ROGER MCNULTY

IT BUSINESS SYSTEMS ANALYSIS & PROCESS MODERNIZATION PORTFOLIO

Prepared by Roger McNulty
Systems Engineer | Business Systems Analyst
Requirements, Process, & IT Modernization Support
MBA – Project Management (In Progress)
Southern New Hampshire University
2025

Purpose of This Portfolio:

To comply with confidentiality agreements and protect proprietary information, all company names, product names, financial figures, and sensitive technical details have been fully anonymized and replaced with a fictional business context. This portfolio demonstrates my skills in analysis, documentation, and structured project execution based on real-world experience.

How to Use This Portfolio:

This portfolio is organized to provide hiring managers and interviewers with a clear, structured view of project experience, technical-operational contributions, and demonstrated leadership capabilities across mission-critical environments.

The Case Studies offer concise, outcome-focused summaries of major initiatives, including collaboration across cybersecurity, operations, engineering, and program management. Each case study presents context, the approach taken, outcomes achieved, and supporting deliverables.

The Exhibits provide visual and documentary evidence of real project outputs, such as workflow diagrams, SOPs, tracking systems, and modernization models. These artifacts illustrate communication style, documentation quality, and the ability to translate complex technical material into structured operational guidance.

The portfolio is designed for interviewers to browse selectively, either reviewing high-level summaries or diving deeper into exhibits where relevant. It complements live interview discussions by providing tangible, professional examples of project work, decision-making, and technical-process alignment.

Table of Contents

About Me

I strengthen mission-critical environments through structured communication, risk-focused planning, and technical-operational alignment.

I am an aspiring IT Project Manager/ Business Analyst with experience in cybersecurity compliance, IT service delivery, infrastructure modernization, system sustainment, and cross-functional coordination in classified defense environments. I have supported critical mission programs across multiple defense contractors and previously led complex operational workflows as an operations manager. My background integrates technical depth, operational leadership, and structured communication, supported by ongoing MBA studies in Project Management and PMP preparation.

Detail	Description
Education	MBA – Project Management (in progress)
Technical Focus	Infrastructure, cybersecurity alignment, IT operations, requirements gathering, risk assessment, workflow documentation

Project Management Competency Summary

Experience in project management has been built through work supporting modernization programs, infrastructure remediation, knowledge-capture initiatives, and workflow optimization across engineering, cybersecurity, digital technology, and operations teams. Project involvement consistently emphasizes structured communication, traceable documentation, and alignment of technical requirements with operational readiness.

