



Achieving Compliance on Microsoft Azure

Gururaj Pandurangi

Frank Simorjay

1

Introductions & Poll

We ask...

2

Achieving Compliance on Azure

A Theoretical View

3

Solution Overview

Walkthrough of the jointly developed solution

4

Q & A

You ask...



Introductions



Gururaj Pandurangi

Founder & Partner

- [Avyan Consulting Corp](#) – cloud consulting services
- [Cloudneeti](#) – An Azure marketplace product for Continuous Governance & Compliance of Azure Assets



gururajp@avyanconsulting.com



Microsoft
Partner
 Microsoft

AZURE PARTNER

Avyan is an [Azure Circle Partner](#)



Frank Simorjay

Sr. Program Manager (Azure Global Ecosystem)

CISSP, ISSA Distinguished Fellow

is a Microsoft cloud security and compliance subject matter expert.

- [Publications](#)



Frank.Simorjay@microsoft.com



Microsoft

How many of you...

Are using Microsoft Azure to build your apps/services?

Have you had to work with an auditor?

Have you stored, managed, handled payment card / Patient health data ?

Would not raise your hands no matter what is being polled?



Azure PaaS – PCI and HIPAA Validated Blueprint

Jointly developed and presented by



Avyan
Consulting Corp



Microsoft



Problem Statement

[Customers / Partners] How to achieve and manage compliance on Azure?



Business Decision Maker

How should I go about achieving and managing compliance on Azure?

E.g. Specific Initiatives and Governance Plans



IT Decision Maker

What should my team and I be doing across SDLC phases?

E.g. proven architectures, accelerators, checklists, trainings etc.



IC Engineering / Operations

What and **How** and do I keep my specific infrastructure and services compliant?

E.g. Architecture, Configurations, 1st and 3rd party choices etc.



Azure has the most comprehensive compliance coverage in the industry

Global



- ✓ CSA STAR Attestation
- ✓ CSA STAR Certification
- ✓ CSA STAR Self-Assessment
- ✓ ISO 22301
- ✓ ISO 27001
- ✓ ISO 27017
- ✓ ISO 27018
- ✓ SOC 1 Type 2
- ✓ SOC 2 Type 2

U.S. Government



- ✓ CJIS
- ✓ DoD DISA SRG Level 2
- ✓ DoD DISA SRG Level 4
- ✓ DoD DISA SRG Level 5
- ✓ FedRAMP
- ✓ FIPS 140-2
- ✓ High JAB P-ATO
- ✓ IRS 1075
- ✓ ITAR
- ✓ Moderate JAB P-ATO
- ✓ Section 508 VPAT
- ✓ SP 800-171

Industry



- ✓ CDSA
- ✓ FACT UK
- ✓ FERPA
- ✓ FFIEC
- ✓ FISC Japan
- ✓ GLBA
- ✓ GxP 21 CFR Part 11
- ✓ HIPAA / HITECH
- ✓ HITRUST
- ✓ IG Toolkit UK
- ✓ MARS-E
- ✓ MPAA
- ✓ PCI DSS Level 1
- ✓ Shared Assessments

Regional



- ✓ Argentina PDPA
- ✓ Australia IRAP/CCSL
- ✓ Canada Privacy Laws
- ✓ China DJCP
- ✓ China GB 18030
- ✓ China TRUCS
- ✓ ENISA IAF
- ✓ EU Model Clauses
- ✓ EU-US Privacy Shield
- ✓ Germany IT Grundschutz
- ✓ India MeitY
- ✓ Japan CS Mark Gold
- ✓ Japan My Number Act
- ✓ New Zealand GCIO
- ✓ Singapore MTCS
- ✓ Spain DPA
- ✓ Spain ENS
- ✓ UK G-Cloud

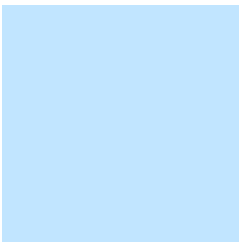
Cloud Services – Shared Responsibility


















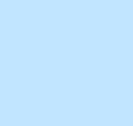


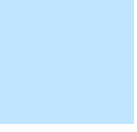
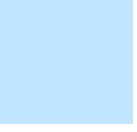


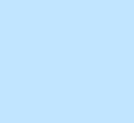
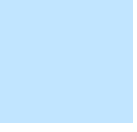

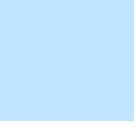


Customer management of risk
Data Classification and data accountability



Shared management of risk
Identity & access management | End Point Devices



Provider management of risk
Physical | Networking

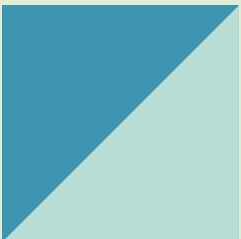
Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification and accountability				
Client & end-point protection				
Identity & access management				
Application level controls				
Network controls				
Host Infrastructure				
Physical Security				



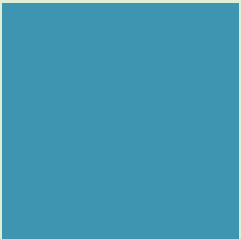
Cloud Services – Shared Responsibility



Customer management of risk
Data Classification and data accountability



Sh
Iden



Provider management of risk
Physical | Networking

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification and accountability				
Client & end-point protection				
Network controls				
Host Infrastructure				
Physical Security				

