DataWorks Global Inc.

Quality Management Plan

DataWorks Security Optimization Initiative

Contents

Quality Management Plan

Purpose

The purpose of the Quality Management Plan is to ensure that all project deliverables meet established quality standards and fulfill project requirements. This plan defines quality objectives, metrics, roles, and responsibilities to maintain consistency, reliability, and compliance with regulatory requirements.

Quality Objectives

- Compliance: Ensure that all security configurations and practices meet industry and regulatory standards (e.g., SOX, GDPR).
- Functionality: Confirm that all security implementations (e.g., identity management, network security, storage encryption) function as expected without adverse impacts on system performance.
- Documentation: Deliver comprehensive, accurate documentation for each configuration, aligned with compliance and internal standards.

Quality Standards and Metrics

Quality Standard	Description	Metric	Target
Regulatory Compliance	All configurations adhere to SOX, GDPR, and other applicable standards.	Compliance Review Score	100% compliance with standards
System Availability	Implementations should not reduce overall system uptime or performance.	System Uptime	99.9% uptime
Configuration Accuracy	Configurations meet project requirements (e.g., MFA, NSGs, RBAC).	Number of Configuration Errors	0 errors post-implementation
Security Incident Response	Detect, respond, and document any security incidents promptly.	Incident Response Time	90% of incidents resolved within SLA
Documentation Completeness	Documentation is clear, complete, and follows compliance standards.	Documentation Review Score	95% accuracy and completeness

Quality Assurance Activities

Quality Assurance (QA) focuses on preventing defects and ensuring processes meet project quality standards through proactive planning and review.

1. Compliance and Regulatory Checks
   - Conduct periodic compliance reviews to ensure that all configurations meet SOX, GDPR, and other regulatory requirements.
   - The Compliance Officer reviews each configuration for adherence to these standards before approval.
2. Configuration and Integration Testing
   - Perform detailed testing of configurations for identity and access, network security, and storage encryption to ensure they function as expected.
   - Integration testing is conducted to ensure Azure configurations integrate smoothly with on-premises systems.
3. Code and Configuration Reviews
   - Azure Security Engineer and IT Security Manager review configurations to verify they meet project specifications.
   - Peer reviews are conducted for critical tasks to identify and correct potential issues early.
4. User Acceptance Testing (UAT)
   - UAT sessions are conducted to validate that security configurations align with user needs and function as required.
   - UAT is done by end-user representatives and stakeholders to confirm usability and functionality.

Quality Control Activities

Quality Control (QC) focuses on identifying and correcting defects through systematic inspection, testing, and validation to ensure deliverables meet the defined quality criteria.

1. Configuration Validation
   - Each configuration undergoes validation to confirm correct implementation, including RBAC, NSGs, MFA, and encryption settings.
   - Results are documented and reviewed by the IT Security Manager for sign-off.
2. Compliance Audits
   - Audits are conducted to ensure documentation accuracy, regulatory compliance, and that all configurations meet project standards.
   - The Compliance Officer performs a final review of all documents and reports to confirm compliance.
3. Incident and Error Tracking
   - A log is maintained to track any security incidents, errors, or issues identified during implementation.
   - The Project Manager oversees error tracking, ensuring that all issues are addressed promptly and that corrective actions are documented.

4. Post-Implementation Testing
    - Conduct final testing of all systems after implementation to confirm that configurations do not impact system performance.
    - Verification includes stress testing, performance testing, and user validation to ensure functionality under typical and peak loads.

Roles and Responsibilities

Role	Description
Project Manager	Coordinates quality assurance activities, oversees compliance with the Quality Plan.
Compliance Officer	Ensures all deliverables meet regulatory standards and compliance requirements.
IT Security Manager	Validates configurations, oversees configuration reviews, and signs off on quality.
Azure Security Engineer	Conducts configuration testing, participates in quality control activities.
End-User Representative	Participates in UAT, validates functionality and usability of configurations.

Quality Documentation

- Test Plans and Results: Detailed testing plans for configurations, with documentation of results.
- Compliance Review Reports: Documentation verifying each configuration’s adherence to regulatory standards.
- Configuration Checklists: Checklists for each security configuration to confirm that all project requirements are met.
- Change Control Log: Records changes and the quality impact of each change.
- Issue Log: Tracks incidents, issues, or defects encountered during the project, along with resolutions.

Continuous Improvement

Retrospective and Lessons Learned

At the end of the project, conduct a retrospective to identify areas for improvement in quality processes. Document lessons learned and recommendations for future projects.

Feedback Loops

Solicit feedback from all team members and stakeholders after key milestones to refine quality processes. Incorporate feedback into ongoing quality activities, enhancing processes for future phases and projects.