Scope Statement: DataWorks Security Optimization Initiative

Date: 11/12/2024

Objective

The objective of the DataWorks Security Optimization Initiative is to enhance DataWorks Global Inc.'s security posture in Microsoft Azure and hybrid environments. This project will ensure compliance with regulatory standards, reduce cybersecurity risks, and improve overall security operations by implementing best practices across identity and access, network, compute, storage, and security monitoring.

Project Deliverables

1. Identity and Acces Management: Implement multi-factor authentication (MFA), single sign-on (SSO), and Conditional Access policies. Configure Microsoft Entra ID to enforce role-based access control (RBAC) and privileged identity management (PIM).

2. Network Security: Configure Network Security Groups (NSGs), Application Security Groups (ASGs), and firewall policies.
Establish secure virtual network peering, VPN gateway, and configure security for VPN connectivity.

3. Compute, Storage, and Database Security: Encrypt virtual machines, storage accounts, and databases. Implement data classification and encryption using Microsoft Purview for sensitive data.

4. Security Operations: Set up Microsoft Defender for Cloud for threat detection and monitoring. Configure Microsoft Sentinel for automated threat responses and integration with security information and event management (SIEM) tools.

5. Compiance Documentation: Document security configurations and controls to meet compliance standards (e.g., SOX, GDPR).
Prepare compliance review documents and validation reports.

Acceptance Criteria

Security Compliance: The project meets SOX, GDPR, and other applicable regulatory standards.

Operational Security: All configurations and security operations meet DataWorks’ internal security benchmarks, as verified by UAT.

Documentation Completeness: Comprehensive documentation is completed and approved by the Compliance Officer.

Sign-Off by Stakeholders: Final approval by CIO, IT Security Manager, and Compliance Officer upon completion.

Project Inclusions	Project Exclusions
Configuration and Implementation: Includes all configurations in Azure related to identity, networking, compute, and storage security.	Non-Azure Environments: Security configurations outside of Microsoft Azure or hybrid integrations outside the current infrastructure are out of scope.
Compliance Documentation: Detailed documentation for all implemented controls, prepared in alignment with regulatory requirements.	Custom Software Development: No development or customization of non-Microsoft solutions will be performed.
User Acceptance Testing (UAT): Conduct UAT to validate that all security configurations are operational and meet project requirements.	End-User Training: General end-user training is excluded; however, project-specific technical team training for new configurations will be provided.
	Ongoing Maintenance: Post-project maintenance and support are not included in this project scope.

Project Constraints	Assumptions
Timeline: The project must be completed by 12/31/2024 to align with regulatory deadlines and internal IT initiatives.	All necessary Azure resources, licenses, and third-party tools will be available and operational throughout the project.
Budget: Budget limitations set by DataWorks Global Inc. finance will dictate resource allocation and any potential procurement of third-party tools.	Compliance and IT Security teams will be available to review and approve configurations promptly.
Resources: The availability of internal and vendor resources for both Azure security configuration and compliance tasks.	No major regulatory changes will occur during the project that could significantly alter the scope.