Customers of Microsoft Azure are ultimately responsible for their own compliance.
<http://Aka.ms/sharedresponsibility>



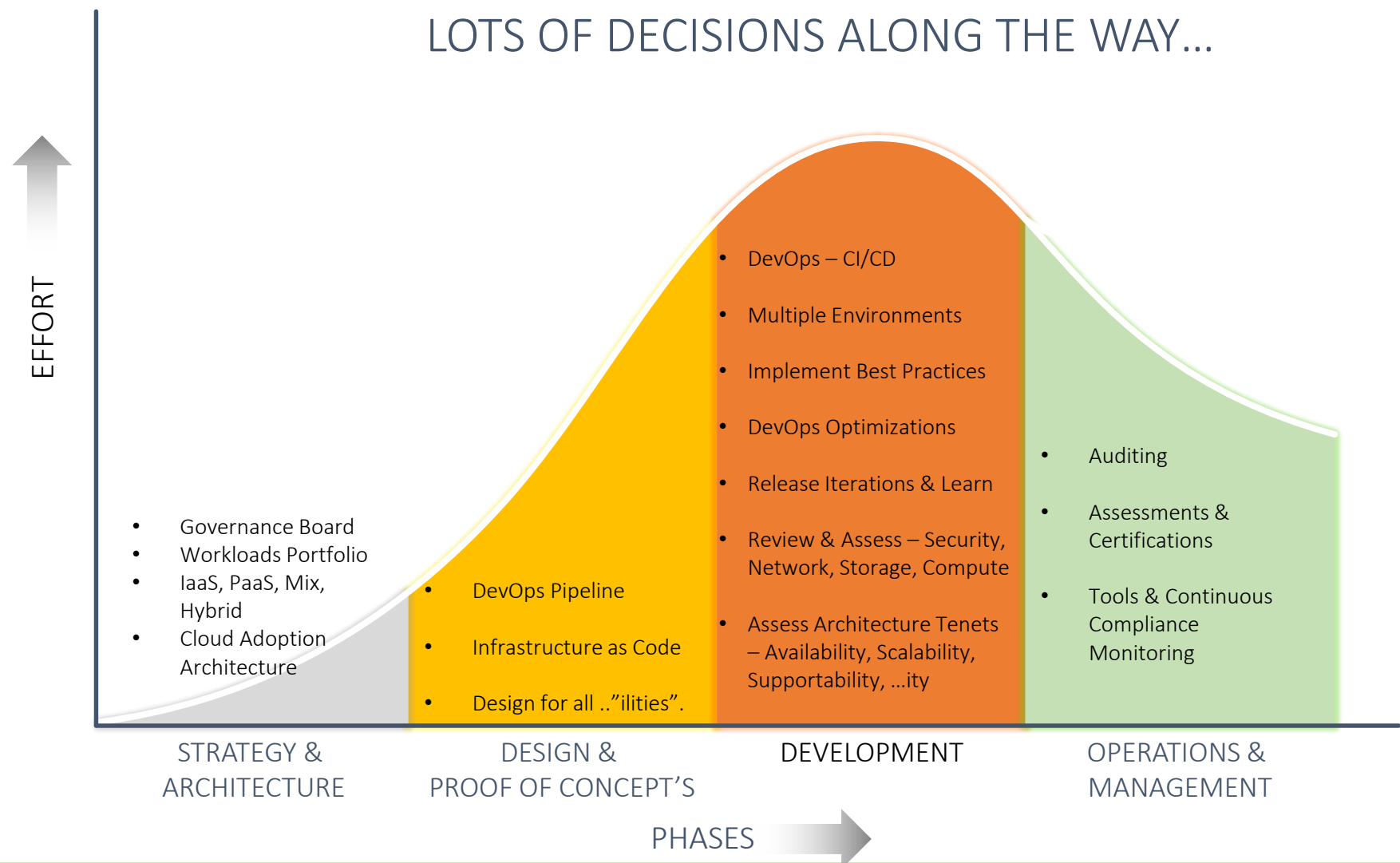
Security and Compliance Standards – High Level Overview

Principles	Standards
Build and Maintain a Secure Network and Systems	1 Install and maintain a firewall configuration
	2 Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Data in transmission and at-rest	3 Protect stored data
	4 Encrypt transmission of data across open, public networks
Maintain a Vulnerability Management Program	5 Protect all systems against malware and regularly update anti-virus software or programs
	6 Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7 Restrict access to data by business on a need to know basis
	8 Identify and authenticate access to system components
	9 Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10 Track and monitor all access to network resources and data
	11 Regularly test security systems and processes
Maintain an Information Security Policy	12 Maintain a policy that addresses information security for all personnel

