



Azure Security Assessment

4-week implementation for XXXXX customers

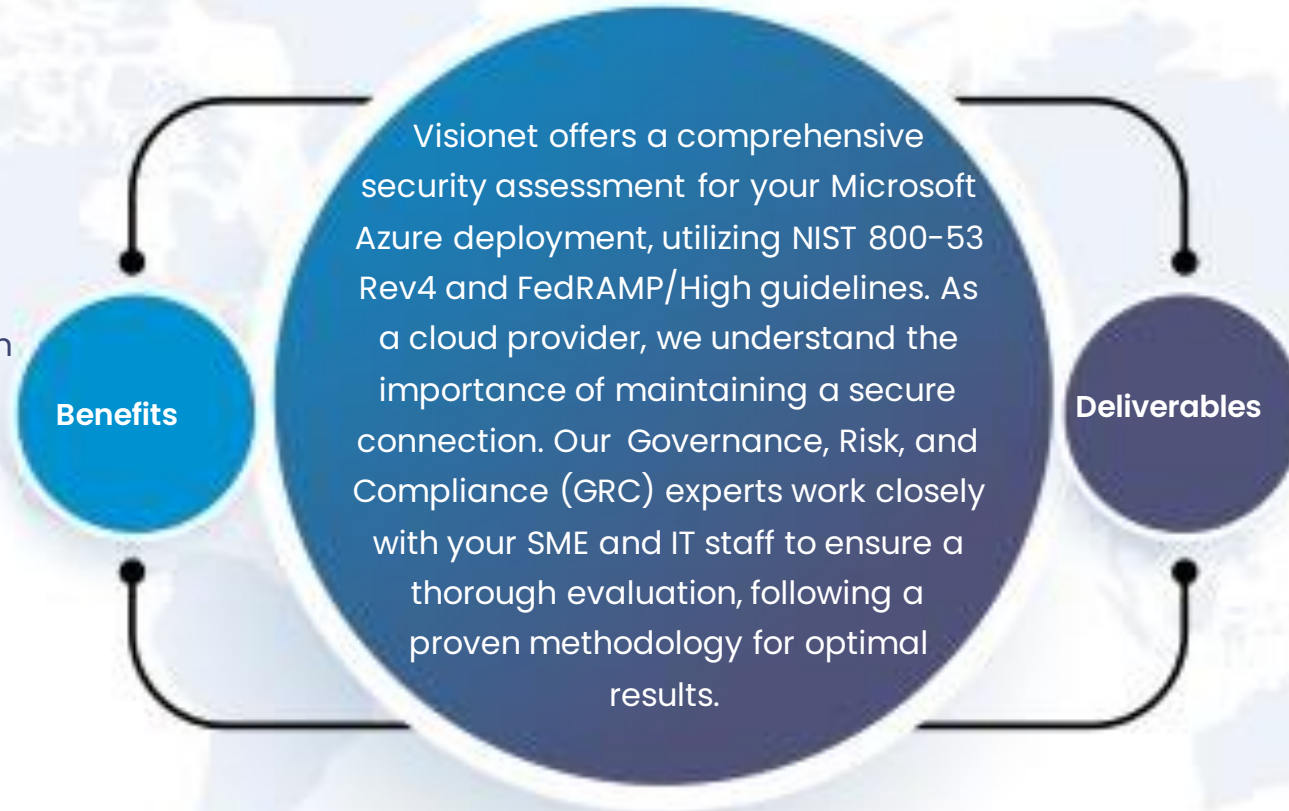
www.visionet.com

VISIONET
Innovation. Simplified.






Azure Security Assessment (NIST 800-53 FedRAMP/High)

4-week implementation for XXXXX customers

- Regulatory compliance – NIST 800-53 Rev4 is a widely recognized security framework used by government agencies
- Enhanced security posture – The assessment process helps identify and address security vulnerabilities and weaknesses in the Azure environment
- Risk Mitigation – A security assessment based on NIST 800-53 Rev4 FedRAMP/high enables organizations to identify and prioritize risks associated with the Azure environment
- Competitive advantage and continuous improvement

