Grant Thornton

Cybersecurity Assessment

Grant Thornton provides an independent voice to serve as your cloud security advisor and assessor for Microsoft security products. We provide expert guidance and conduct in-depth security assessments tailored to your cloud infrastructure. Our assessments encompass thorough evaluations of your cloud environment's security posture, covering aspects such as vulnerability management, data protection, and compliance.

Cloud Security Benefits

- ✓ **Identify** control gaps and vulnerabilities within your cloud environment
- ✓ **Enhance** security posture through practical recommendations
- ✓ **Strategic** guidance to achieve desired future state maturity
- ✓ **Optimize** security solutions native to your cloud service provider's offering
- ✓ **Insight** to further align your cyber and business risk strategies

Building a robust cloud security environment

As organizations are embarking on their cloud transformation journeys, it is crucial to understand the security requirements for keeping data safe within the cloud.

Grant Thornton will perform a comprehensive cybersecurity assessment on your cloud environment to ensure the highest standards of security, compliance, and resilience are met. Through our analysis, we will boost your cloud environment's security posture, identify potential vulnerabilities, and provide actionable recommendations to enhance your overall security stance and safeguard your digital assets effectively and efficiently.

Goals & Objectives

Grant Thornton's assessment aims to help the customer achieve the following goals and objectives:

- **Discover Vulnerabilities** – Help the customer gain visibility into vulnerabilities in the M365 Cloud, servers, and endpoints using Microsoft Defender and Microsoft Secure score.
- **Identify Insider Risk** – Identify potentially risky data handling activities and gain visibility and understanding of the sensitive data that resides within the customer's environment.
- **Prioritize Remediation** – Define next steps and remediation roadmap with the help of the customer to help prioritize identified remediation opportunities from the assessment.

Cloud Security Challenges

Cloud Data Breaches

Increased risk of data breaches within the cloud due to misconfigured cloud environments, inadequate access / encryption controls, or malicious activities

Compliance Concerns

Lack of adherence to regulatory requirements and industry standards across cloud environments

Shared Responsibility Model

Insufficient understanding and management of security responsibilities between Cloud Service Providers (CSPs) and customers

Limited Cloud Security Expertise

Shortage of skilled professionals with expertise in cloud security to implement effective security measures within the cloud environment

Grant Thornton's Cybersecurity Assessment Engagement Approach:

Engagement Setup

- Identify key stakeholders and confirm engagement scope
- Gain access to cloud environment with necessary privileges
- Customer to go through change management for cloud environment changes
- Prepare the Azure environment for the engagement, including assigning trial licenses if required
- Configure Microsoft Defender and Purview with necessary policies and settings

Key Outputs:

- Kickoff slide deck
- Customer questionnaire

Engagement Execution

- **Environment Analysis:** Analyze the customer environment based on v8 of the CIS Critical Security Controls
- **Vulnerability Exploration:** Discover and analyze vulnerabilities identified leveraging Microsoft Defender Vulnerability Management
- **Data Security Exploration:** Discover and analyze data handling risks leveraging Microsoft Purview
- [Optional] **Cloud App Exploration:** Review cloud application usage to identify unsanctioned app usage

Key Outputs:

- Deployment review with customer staff

Results & Outcome

- Analyze identified vulnerabilities and recommendations provided by Microsoft Security products with the customer
- Develop high-level roadmap of recommendations to help prioritize remediation efforts
- Conduct knowledge transfer sessions with customer teams to help operationalize assessment

Key Outputs:

- Assessment Findings/Observations
- Remediation Roadmap

Why Grant Thornton?

- ✓ Microsoft certified services partner with direct access to Microsoft's engineering, product development and customer support teams
- ✓ Experience and expertise with the implementation and operation of Microsoft technologies for numerous programs including, but not limited to Microsoft Defender, Sentinel, Entra ID, Purview, and Intune
- ✓ Specific risk models and workflows built for Microsoft to support cybersecurity programs
- ✓ Backed by a national team of cybersecurity and privacy professionals to meet the needs of your cyber program

Contact

John Pearce
Principal
T +1 703 637 4071
E John.Pearce@us.gt.com

Victor Chavalit
Senior Manager
T +1 312-602-8945
E Victor.Chavalit@us.gt.com

Microsoft Solutions Partner
Security
Specialist
Cloud Security
Threat Protection

Grant Thornton