

DataWorks Global Inc.

# Project Charter: Security Optimization Initiative

IT Security Department

11-11-2024

Contents

Project Overview .....2

    Purpose .....2

    Project Objectives .....2

    Success Criteria.....2

Project Scope .....3

Methodology .....3

Milestone Schedule .....4

Roles and Responsibilities.....4

Project Risks and Mitigations .....4

Communication Plan.....5

Approvals .....5

# Project Overview

Project Name: DataWorks Security Optimization Initiative

Project Sponsor: DataWorks Global Inc. IT Security Department

Vendor: Azure Security Engineering – Daniel R.

Date: 11/11/2024

## Purpose

The purpose of this project is to enhance DataWorks Global Inc.'s security posture in Microsoft Azure and hybrid environments, addressing regulatory compliance requirements and mitigating evolving cyber threats. The project will implement robust security controls in identity and access management, secure networking, compute, storage, and security operations.

## Project Objectives

1. Identity and Access Management: Improve security controls by implementing multi-factor authentication, conditional access, and role-based access management using Microsoft Entra ID.
2. Network Security: Secure Azure networks through Network Security Groups (NSGs), Application Security Groups (ASGs), VPN configurations, and firewall policies.
3. Compute, Storage, and Database Security: Protect sensitive data by implementing encryption, securing Azure SQL databases, and enabling data classification using Microsoft Purview.
4. Security Operations: Strengthen monitoring and incident response capabilities with Microsoft Defender for Cloud and Microsoft Sentinel to detect, investigate, and mitigate security incidents.

## Success Criteria

- Compliance: Achieve and maintain compliance with regulatory standards (SOX, GDPR) through documented configurations and controls.
- Improved Security Metrics: Increase security score in Microsoft Defender for Cloud by 20%.
- Reduced Incident Response Time: Reduce average incident response time by 30% using Microsoft Sentinel automation.
- Stakeholder Satisfaction: Achieve stakeholder satisfaction with the security implementation and transition.

# Project Scope

## In-Scope:

- Implementation of identity, network, compute, storage, and operational security enhancements in Microsoft Azure.
- Integration with on-premises resources as part of DataWorks' hybrid environment.
- Compliance documentation and verification.

## Out of Scope:

- Security configurations outside Microsoft Azure environments.
- Implementation of non-Azure-specific tools.

# Methodology

The project will use a Scrum framework integrated with DevSecOps for continuous security improvements and an iterative approach to meet security and compliance requirements.

## Project Phases:

1. Initiation and Planning: Define requirements, develop WBS, and establish initial sprint planning.
2. Execution: Implement security configurations across identity, networking, compute, storage, and security operations in Azure.
3. Monitoring and Control: Continuous tracking of risks, changes, and project status through each sprint.
4. Closure: Final review, documentation, and project handover.

## Milestone Schedule

Milestone	Description	Target Completion
Kickoff Meeting	Define project objectives, roles, and methodology.	Day 1
Identity and Access Management Complete	Implementation of MFA, SSO, and access policies.	End of Week 2
Network Security Complete	Network configurations with NSGs, VPNs, and firewalls	End of Week 4
Compute, Storage, and Database Security	Implementation of encryption and data classification	End of Week 6
Security Operations Complete	Setup of Microsoft Defender for Cloud, Sentinel	End of Week 8
Final Review and Project Closeout	Documentation, review, and handover	End of Week 9

## Roles and Responsibilities

Role	Responsibilities	Contact
Project Sponsor	Provide direction, ensure resources, and approve project deliverables	IT Security Manager
Azure Security Engineer	Configure, implement, and document Azure security solutions	Daniel R.
Project Manager	Oversee project timeline, manage risks and resources, handle changes	Daniel R.
Compliance Officer	Ensure configurations meet regulatory standards	Compliance Officer

## Project Risks and Mitigations

Risk	Impact	Mitigation Strategy
Regulatory Changes	Potential delays due to additional controls.	Review compliance standards periodically.
Cybersecurity Threats	Increased security risks during configuration.	Implement security controls incrementally and monitor.
Vender Dependency	Dependency on third-party tools may cause delays.	Validate tools and SLAs before integration.

## Communication Plan

- Weekly Status Meetings: Weekly touchpoints with all stakeholders to review project progress, risks, and any open issues.
- Sprint Reviews: Conduct sprint reviews with detailed updates on completed work and any adjustments in scope.
- Change Control Process: Track all requested changes in a change control log and escalate to Change Control Board (CCB) as needed.
- Final Project Handover: Conduct a closing presentation to review the project deliverables, lessons learned, and any post-implementation support requirements.

## Approvals

Stakeholder	Signature	Date
Project Sponsor	Approved	11/11/2024
Compliance Officer	Approved	11/11/2024
Azure Security Engineer	Approved	11/11/2024
Project Manager	Approved	11/11/2024