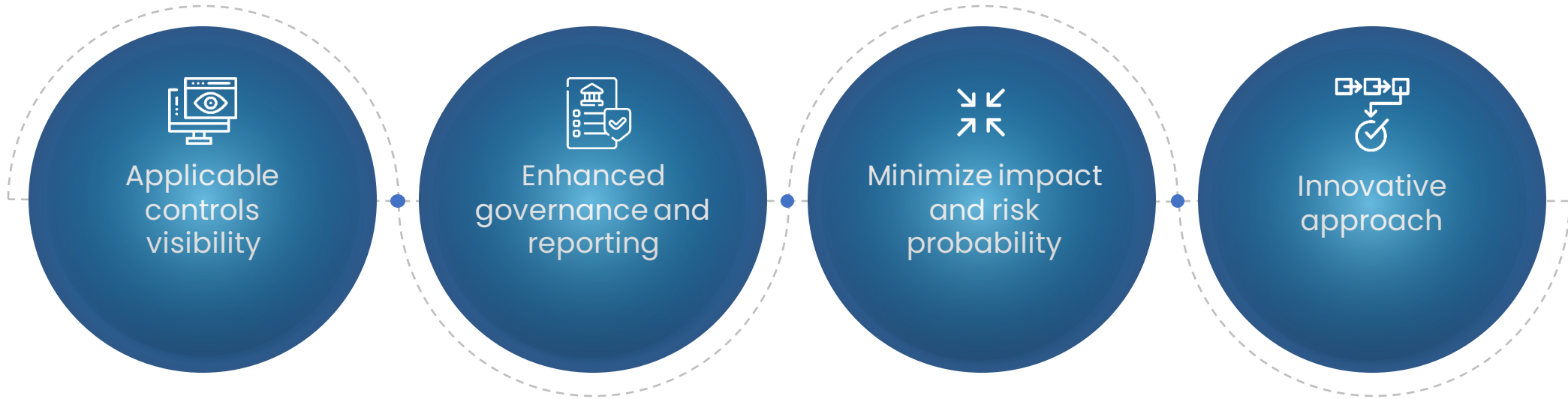


- Establishing the existing cybersecurity posture
- Security assessment report
- Remediation recommendations list as per gap assessment report

 Scoping	 Documentation review	 Controls Mapping and Gap Analysis	 Vulnerability Assessment and Configuration Audit	 Remediation Planning and Implementation Guidance
<ul style="list-style-type: none">• Define the scope of assessment identifying the Azure resources and services to be evaluated.	<ul style="list-style-type: none">• Gather relevant documentation, including Azure architecture diagrams, system documentation, security controls documentation, and existing security policies and practices.	<ul style="list-style-type: none">• Map NIST 800-53 Rev4 – FedRAMP/High security controls to the corresponding Azure security controls and services.• Perform gap analysis by comparing the existing controls and configurations with the requirements of NIST 800-53 Rev 4 – FedRAMP/High• Identify gaps, vulnerabilities and non-compliance areas that need to be addressed.	<ul style="list-style-type: none">• Conduct a vulnerability assessment of the azure environment using appropriate scanning tools and techniques.• Perform a configuration audit to evaluate access controls, network settings, the management of encryption mechanisms, and other relevant configurations.• Review the document and prioritize the identified vulnerabilities and misconfigurations.	<ul style="list-style-type: none">• Provide remediation steps based on the prioritized vulnerabilities and gaps.• Offer guidance for implementing security controls, making configuration changes, and updating policies to align with NIST 800-53 rev 4 – FedRAMP/High requirements.

Post-assessment Outcomes

Visionet's Deliverables



Attack Surface Summary
(Overall risks, risks by group, risks by regions)

Compliance Health report

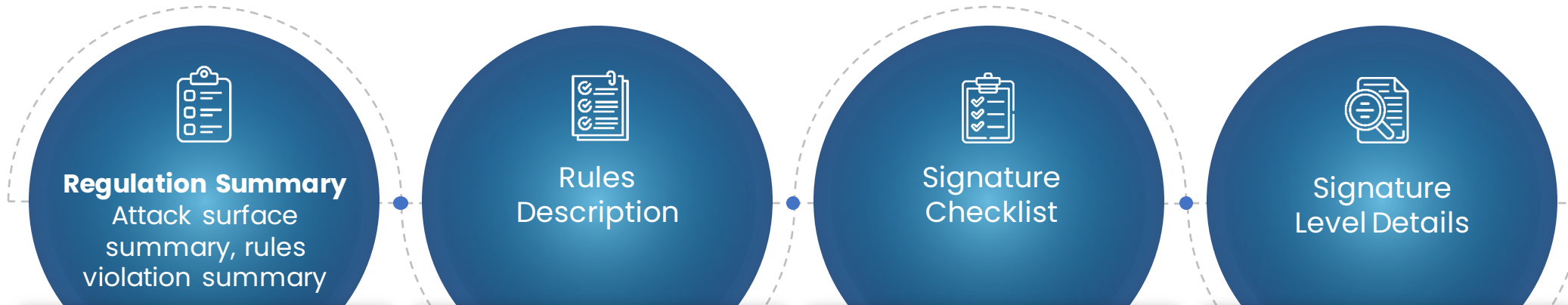
Signature checklist with flags, including severity, services, category, and remediations.

