!mpactmakers

Better Business. Better Community.

Compliance & Security in Azure

April 21, 2018

Presenter Bio

Jeff Gainer, CISSP

- Senior Information Security & Risk Management Consultant
- Senior Security Architect

- Have conducted multiple Third-Party risk assessments of cloud platforms including Office 365 and Azure

Session Agenda

Compliance

- How Microsoft goes about their process
- Shared responsibility model for cloud computing
- How you go about the process

Security Controls

- What are security controls
- Use of Azure Security Blueprints to help
- Security architecture walkthrough

01 | Compliance

Compliance – Before We Get Started

Compliance in this context means conforming to a set of requirements that have been determined by a governing body

Quick Survey to the Group….By a Show of Hands

WHO HAS A COMPLIANCE REQUIREMENT TO INCLUDE IN YOUR TECHNOLOGY DEPLOYMENT, SUCH AS HIPAA/HITECH, PCI-DSS, FFIEC, GLBA, ETC?

WHO HAS BEEN TOLD YOU CAN'T MOVE THAT SAME TECHNOLOGY TO THE CLOUD BECAUSE OF IT?

Compliance – How Microsoft goes about the process

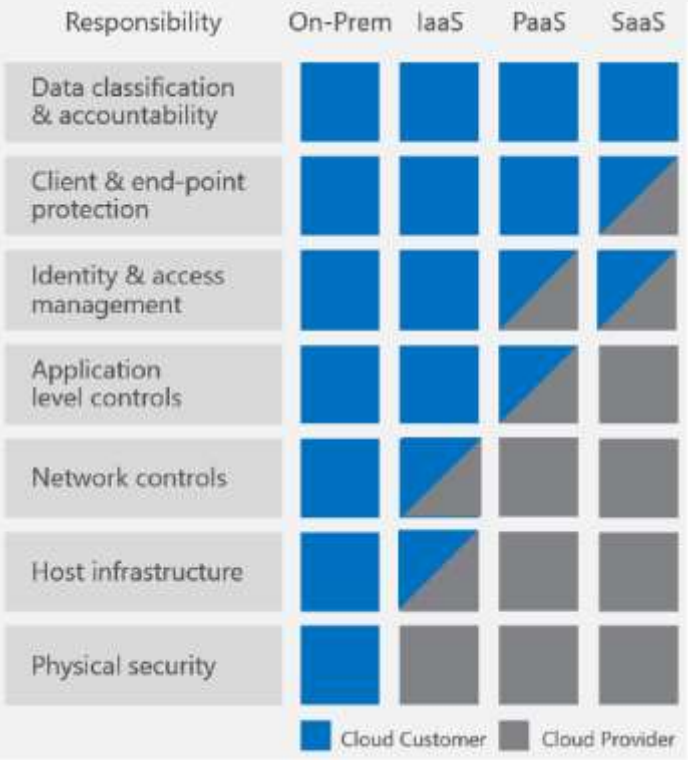
Azure compliance offerings are grouped into four segments:

Globally Applicable	US Government	Industry	Region/Country
▪ CSA STAR (3) ▪ ISO 20000-1:2011 ▪ ISO 22301:2012 ▪ ISO 27001:2013 ▪ ISO 27017:2015 ▪ ISO 27018:2014 ▪ ISO 9001:2015 ▪ SOC 1 Type 2 ▪ SOC 2 Type 2 ▪ SOC 3 ▪ WCAG 2.0 (ISO 40500:2012)	▪ CJIS ▪ DFARS ▪ DoD DISA SRG Level 2 / 4 / 5 ▪ DoE 10 CFR Part 810 ▪ EAR ▪ FedRAMP Moderate / High ▪ FIPS 140-2 ▪ IRS 1075 ▪ ITAR ▪ NIST Cyber Framework (CSF) ▪ NIST SP 800-171 ▪ Section 508 VPATs	▪ 23 NYCRR 500 ▪ CDSA ▪ FERPA ▪ FFIEC ▪ GLBA ▪ GxP (21 CFR Part 11) ▪ HIPAA and the HITECH Act ▪ HITRUST ▪ MARS-E ▪ PCI DSS Level 1 ▪ Shared Assessments ▪ Sarbanes Oxley (SOX) ▪ 8 Other International Regs	▪ Argentina ▪ Australia ▪ Canada ▪ China (3) ▪ EN 301 549 ▪ EU / UK (6) ▪ Germany (2) ▪ India ▪ Japan (2) ▪ Netherlands ▪ New Zealand ▪ Singapore ▪ Spain (2)

- ❑ Compliance Reports — Includes SOC & ISO Reports, FedRAMP and Various Assessment Reports
- ❑ Trust Documents — Includes FAQs, White Papers, Pen Test Results, and Compliance Guides for the list of services approved to use for each Compliance requirement

Compliance – Shared responsibility model

Cloud computing requires that the cloud service provider (CSP) and customer be responsible for the security and operation of certain layers of the cloud offering based on the cloud model.



- **On-Prem**: Customer is both accountable and responsible for all aspects of security and operations.
- **IaaS**: The CSP manages buildings, servers, networking hardware, and hypervisor layers. The customer is responsible for securing and managing the operating system, network configuration, applications, identity, clients, and data.
- **PaaS**: The CSP owns the IaaS layers and is additionally responsible to manage and secure the network controls along with some application and identity controls . The customer is still responsible for securing and managing applications, identity, clients, and data.
- **SaaS**: The CSP provides the application to the customer. The customer continues to be accountable to ensure that data is classified correctly, along with managing their users and end-point devices.

Azure is responsible for security ***of*** the cloud, while the customer is responsible for security ***in*** the cloud.

