NOVENTIQ
Global expertise, local outcomes

Security and Compliance Assessment

Fixed Scope Services

Introduction

Security assessment on Azure offering comprehensively evaluates your Azure environment’s security posture.

It aims to identify vulnerabilities, assess risk, and provide recommendations for enhancing security and compliance appropriately.

Customer Pain Points

Security & compliance assessment is highly after for working on different pain areas and accordingly gives solutions as per your business needs.

- **Compliance Challenges**
Evaluating customer’s Azure environment against different compliance standards (like GDPR, HIPAA, etc) and provide recommendations to ensure compliance.

- **Lack of network security**
Evaluates network configurations, firewall rules, and network security groups to ensure proper segmentation and protection against cyber threats.

- **Misconfigured resources**
Identifies misconfigured settings in Azure resources like storage accounts, virtual machines, databases, and thereby reduces the risk of exposure.

- **Inadequate identity and access management**
Reviewing identity and access controls in Azure AD, ensuring proper authentication and authorization mechanisms are in place, and reduces unauthorized access.

- **Data breaches & unauthorized access**
Identifies the vulnerabilities in data storage, access controls, authentication mechanisms, and helps to prevent unauthorized access.

- **Lack of incident response plan**
Helps customer develop an effective incident response plan and conduct tabletop exercises to decrease downtime and data loss.

Security and Compliance Assessment

Noventiq utilizes Modern tools to Analyze the Apps, DB and the other components, providing insights along with recommendations.

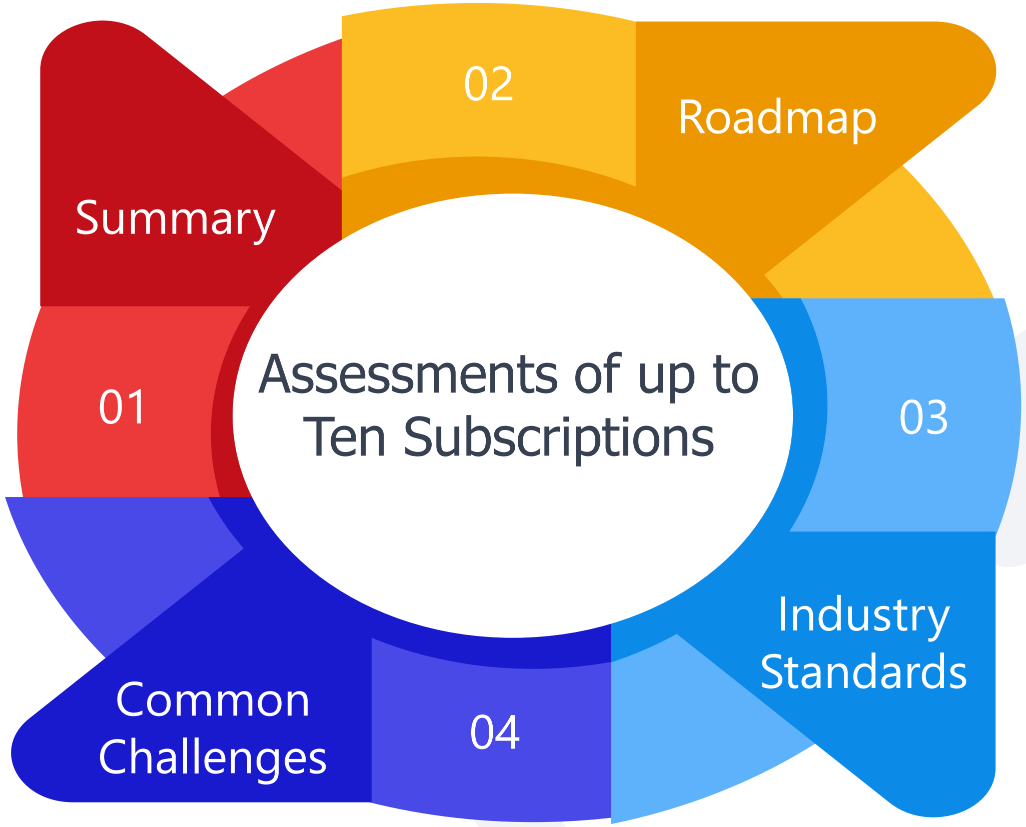
- Understanding the infrastructure, including all networks, storage accounts, and more
- Risk and vulnerability analysis to check for any vulnerabilities in the environment.
- Assessment of all security measures from encryption to firewalls, logging, and monitoring.
- Security Recommendations tailored to your needs.
- Compliance with appropriate industry standards like CIS, benchmarks, best practices, and regulatory requirements such as GDPR and HIPAA.
- It helps in raising sustainability and advanced digital maturity.

Security and Compliance Assessment

What do customers receive post-assessment?

- Summary of the complete assessment results, key findings, that will help management and decision-makers for making informed decisions.

- Insights on potential vulnerabilities in your environment and guidance on implementing essential security measures.



- Roadmap that gives the detail of recommended changes, timelines, dependencies, and workload impacts.

- Compliance with industry standards for a secure environment.

Security and Compliance Assessment

What are the prerequisites of the Assessment?

- Access and credentials for detailed assessment of Azure workloads.
- Stable workloads without any impact on the production environment.
- Resources for a smooth assessment by effective collaboration throughout the process.
- Tools and licenses, whichever is required.

Security and Compliance Assessment

Frequently Asked Questions.

1. What is the Security Assessment on Azure Offer?
The Security Assessment on Azure Offer is a comprehensive evaluation of your Azure environment's security posture. It identifies vulnerabilities, assesses risk, and provides recommendations to enhance security and compliance.

2. Why do I need a Security Assessment on Azure?
Azure environments can have security gaps that expose your data to risks. This assessment helps you identify potential vulnerabilities, ensuring a proactive approach to securing your cloud infrastructure.

3. Who conducts the assessment?
The assessment is typically conducted by Azure security experts who are well-versed in the latest security best practices and Azure's security features.

4. What areas of my Azure environment will be assessed?
The assessment covers many areas, including identity and access management, data security, network security, compliance, vulnerability management, threat detection, and incident response.

5. How long does the assessment take?
The duration can vary based on the complexity of your environment, but it usually takes a few weeks. This includes planning, assessment, analysis, and reporting.

NOVENTIQ

Global expertise, local outcomes

Thank You!