Visibility into protection capability gaps

A complete strategy related to Azure cloud security and regulatory compliance requirements involves several key components.

Post-assessment Outcomes

Visionet's Deliverables



1.Regulation Summary

1.1 Attack Surface Summary

Total 57 Surface Items found

Category	Item	Count
Computing	AWS EC2 Instance	0
	AWS Lambda	0
	Azure Virtual Machine	14
	GCP Cloud Functions	0
	GCP VM	0
Database	AWS DynamoDB	0
	AWS RDS	0
	Azure SQL Database	2
Storage	AWS S3	0
	Azure Storage Accounts	41
	GCP Storage	0
IAM	AWS IAM	0
	Azure Active Directory	0
	GCP Service Account	0

1.2 Attack Surface Summary

Overall Risk: pass 66.03%

Risks by Group: Networking, Encrypt..., IAM, Security, Monitoring, Disaster..., Logging

Risks by Region: eastasia, southeasia, centralus, euwest, eastus, westus, westcentralus, centralindia, southus, westus2

2. Rules Description

Configuration Management Control Family (CM)

(CM-7 (1)(a) | CM-7 (1)(b)) Periodic Review: 256 Passed | 72 Failed | Resources: 328

Signature	Resources	Risk Level	Status
[AZUSG-001] Ensure that RDP access is restricted from the internet	21 Passed 61 Failed	High	⊗
[AZUSG-002] Ensure that SSH access is restricted from the internet	71 Passed 11 Failed	High	⊗
[AZUSG-003] Ensure that Global Telnet access is restricted from the internet	82 Passed 0 Failed	High	⊙
[AZUSG-004] Ensure that Global MySQL access is restricted from the internet	83 Passed 0 Failed	High	⊙

Configuration Management Control Family (CM)

(CM-7a | CM-7b) Least Functionality: 120 Passed | 19 Failed | Resources: 139

Signature	Resources	Risk Level	Status
[AZU-SA-002] Ensure that 'Storage service encryption' is set to 'Enabled' for File Service	41 Passed 0 Failed	High	⊙
[AZU-SA-003] Storage Account Have Public, Accessible Containers	25 Passed 4 Failed	High	⊗
[AZU-VM-001] Ensure that OS disk are encrypted	13 Passed 1 Failed	High	⊗
[AZU-VM-002] Ensure that Data disks are encrypted	0 Passed 14 Failed	High	⊗
[AZU-SA-002] Ensure that 'Storage service encryption' is set to 'Enabled' for File Service	41 Passed 0 Failed	High	⊙

3. Signature Check list

Signature Name / Description	Severity	Service	Category	Provider
[AZUSG-001] Ensure that RDP access is restricted from the internet	High	NSG	Security	Azure
[AZUSG-002] Ensure that SSH access is restricted from the internet	High	NSG	Security	Azure
[AZUSG-003] Ensure that Global Telnet access is restricted from the internet	High	NSG	Security	Azure
[AZUSG-004] Ensure that Global MySQL access is restricted from the internet	High	NSG	Security	Azure
[AZU-SA-002] Ensure that 'Storage service encryption' is set to 'Enabled' for File Service	High	SA	Storage	Azure
[AZU-SA-003] Storage Account Have Public, Accessible Containers	High	SA	Storage	Azure
[AZU-VM-001] Ensure that OS disk are encrypted	High	VM	Cryptography	Azure
[AZU-VM-002] Ensure that Data disks are encrypted	High	VM	Cryptography	Azure
[AZUSQLDB-002] Ensure that SQL Database 'Data encryption' is set to 'On'	High	SQLDB	SQL Database	Azure
[AZU-SA-002] Ensure that 'Storage service encryption' is set to 'Enabled' for Blob Service	High	SA	Storage	Azure
[AZUSG-001] Ensure that RDP access is restricted from the internet	High	NSG	Security	Azure
[AZU-VM-003] Internet-facing Virtual Machine Should be Protected with Network Security Group	High	VM	Networking	Azure
[AZU-SQLDB-002] Ensure that 'Threat Detector' on SQL Database is set to 'On'	High	SQLDB	SQL Database	Azure