Compliance – How you go about the process

Performing a compliance due diligence review for Azure

1. Determine which regulation influencers are in scope for the technology deployment.
2. Acquire the Microsoft Azure Compliance Offerings document from the Microsoft Service Trust Portal.
3. Identify the in scope regulations in the document and identify the available Azure artifacts to be used for the assurance review.
4. Confirm that the services in your planned Azure architecture are in scope of the Azure Compliance Offering. If not included, then may need to rearchitect with in scope services or determine the risk of non-compliance for your organization.
5. Perform the compliance assurance due diligence review using the Azure Compliance Offering artifacts to identify any compliance gaps in the Azure platform.

02 | Security Controls

Security Controls to Support Compliance

Security controls are safeguards used to prevent, detect, and respond to security risks to physical property, information, systems, or other assets.

- A set of techniques that address many of the various compliance requirements
- Available as a framework or catalog of controls:
  - ISO 27002:2013 – Code of Practice for Information Security Controls
  - NIST SP800-53r5 – Security and Privacy Controls for Federal Systems & Organizations
  - CIS - 20 Critical Security Controls

- Access Control
- Awareness and Training
- Audit and Accountability
- Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environment Protection
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Communication Protection
- System and Information Integrity

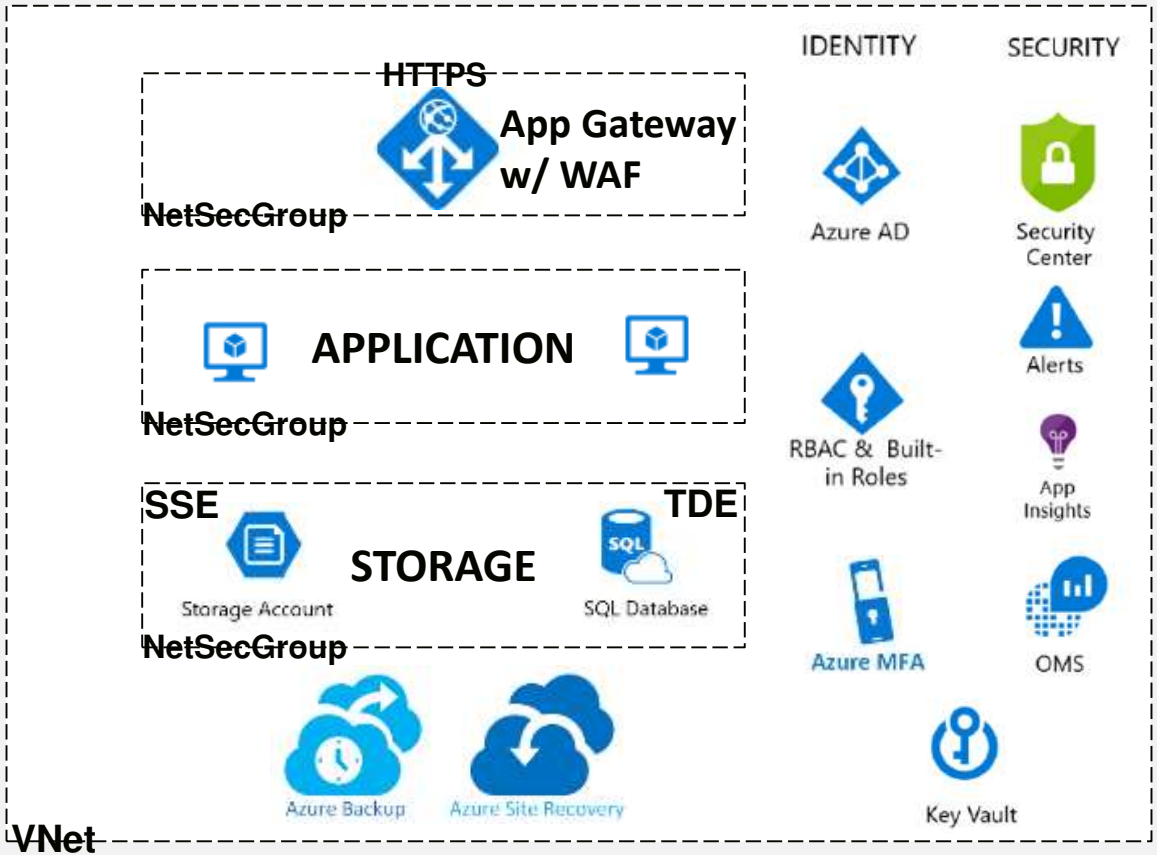
Security Controls Using Azure Services

Azure offers Compliance Blueprints for some of the more popular regulations that describe the shared responsibility model and use of Azure Security Services to address them:

- US Department of Defense (DoD)
- FedRAMP
- FFIEC Cybersecurity Standard
- Healthcare (HIPAA and HITRUST)
- NIST Cybersecurity Framework (CSF)
- PCI Data Security Standard (PCI-DSS)
- UK National Cyber Security Centre (NCSC)

It's All About Protecting Data and Controlling Access with Proactive Monitoring

Security Controls Using Azure Services



Security Controls Addressed:

- Access Control
- Audit & Accountability
- Configuration Management
- Contingency Planning
- Identification & Authentication
- Incident Response
- System & Communication Protection
- System & Information Integrity

Summary

- Azure realizes that to gain and retain customers, they need to be regulation ready.
- There is a comprehensive approach in addressing the compliance need.
- Compliance and security is a shared responsibility between Azure and the customer.
- Not all Azure services may be compliant to every regulation yet.
- Many security controls expected to address regulations can be achieved within the platform.

Key Resources for use in compliance and security efforts include:

- Service Trust Portal (STP)
- Regulation Specific Shared Responsibility Matrices
- Azure Compliance Blueprints