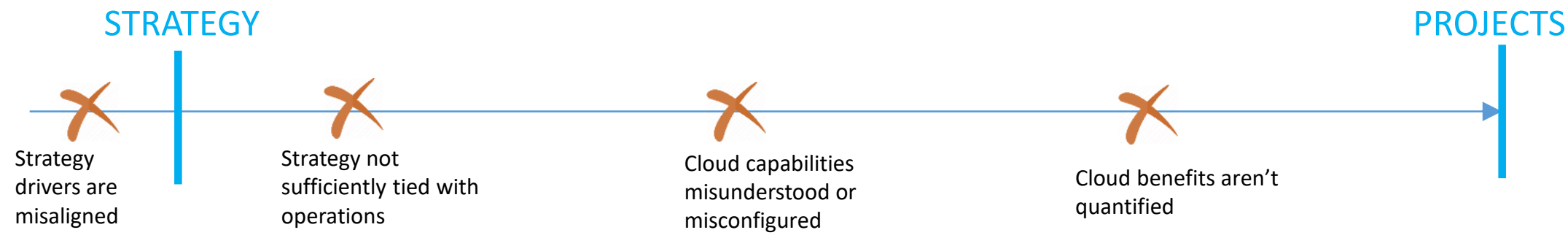


Achieving compliance in the cloud

HIGH LEVEL OVERVIEW ACROSS THE PROGRAM PHASES



... Leading to failure points between strategy and implementation phases



Is my cloud infrastructure compliant?

Are my applications configured for high availability?

Is my cloud spend controlled?

Can I tell who's changing what?

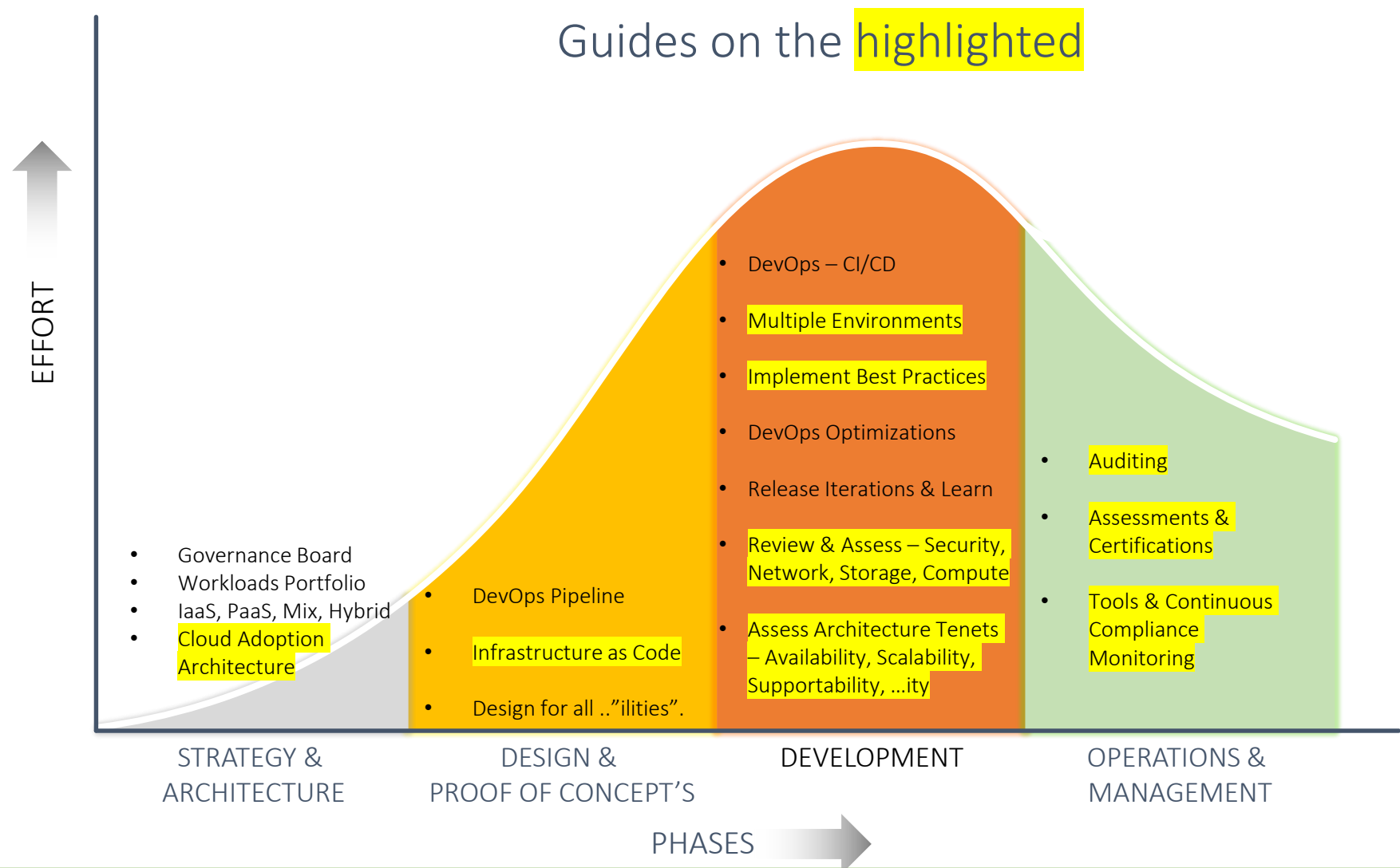
Is my application secure?