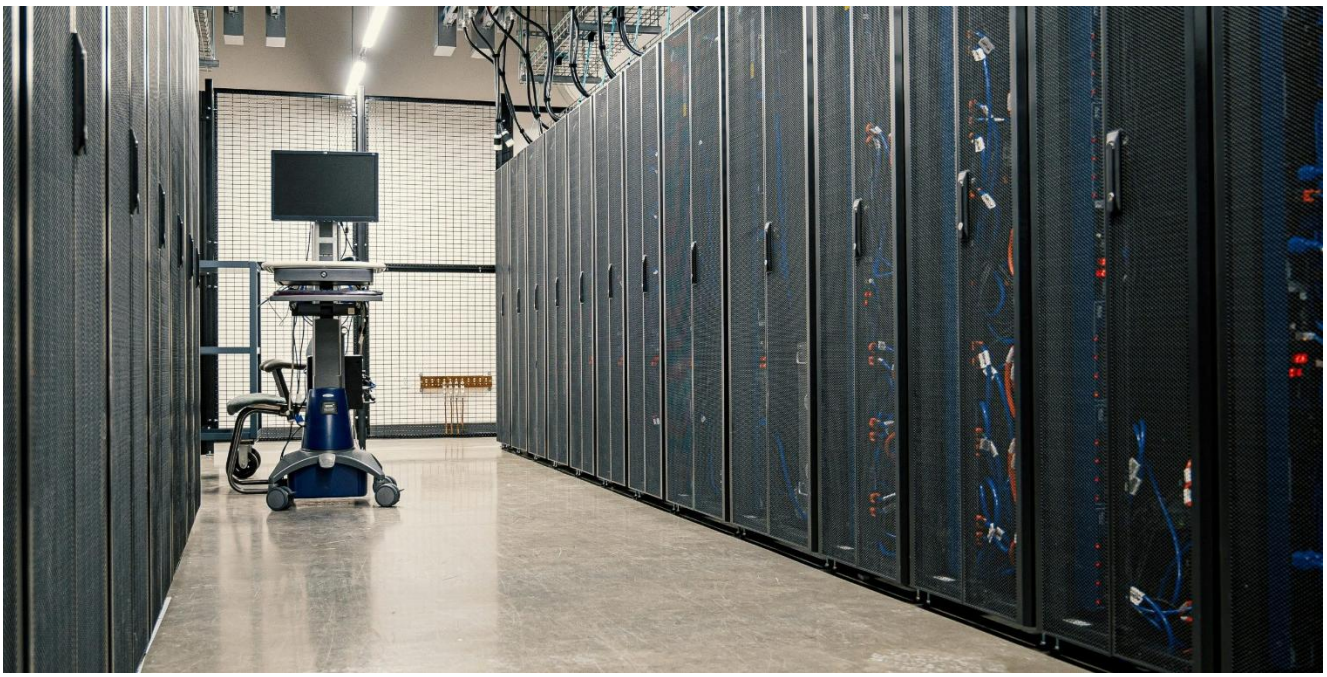
Competency in stakeholder alignment includes translating technical issues into business impacts, clarifying expectations across teams, and maintaining transparency through status updates and requirements summaries. Experience in risk identification and mitigation includes recognizing system dependencies, anticipating operational constraints, and developing structured SOPs and sequencing guides to reduce uncertainty during execution.

Requirements gathering capabilities include working with diverse stakeholders to extract functional and non-functional requirements, organizing them into structured documentation, and confirming interpretation accuracy. Process improvement experience includes creating new workflows, standardizing undocumented procedures, reducing single-point-of-failure risk, and replacing legacy tribal-knowledge processes with validated SOPs, diagrams, runbooks, and onboarding materials.

This portfolio collectively demonstrates a project-oriented approach focused on clarity, risk management, repeatability, and measurable operational improvement.

Project Index

Case Study 1: Data Center Shutdown Procedure



Project Overview	Details
Environment	Data Center
Objectives	Develop a structured, repeatable shutdown and startup procedure to coordinate sequence, protect critical hardware and logistics data integrity, and reduce operational and equipment risk during planned maintenance.

Details

Collaboration	Operations | Cybersecurity | Facilities | Engineering
Approach	Created shutdown sequencing workflow based on technical dependencies, documented risk and control steps, and coordinated execution with all business and infrastructure stakeholders.
Outcome	Reduced the risk of equipment damage and enabled repeatable, controlled shutdowns and startups, minimizing downtime duration and uncertainty.

Deliverables

Deliverable	Description
Shutdown SOP	Standard Operating Procedure document detailing the full power-down and power-up sequence.
Sequencing Checklist	Step-by-step checklist for execution used by multiple teams during maintenance windows.
Risk/Control Documentation	Analysis of potential risks (e.g., data corruption, component failure) and mitigation steps.
Supporting documentation for this procedure is provided in Exhibit A.	

Case Study 2: Equipment Cost-Saving Deployment

Project Overview	Details
Environment	Enterprise IT
Objectives	Execute a cost-efficient modernization of student and faculty devices while reducing long-term hardware replacement costs.

Details

Collaboration	Administrators | Staff
Approach	Conducted requirements analysis based on operational needs, evaluated mobile device options for cost and longevity, and led the deployment, configuration, and onboarding process across regional hubs.

Outcome	Reduced hardware costs and improved device uptime district wide.

Deliverables

Deliverable	Description
Cost Comparison Data	Data showing the long-term cost savings and Return on Investment (ROI) from the new device rollout model.
Deployment Workflow	Step-by-step plan for device procurement, configuration, and rollout to field teams.
User Onboarding Guides	Guides for employees on using the new devices.