4. Signature Level Details

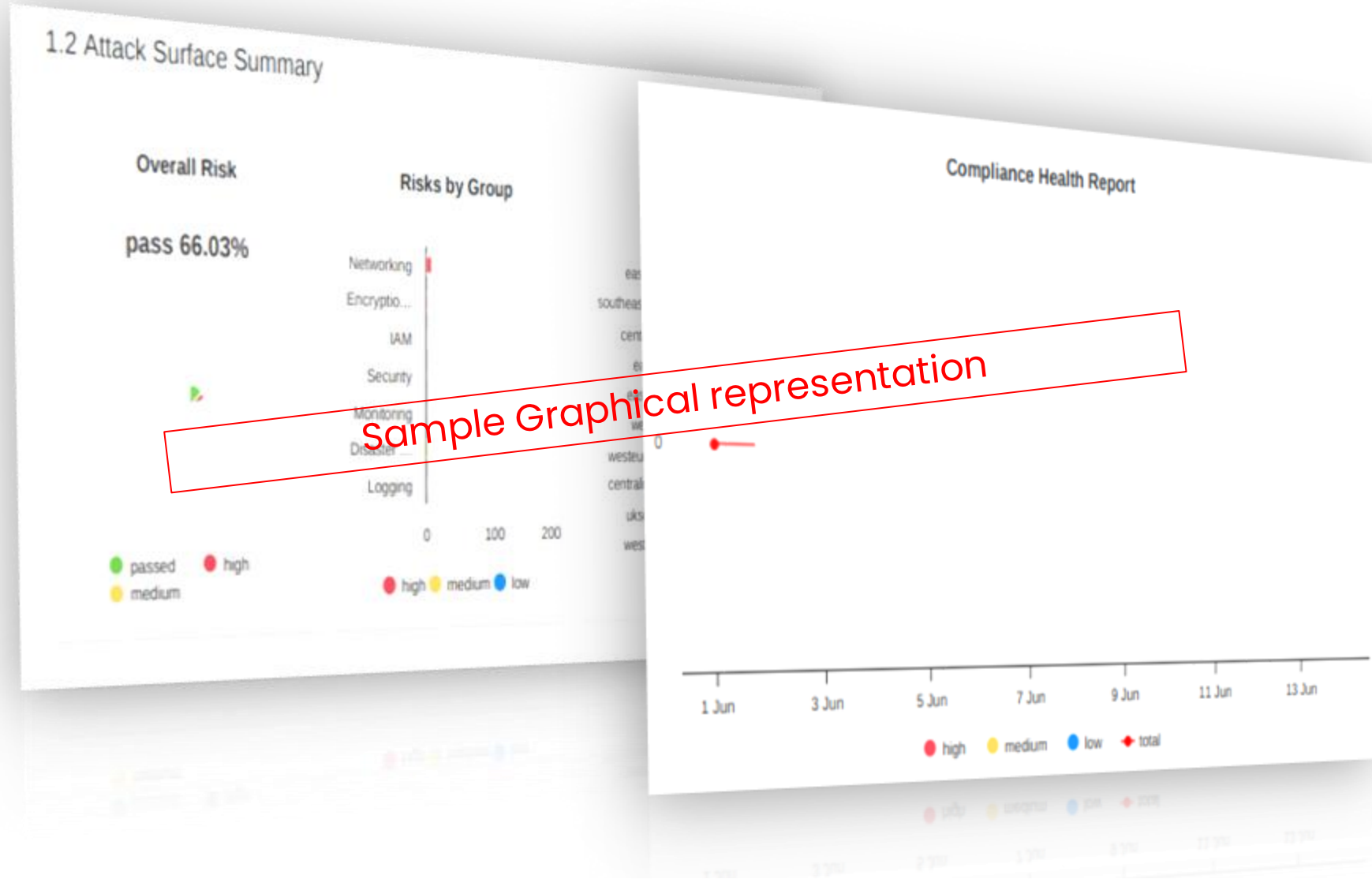
AZU:AD-005
Ensure that a maximum of 3 owners are designated for the subscription