Solution

What if.. ?

A blueprint is available that already ...



What if ...?

there was...



Business Decision Maker



Guidance



Pre-Attested
Solution



Information Technology
Decision Maker

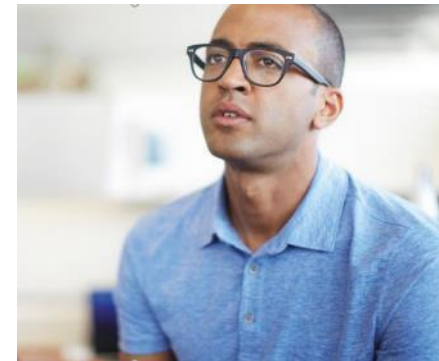


Scenarios



Reference
Architecture

- Covering Workload, Security, Compliance,
Auditing etc.



IC Engineering / Operations



1-click deploy



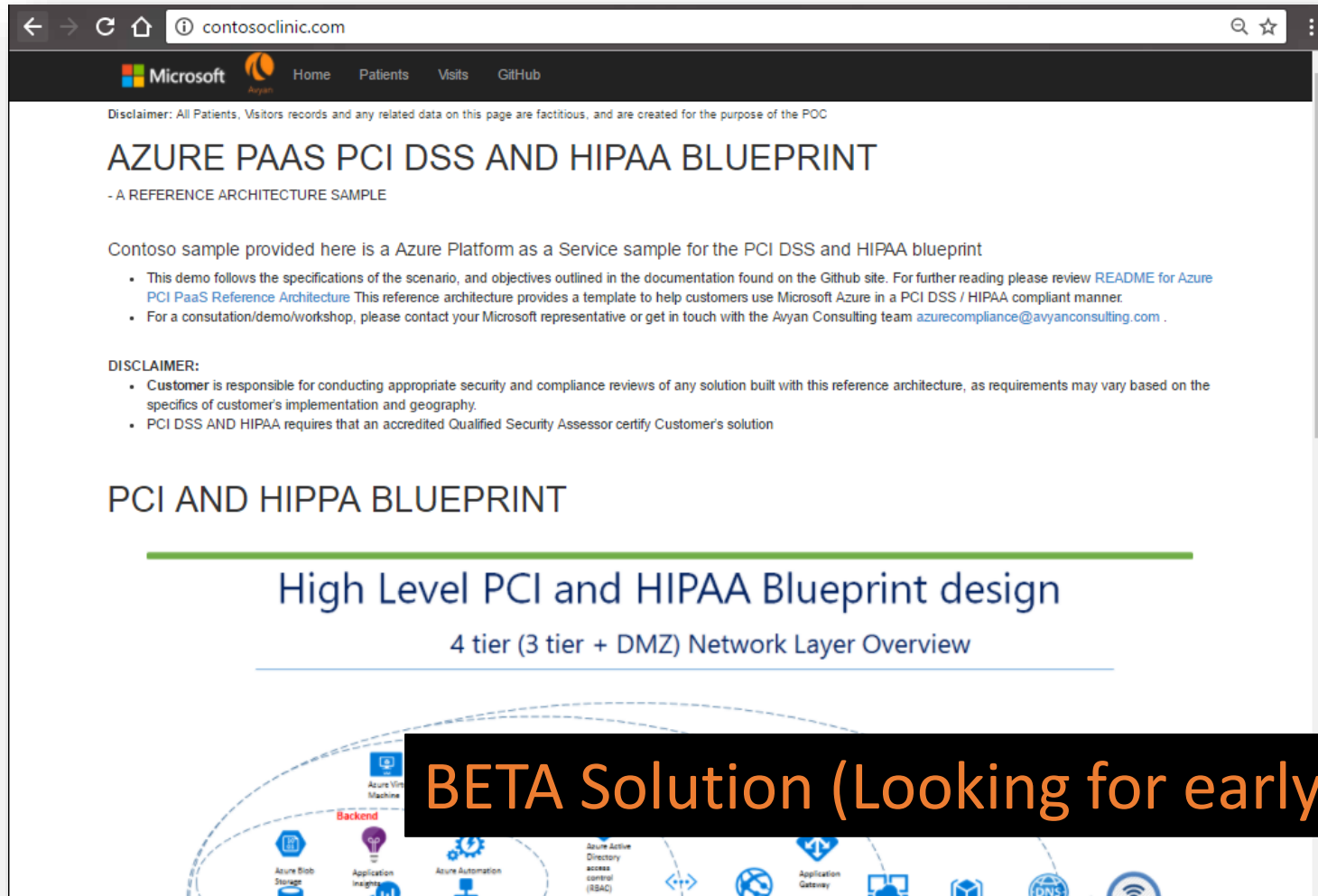
Configurations



There is...