Case Study 3: Inventory & Asset Management Overhaul

Project Overview	Details
Environment	Infrastructure Hardware Storage, Shipping/Receiving, Asset Tracking
Objectives	Restore accountability, rebuild inventory tracking systems, streamline shipping/receiving workflows, and establish audit-ready, scalable asset management processes to support IT infrastructure.

Details

Collaboration	Infrastructure | Operations | Security | Logistics | Program Management
Approach	Conducted full physical inventory, rebuilt the asset-tracking structure, redesigned end-to-end shipping/receiving workflows (as-is/to-be), implemented lifecycle tracking, reorganized the physical staging layout, and

	created new SOPs to eliminate reliance on undocumented knowledge.
Outcome	Improved inventory accountability, reduced operational risk, enhanced cross-team coordination, and established a scalable, fully documented process ready for compliance audits.

Deliverables

Deliverable	Description
Centralized Asset Tracking Register	Rebuilt and reconciled end-to-end asset tracking, including lifecycle status, staging, and audit traceability.
Shipping & Receiving SOP	Standardized workflow for intake, tagging, documentation, transfer, and reconciliation.
Inventory Reconciliation Report	Full physical-to-digital audit comparison with discrepancy corrections.
Workspace Organization & Labeling System	Reorganized physical storage layout, implemented labeling, bin systems, and staging zones for efficiency.
Knowledge Transfer Documentation	Captured undocumented processes, created SOPs, and reduced single-person SME dependency.
Supporting training materials for this overhaul are included in Exhibit B.	

Case Study 4: Legacy SME Knowledge Capture & Transition

Project Overview	Details
Environment	Legacy Systems
Objectives	Capture undocumented SME knowledge for long-term system continuity and develop structured onboarding guides for future engineers.

Details

Collaboration	SMEs | Engineering | Digital Technology | Operations
Approach	Conducted interviews with legacy SMEs, documented workflows, command sequences, and logic flows, and built onboarding guides and continuity SOPs.
Outcome	Reduced single-point-of-failure risk and improved onboarding efficiency.

Deliverables

Deliverable	**Description**
Knowledge Base	Unix-Based Platform Knowledge Base
SME Transition Guide	Guide for transferring expert knowledge.
Workflow Documentation	Diagrams of system logic and command sequences.
Supporting materials, including task tracker and the project charter, are provided in Exhibit C.	

Case Study 5: CMDB Modernization Project

Project Overview	Details
Environment	Cross-functional asset management
Objectives	Develop a proof-of-concept (POC) and requirements package for a modernized Software & Hardware Configuration Management Database (CMDB) to improve lifecycle tracking, asset accuracy, and cross-functional transparency across the organization.

Details

Collaboration	Cybersecurity | Operations | Engineering | Program Management | Infrastructure | Leadership | Asset Management | Finance
Approach	Identify CMDB gaps and clarify lifecycle, compliance, and tracking needs.

	Consolidated those inputs into clear user stories, requirements, and a proof-of-concept model showing how an updated CMDB could improve data accuracy, workflow consistency, and operational visibility across the entire organization.
Outcome	Delivered a unified vision for a modernized CMDB, enabling leadership to evaluate resource needs, platform improvements, workflow updates, and next-phase implementation planning.

Deliverables

Deliverable	Description
CMDB Requirements Summary	Core functional needs for lifecycle tracking, asset tagging, and bulk updates.
User Stories Package	Concise Agile stories outlining expected behavior for key CMDB functions.
POC Workflow Model	High-level workflow showing improved compliance and operational clarity.

The user stories, requirements, and workflow models supporting this modernization effort are included in Exhibit D.

Exhibit A — System Shutdown & Startup Operations Guide

This exhibit provides a detailed technical procedure guide outlining the safe shutdown and startup sequence for the environment. The document captures system dependencies, hardware preparation steps, credential validation, risk-mitigation tasks, and the correct order of operations for powering down and restoring a multi-system architecture.

