Presentation and
Discussion Item 11

MesaWater
DISTRICT©

IT Operations Assessment Report

January 25, 2022

Nth Generation: Renee Sanshu and Jim Westover

Agenda

- Assessment Methodology
- Assessment Scoring Criteria
- Assessment Scores
- Four Key Areas of IT Assessment
  - System Architecture
  - IT Operations
  - Status Reporting
  - Continuous Service Improvement
- Closing Remarks

Assessment Methodology

- National Institute of Standards and Technology (NIST) framework
  - Adaptable to many tools, technologies, and processes
- NIST Framework functions—identify, protect, detect, respond, and recover
  - Determine current level of IT operational excellence
  - Set goals for IT operations that are in sync with business environment
  - Establish a plan for improving or maintaining IT infrastructure and security posture

Assessment Scoring

Policy Maturity

- Covers major IT facilities, assets, and operations
- Lays the foundation necessary to reliably measure progress and compliance
- Defines penalties and disciplinary action to be used if policy is not followed

IT Audit Score	Maturity Level	Expectation of Policy Maturity Level
Red	Level 1 - Initial	Policy or standard does not exist or is not formally approved by management.
Red	Level 2 - Repeatable	Policy or standard exists but has not been reviewed for more than 2 years.
Green	Level 3 - Defined	Some policies and standards exist with formal management approval.
Green	Level 4 - Managed	All policies and standards exist with formal management approval.
Gold	Level 5 - Optimizing	All policies and standards exist with formal management approval. Policy exceptions are documented, approved, and rarely occur.

Procedure Maturity

- Clarifies ***where*** the procedure is to be performed, ***when*** it is to be performed, ***who*** is to perform it, and ***how*** the procedure is to be performed
- Identifies individuals or resources to be contacted for further information, guidance, and compliance
- Defines the accuracy needed

IT Audit Score	Maturity Level	Expectation of Procedure Maturity Level
Red	Level 1 - Initial	Standard process does not exist.
Red	Level 2 - Repeatable	Ad-hoc process exists and is done informally.
Green	Level 3 - Defined	Formal processes exist and are documented. Evidence can be provided for most activities. Some exceptions occur.
Green	Level 4 - Managed	Formal processes exist and are documented. Evidence can be provided for all activities and detailed metrics of the process are captured and reported. Minimal exceptions occur with minimal recurring exceptions.
Gold	Level 5 - Optimizing	Formal processes exist and are documented. Evidence can be provided for all activities and detailed metrics of the process are captured and reported. No process exceptions occur.

Baseline audit conducted in FY2019

FY2021 Assessment Scores

Areas Measured

- **System Architecture**
  - Data Center Facilities
  - Physical Servers
  - Virtual Servers
    - On premise
    - Cloud
  - Data Storage and Backups
  - Network
  - Client computers
- **Operations**
  - IT Policies
  - IT Procedures
- **Status Reporting**
  - Daily metrics
  - Monthly IT Management Reports
- **Continuous Service Improvement**
  - Incident Logs
  - Root Cause Analysis (RCA)
  - Change management

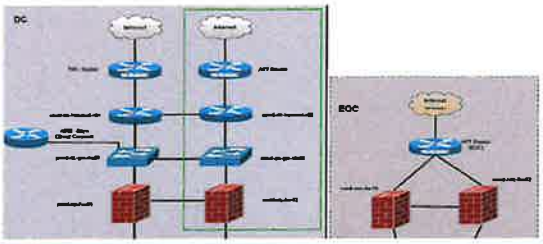
Audit Component	Policy Score	Procedure / Practice Score
System Architecture	3	4.4
Operations	3	4
Status Reporting	3	4.5
Continuous Service Improvement	5	4.5

System Architecture

Audit Component	Policy Score	Procedure / Practice Score
System Architecture	3	4.4

Findings

- Redundancy and high-availability were improved in several areas of the enterprise architecture
- The Cloud and on-premises infrastructure are managed in single pane of glass with a leading management tool – SolarWinds
- Cloud and on-premises environments need regular fail-over testing



Corrective Actions

- Upgrade or replace storage arrays
- Replace two older UPS
- Plan to replace End-of-Life Cisco switches
- Upgrade the following:
  - VMware to v7, current version is end of support in Oct
  - Veeam v11 with the goal of ransomware immutable backup options for server and storage
- Implement Best Practice health checks for Palo Alto Networks firewalls
- Re-examine data center temperature thresholds when adding/removing equipment; align with ASHRAE standards

IT Operations

Audit Component	Policy Score	Procedure / Practice Score
Operations	3	4

Findings

- Implemented two Corrective Actions from baseline FY2019
  - Define and document goals for inventory lifecycle management
  - Use Track-IT! as the single repository for physical IT asset management
- Five out of 11 IT procedures are tied to policies
  - Six lack a purpose statement, penalties and accuracy required
- Repeatable processes need more detailed documentation that would allow an independent third party to perform the task successfully

Corrective Actions

- Create policy statements for IT procedures not related to the two existing IT policies
  - This will lay the foundation necessary to reliably measure progress and compliance
- Create a Procedure Template
  - Template should have both text and flowcharts
- Update the following IT Procedures:
  - 1.12 add a decision box for when an RCA is needed
  - 1.13, 1.14, 1.15 and 1.16 to remove references to retired spreadsheets
  - 1.15 add a list of approved software
  - 1.21 and 1.22 rewrite, clarify steps, add criteria

Status Reporting

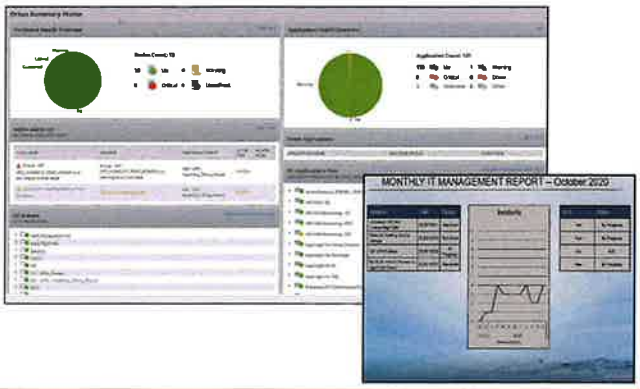
Audit Component	Policy Score	Procedure / Practice Score
Status Reporting	3	4.5

Findings

- Implemented two Corrective Actions from baseline FY2019
  - Ensured that default or past values are cleared
  - Added Temperature and Humidity criteria into system monitoring procedures
- Three IT Monthly Management Reports had missing incident data and/or an incorrect metric
- Asset Aging metric incorrectly moved to green starting in January 2021

Corrective Actions

- Conduct an internal QC check on monthly reports prior to submission



Continuous Service Improvement

Audit Component	Policy Score	Procedure / Practice Score
Continuous Service Improvement	5	4.5

Findings

- Very timely response to incidents that occurred in FY2021
- Change Orders are entered and tracked in a Change Management Log
- Regular server patching procedures are defined and executed monthly
- Backups are performed nightly and checked daily
  - However, there is no IT policy or procedure requiring backup recovery testing
- Procedure 1.21 identifies catastrophic events and potential mitigation strategies but there is no IT Business Continuity Plan

Corrective Actions

- Conduct a business impact analysis
- Create an IT Business Continuity Plan
- Generate and test the validity of an IT Disaster Recovery Procedure
- Update procedures 1.12 IT RCA-CQI and 1.01 IT Incident Notification flowcharts
- Consider using the Track-IT!'s Change Management feature for Change Orders

Closing Remarks

- Continuous improvement is demonstrated on a daily basis
- The Road to Gold