All of it and much more., available here

<https://contosoclinic.com>



The screenshot shows a web browser window with the URL contosoclinic.com. The page features a Microsoft and Avyan logo in the header, with navigation links for Home, Patients, Visits, and GitHub. A disclaimer states that all data is fictitious. The main heading is "AZURE PAAS PCI DSS AND HIPAA BLUEPRINT" with a subtitle "- A REFERENCE ARCHITECTURE SAMPLE". The text describes the demo as an Azure Platform as a Service sample for PCI DSS and HIPAA compliance. It includes a list of bullet points: "This demo follows the specifications of the scenario, and objectives outlined in the documentation found on the Github site. For further reading please review [README for Azure PCI PaaS Reference Architecture](#) This reference architecture provides a template to help customers use Microsoft Azure in a PCI DSS / HIPAA compliant manner." and "For a consultation/demo/workshop, please contact your Microsoft representative or get in touch with the Avyan Consulting team azurecompliance@avyanconsulting.com". A "DISCLAIMER:" section follows, stating that the customer is responsible for security and compliance reviews, and that PCI DSS AND HIPAA requires certification by a Qualified Security Assessor. Below this is a section titled "PCI AND HIPPA BLUEPRINT" with a green horizontal line, followed by "High Level PCI and HIPAA Blueprint design" and "4 tier (3 tier + DMZ) Network Layer Overview" with a blue horizontal line. At the bottom, a diagram shows various Azure services like Azure Blob Storage, Azure Active Directory, and Azure Automation. A large black banner with orange text "BETA Solution (Looking for early adopters)" is overlaid on the bottom right of the screenshot.

Microsoft Avyan Home Patients Visits GitHub

Disclaimer: All Patients, Visitors records and any related data on this page are fictitious, and are created for the purpose of the POC

AZURE PAAS PCI DSS AND HIPAA BLUEPRINT

- A REFERENCE ARCHITECTURE SAMPLE

Contoso sample provided here is a Azure Platform as a Service sample for the PCI DSS and HIPAA blueprint

- This demo follows the specifications of the scenario, and objectives outlined in the documentation found on the Github site. For further reading please review [README for Azure PCI PaaS Reference Architecture](#) This reference architecture provides a template to help customers use Microsoft Azure in a PCI DSS / HIPAA compliant manner.
- For a consultation/demo/workshop, please contact your Microsoft representative or get in touch with the Avyan Consulting team azurecompliance@avyanconsulting.com.

DISCLAIMER:

- Customer is responsible for conducting appropriate security and compliance reviews of any solution built with this reference architecture, as requirements may vary based on the specifics of customer's implementation and geography.
- PCI DSS AND HIPAA requires that an accredited Qualified Security Assessor certify Customer's solution

PCI AND HIPPA BLUEPRINT

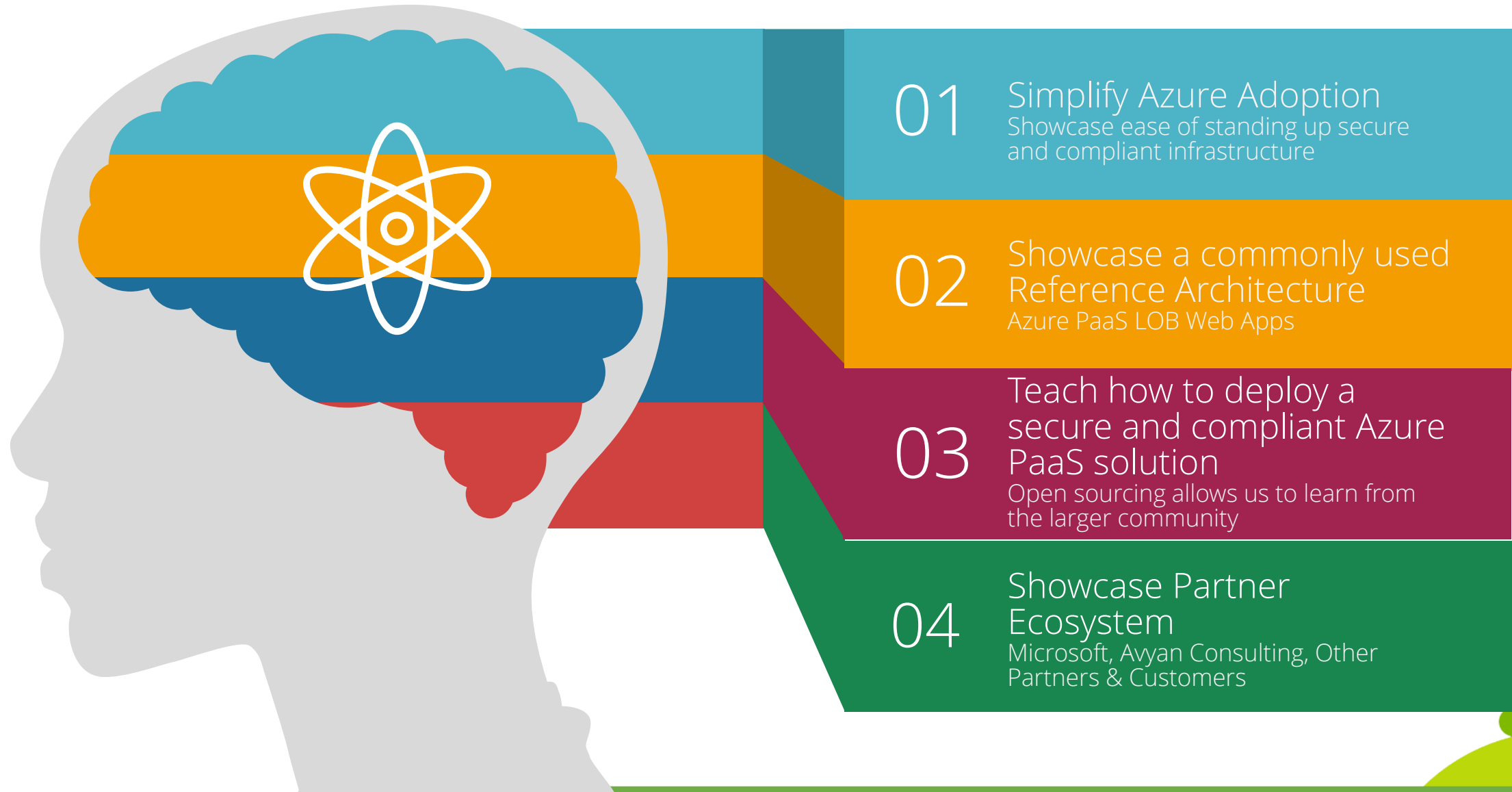
High Level PCI and HIPAA Blueprint design