1. Shutdown Procedure: Critical Sequence

Prerequisites

- All necessary approvals from IT Operations, Cyber Security, DevSecOps and Infrastructure teams have been received before the shutdown process begins.
- Ensure the IP addresses and administrator credentials for the Primary Storage Array, Virtualization Management Cluster (VMC), and all Hypervisors are validated.
- Confirm that all administrative passwords work correctly prior to initiating the shutdown.
- Physically log in to the Primary Storage Array and Hypervisor consoles to verify current status.

Pre-Shutdown Actions

1. SNAPSHOTS

Log in to the VMC and perform snapshots of ALL applicable virtual machines. Verify snapshots performed successfully.

2. AUTOMATED SHUTDOWN

Schedule the Automated Client Shutdown Package to shut down all production workstations. Ensure the package includes a 15-minute timer. Crucially, ensure any administrator workstations are excluded from the package list.

3. AUTO POWER-ON CHECK

Verify the Domain Controller, Application Server, and VMC VM are set to automatically power on in the event of power loss. *(If not set, they must be manually powered on via the Hypervisor console).*

Phase 1: Virtual Machine (VM) Shutdown

1. Power Down UNSUPPORTED VMs

Log in to the VMC and power down ALL Test/Development/Unsupported virtual machines (RMB, use the shutdown guest OS option).

2. Power Down Production VMs

Exhibit B — Receiving, Cable Management & Shipping Training

This exhibit showcases a structured training presentation designed to standardize receiving, cable management, and shipping workflows within the technical operations environment. The training module was created to eliminate inconsistencies, improve hardware handling accuracy, and reduce risk across shipping/receiving tasks.

Exhibit C — Task Tracking Overview

A sample snapshot of the internal tracking board used to document and validate inherited tasks across various systems. This artifact demonstrates the level of detail required to ensure continuity during knowledge transfer and minimize single-point-of-failure risk.

Process Documentation Task Tracker

Task	Status	Urgency	Notes
Daily			
Monitor Legacy Mainframe Login Failures and unauthorized access attempts.	🟡		SOP for escalating security events and unlocking accounts.
Check Critical Error Log (CEL) for the Tier 1 Inventory Processing Application for anomalies.	🟡		SOP for diagnosing common application errors (e.g., memory overflow, service failure).
Verify Real-Time Data Replication Health between the primary server and the standby failover node.	✅		Runbook for diagnosing replication latency or failure scenarios.
Confirm scheduled End-of-Day (EOD) Batch Jobs (e.g., inventory reconciliation) completed successfully.	🔵		Checklist for validating EOD output reports and restart procedures.
Weekly			
Review System Backup Integrity (check log success, perform random test restores) for the legacy database.	🔴		SOP detailing the weekly tape rotation, offsite transfer, and test restoration procedure.
Audit User Access Changes and security group modifications made in the legacy system during the previous week.	🟡		Procedure for reviewing access logs, validating changes against approved tickets, and revoking unauthorized access.
Prepare and distribute Weekly Performance Metrics Report on CPU, memory, and disk utilization to IT leadership.	✅		Template for the weekly report format, data extraction method, and distribution list.
Clean up temporary files, perform disk defragmentation, and archive non-critical system logs older than 90 days.	🟢		Runbook for log archiving commands and approved storage location.
Monthly			
Analyze Capacity Trends (database size, storage usage) and forecast resource needs for the next 6-12 months.	✅		Methodology document for capacity forecasting and procurement request submission.
Review and update the Disaster Recovery (DR) Plan for the legacy environment (e.g., contact lists, restoration sequence).	🔴		SOP for annual review cycle and procedure for executing the DR failover test (e.g., running the OS image on a virtual machine).
Conduct Vulnerability and Patch Management Review and coordinate with operations to apply critical OS/application patches.	🟡		Procedure for patch testing in the development environment and scheduling production deployment windows.
Validate Operational Runbooks and System Diagrams for accuracy against the current production environment configuration.	🟢		Checklist for validating system documentation and submitting corrections to the centralized knowledge base.