In an Azure Subscription, as a security best practise, we ensure that there are not more than three designated Owners that belong to the subscription

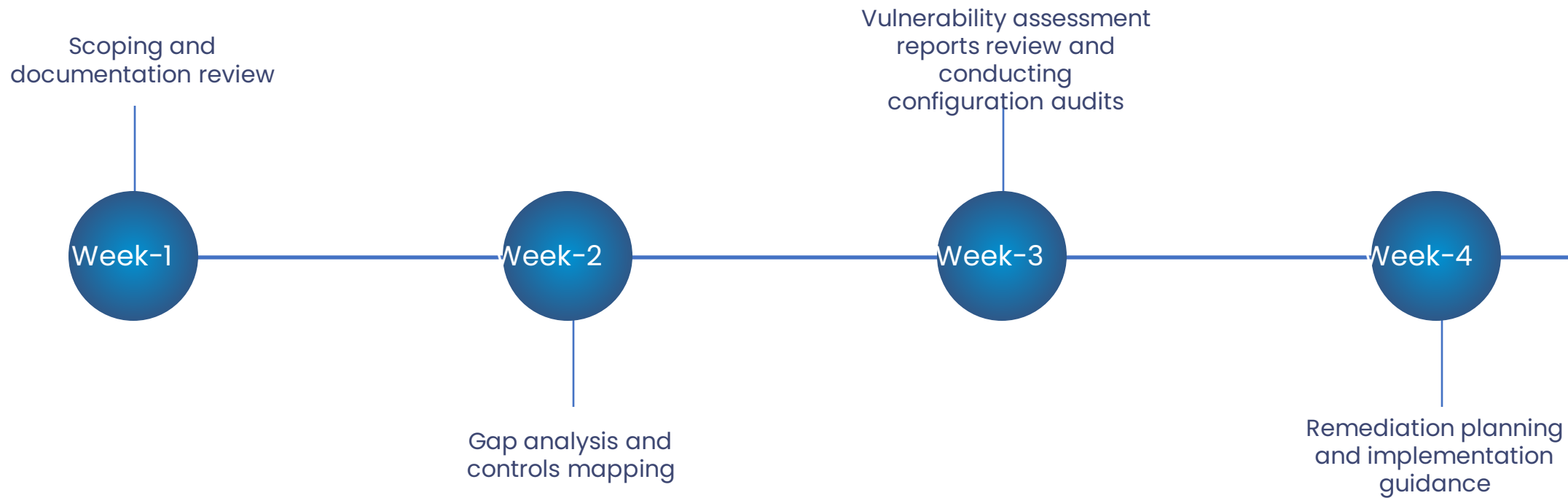
Name	Service	Region	VPC	Status
Azure_experience_center	cloudAccount	eastasia, southeasia, northeuope, westeuope, japanwest, japaneast, australiaeast, australiasoutheast, canadacentral, canadaseast, uksouth, ukwest, koreacentral, koreasouth, southindia, centralindia, westindia, brazilsouth, centralus, eastus, westus2, westus, northcentralus, westcentralus, westcentralus, westus2	N/A	⊗

Post-assessment Outcomes

Visionet's Deliverables sample report



Assessment Roadmap/Timelines



Your Trusted Technology Partner

Visionet is an engineering-led company driven by innovation. In our 27+ year journey, we've helped over 350 clients across various industries to innovate faster, stay relevant, and create superior products and services.

With more than 8,000 people worldwide, across our 14 locations, Visionet provides transformative consulting, technology, and outsourcing services and solutions for a wide range of industries, including Retail & Consumer Goods, Pharmaceutical, Banking and Financial Institutions (BFSI), Insurance, Foods & Beverage, Manufacturing & Distribution, and Apparel & Footwear. Through our alliance with global innovators like Microsoft, Salesforce, Amazon Web Services, and Adobe, we offer next-generation services and solutions in Cloud, Digital, Data and AI, and Business Process Management.

Learn more about Visionet at www.visionet.com

Headquarters

4 Cedarbrook Drive, Bldg. B
Cranbury, NJ 08512
Tel: +1 609 452 0700
Fax: +1 609 655 5232

United Kingdom

Yoooserv, Dakota, De
Havilland Dr,
Weybridge KT13 0YP

Germany

c/o Design Offices Berlin
am Zoo, Budapeststr.
Strasse 35, 10787 Berlin



VISIONET