4 tier (3 tier + DMZ) Network Layer Overview

BETA Solution (Looking for early adopters)

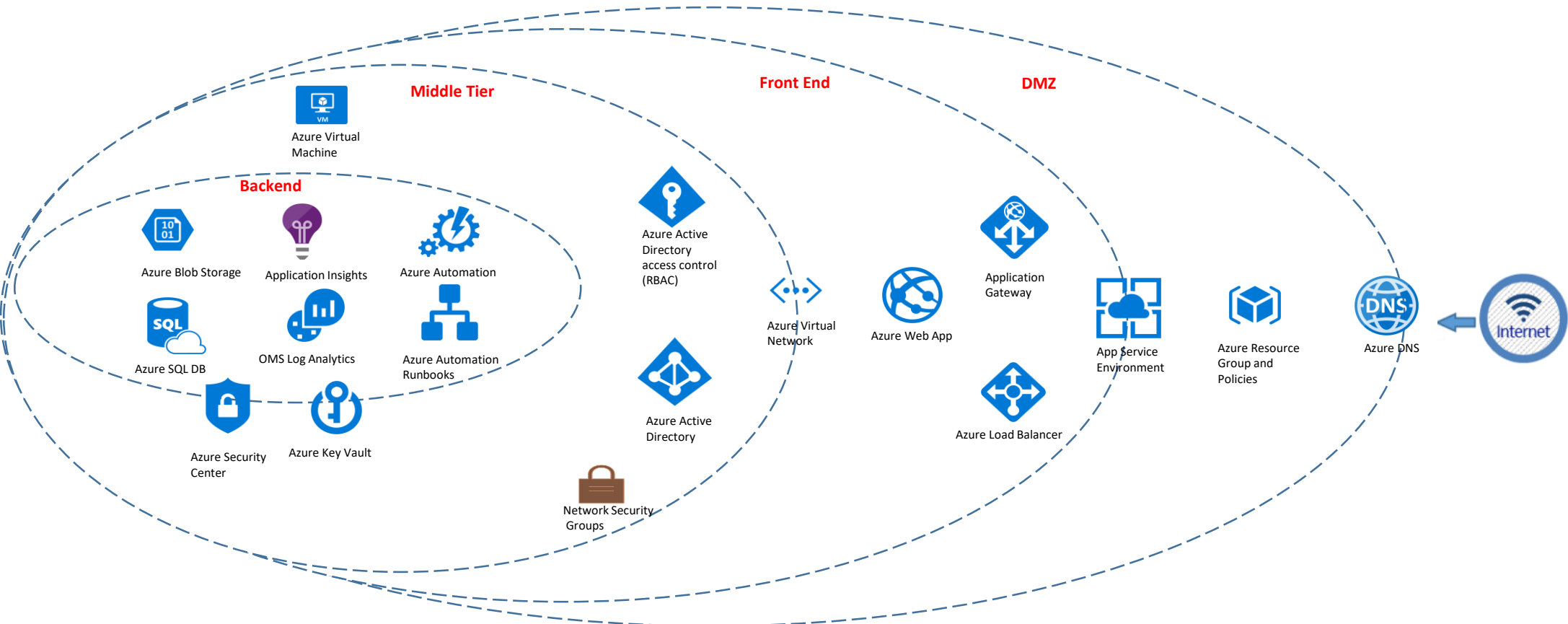


Avyan and Microsoft, Jointly built this Quickstart to...



