IT costs, increase agility, and expand reach, they can also help reduce the costs and complexity of meeting compliance requirements. You will need to review the attestations of the cloud platform service provider and your security vendors to understand what they can cover and what you are still responsible for. It is always good to limit the resources that can access sensitive data, separate them from the rest of your environment, and minimize access to those resources. Finally, implementing more proactive security monitoring and revising your metrics to measure the effectiveness of your team will help ensure this data is protected and your audits go smoothly.

## HELPFUL LINKS

**Microsoft Attestations** https://www.microsoft.com/en-us/trustcenter/cloudservices/azure

**Microsoft Common Controls Hub** https://www.microsoft.com/en-us/trustcenter/Common-Controls-Hub

**How to Use the Microsoft Compliance Guidance** https://www.microsoft.com/en-us/trust-center/compliance/compliance-overview

**Azure Identity Management and access control security best practices** https://docs.microsoft.com/en-us/azure/security/azure-security-identity-management-best-practices

**Overview of the Azure Activity Log** https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-activity-logs



ALERT LOGIC®