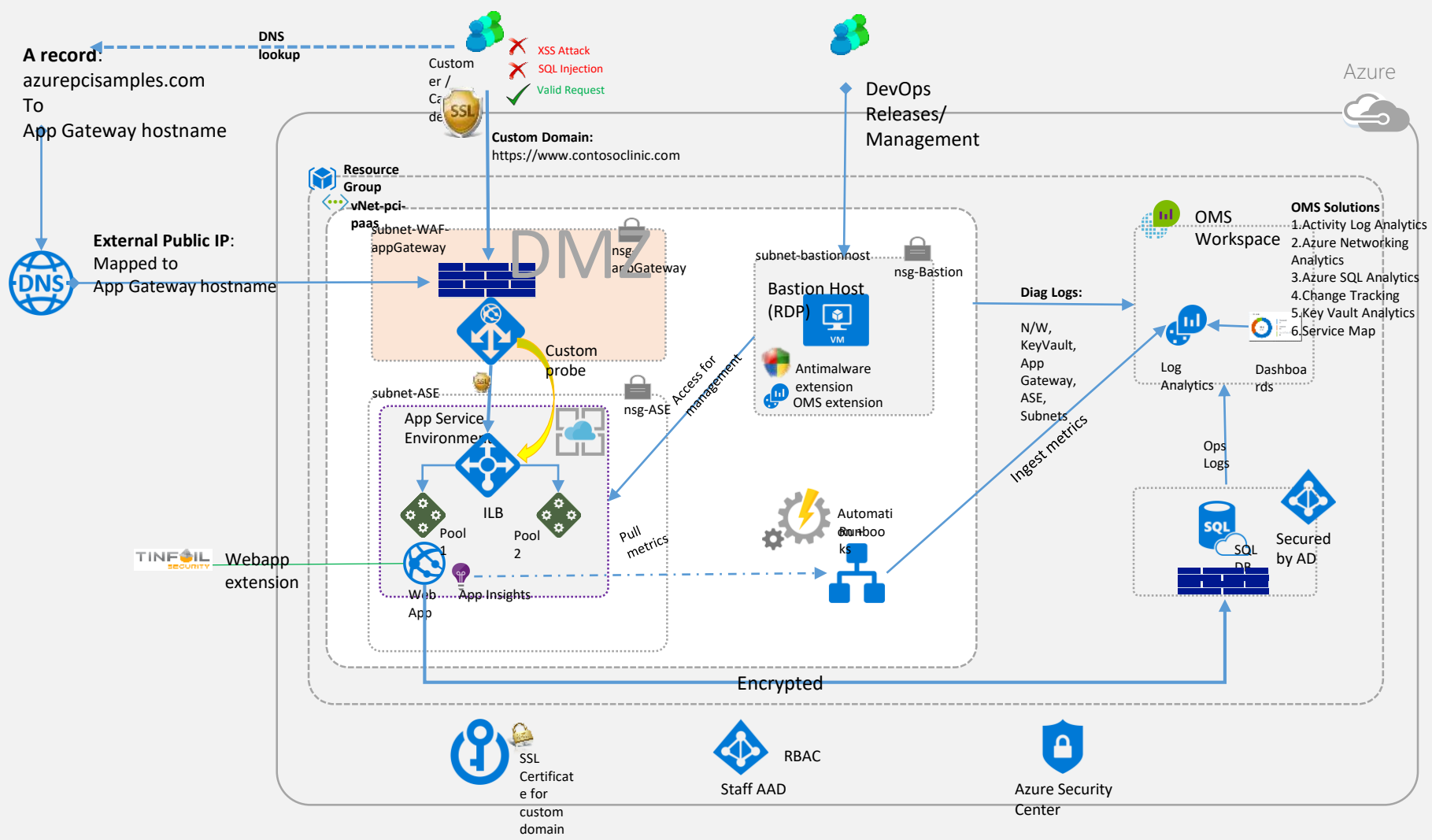
High Level PCI and HIPAA Blueprint Architecture

4 tier (3 tier + DMZ) networking layers overview



High Level PCI and HIPAA Blueprint Architecture

Reference Architecture



Configurations – Secure and Compliant

subnet-WAF-appGateway

Application Gateway

- [SSL Offload](#)
- [Custom Healthprobes](#)
- [Prevention mode](#)
- [Diagnostics Logging](#)
- [Web Application Firewall](#)
- [Disable TLS v1.0 and v1.1](#)

10.0.1.0/24

VM Bastion Host

- [Antimalware Extension](#)
- [OMS Monitoring](#)
- [VM Diagnostics Extension](#)
- [Encrypted Disk](#)
- [AutoShutDown Policy](#)

10.0.2.0/24

subnet-ASE

App Service Environment

- [Disable TLS 1.0](#)
- [Change TLS cipher](#)
- [Control inbound traffic N/W ports](#)
- [WAF – Restrict Data](#)(Third party)
[Allow SQL DB traffic](#)

Web App Configuration

- [Custom Domain](#)
- Extension:
 - Vulnerability Scanner: Tinfoil
 - Security WebApp Extension
- [Enable Diagnostics Logging](#)

Application Insights

- Server Requests, Failures, Exceptions, Availability WebTests

10.0.3.0/24

Infrastructure

NSG

- [Enable Diagnostics Logging](#)
- Inbound outbound Traffic rules

Resource Group

- [RBAC – Access Policies](#)

Azure Security Center

- Policies
- [Recommendations](#)

Key Vault

- Store Certificate
- [Enable Diagnostics Logging](#)

Management and Operations

OMS Log Analytics

- Data Retention: 365 days
- Dashboards for WebApp and SQL
- [OMS SQL DB Auditing View](#)
- [App Insights Extension](#)
- [Activity Log Analytics](#)
- [Azure Networking Analytics](#)
- Azure SQL Analytics
- [Change Tracking](#)
- [Key Vault Analytics](#)
- [Service Map](#)
- [Security And Audit Solution](#)

Azure Monitor

- [Monitoring Activity Logging](#)

PowerBI

- [Analyze Audit logs](#)

Automation

- [Azure automation](#)
- SQL and Web metrics Ingestion Runbooks

Databases

SQL DB

- [Auditing Enabled](#)
- [Transparent Data Encryption Enabled](#)
- Firewall rules (ASE worker pools)
- [Enable Diagnostics Logging](#)
- [Threat Detection](#)
- [Enable Always Encrypted Columns](#)(Permission issue)
- [Dynamic Data masking](#)(Powershell)
- Connection string encrypted
- [AD Authentication and Authorization](#)



Demo

Shameless Plug

Continuous Governance using



An Azure marketplace product for
Automated Governance, Compliance, Reliability and Risk Monitoring solution for enterprises using Azure

a complete governance solution built on Azure to ease and empower
your cloud journey



MANAGE COMPLIANCE

Baseline Compliance posture of
your cloud assets

- ✓ Industry standard Benchmarks - PCI DSS, HIPAA, CIS Security.
- ✓ Do you have appropriate controls to ensure network security?
- ✓ Do you have appropriate anti-malware, antivirus systems deployed and configured?



REDUCE BUSINESS RISK

Get recommendations to reduce
business risk

- ✓ Do you have appropriate levels of controls with proactive alerts configured on policy violations?
- ✓ Are all your secrets securely stored as per policies?
- ✓ Do you have detection mechanisms for non-compliant configurations?



OPTIMIZE COSTS

Baseline Spend Analysis and
Recommendations

- ✓ Are you on a cost-effective subscription?
- ✓ Do you have a large deployment for staging and testing slots that is not utilized well?
- ✓ Are your dev/test environments configured for optimal use?



IMPROVE RELIABILITY

Maximize reliability and availability
of your assets

- ✓ Are your deployments following architecture best practices?
- ✓ Do you get alerted on downtimes or availability impacting events?
- ✓ Are your mission critical environments backed-up regularly and automatically?

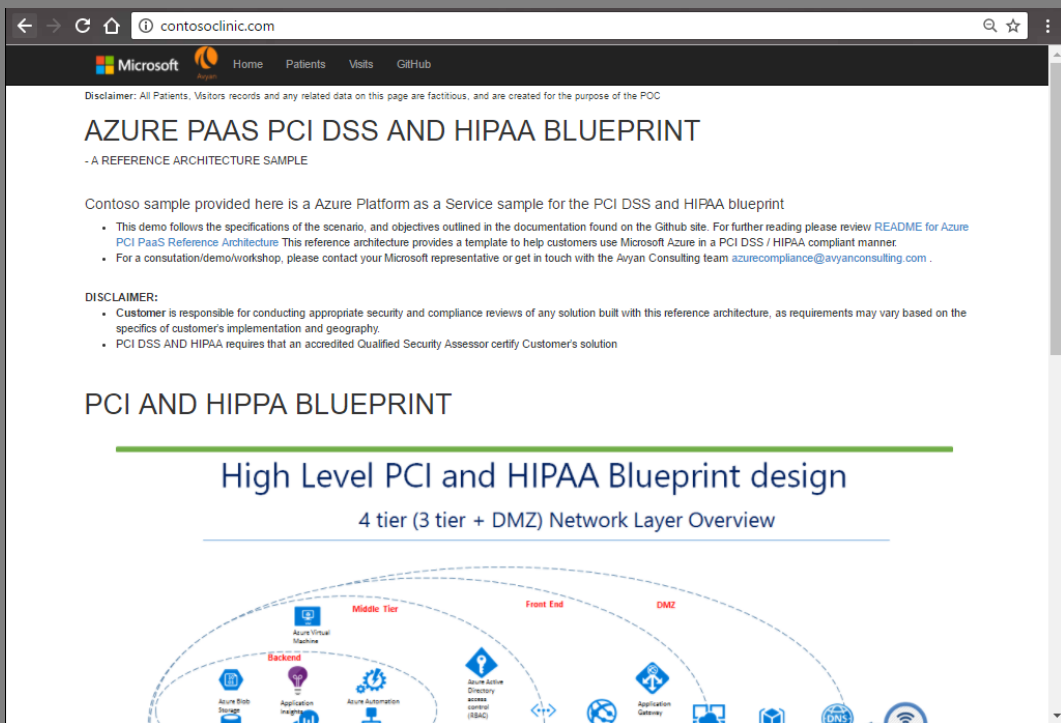


References

Reference Links

Demo Site - BETA

<http://contosoclinic.com>



Azure Trust Center

<https://azure.microsoft.com/en-us/support/trust-center/>

GitHub Location

Staging

<https://github.com/AvyanConsultingCorp/pci-paas-webapp-ase-sqldb-appgateway-keyvault-oms/>

Azure Quick Starts

<https://github.com/Azure/azure-quickstart-templates/tree/master/pci-paas-webapp-ase-sqldb-appgateway-keyvault-oms>



Q & A