✅ = Completed	🟡 = In Progress	Low
🟢 = Ready for Review	⚪ = Pending / Not Assigned	Medium
🔵 = On Hold	🔴 = Not Yet Started	High

This Project Charter provides the foundational scope and business justification for the Legacy Platform Knowledge Capture Initiative. As an artifact, it demonstrates your ability to structure complex projects by formally defining objectives, key deliverables, and detailed scope (including what is out-of-scope). Furthermore, it highlights competence in risk management by identifying operational risks, such as single-point-of-failure dependency, and formally outlining the necessary mitigation strategies to ensure system continuity and operational stability.

PROJECT CHARTER

Project Purpose / Business Need

Critical operational and troubleshooting knowledge for the Legacy Computing Platform resides with a limited number of Subject Matter Experts (SMEs). Many essential tasks are currently executed via undocumented procedures and ad-hoc troubleshooting. This creates high operational risk, slows system recovery times, and creates an unhealthy dependency on individuals rather than standard processes.

The project exists to capture, formalize, and transition this critical SME knowledge into documented, repeatable, and auditable processes, ensuring system continuity and readiness for core enterprise operations.

Project Objectives

1. Identify and capture all routine and on-demand system maintenance tasks performed by current SME staff.
2. Develop complete, accurate, and standardized process documentation for the platform's core operations.
3. Establish a repeatable onboarding and knowledge-transfer framework for future maintainers.
4. Reduce single-point-of-failure risk and increase system stability.
5. Enable support scalability and improve training efficiency for support personnel.
6. Provide leadership with objective visibility into system support readiness and risk profile.

Scope Definition

In Scope

- Inventory of all tasks performed by SME staff across the platform's subsystems.
- Documentation of all task frequencies (daily, weekly, monthly, on-demand)
- Review of logs, system close-out procedures, and routine reports.
- Development of SOPs, runbooks, and step-by-step guides.
- Creation of exhibits (task tracker, process flow diagrams, knowledge maps)
- Formal transition of responsibilities from existing SME to new maintainers.

Out of Scope

- Hardware refresh or system modernization activities.
- Software rewrite or migration off the Legacy Computing Platform.
- Deep security remediation beyond documentation alignment.
- Any changes to program funding outside of this knowledge initiative.

This presentation outlines a structured SME transition and task-documentation initiative designed to capture, standardize, and transfer legacy system responsibilities. It highlights current risks, defines the scope of daily through annual workflows, and presents a phased 12–24-month roadmap to ensure continuity, reduce single-point-of-failure exposure, and strengthen long-term operational support.”

AGENDA

- CURRENT STATE: WHERE WE ARE TODAY
- WHY THIS INITIATIVE MATTERS
- SCOPE OF WORK: TASK DOCUMENTATION OVERVIEW
- ROADMAP: NEXT 12–24 MONTHS
- METRICS & REPORTING: HOW WE’LL SHOW VALUE
- CALL TO ACTION & NEXT STEPS

ROADMAP: NEXT 12–24 MONTHS

- **PHASE 1 (0-3 MONTHS):** CAPTURE AND DOCUMENT HIGH-FREQUENCY TASKS (DAILY/WEEKLY)
- **PHASE 2 (3-12 MONTHS):** DOCUMENT MONTHLY/YEARLY/ON-DEMAND TASKS; TRANSFER OWNERSHIP
- **PHASE 3 (12-24 MONTHS):** OPERATIONALIZE SME ROLE: MONITORING, REPORTING, CONTINUOUS IMPROVEMENT
- REGULAR STAKEHOLDER REVIEWS (MONTHLY UPDATES, QUARTERLY DEEP DIVES)

Exhibit D — CMDB User Stories, Use Cases & Requirements

This exhibit compiles the user stories, acceptance criteria, and requirements that shaped the CMDB modernization POC. Drawn from stakeholder workshops and operational gap analysis, the materials outline improvements to baseline management, inventory tracking, lifecycle visibility, project workflow integration, and capital-asset governance.

CONFIGURATION DATABASE (CMDB) REQUIREMENTS & USER STORIES

1. INVENTORY LIFECYCLE MANAGEMENT

SOFTWARE BASELINE & END-OF-LIFE (EOL) MANAGEMENT

USER STORY	As a Software Asset Manager, I want the ability to include End-of-Life (EOL) dates for software baselines in the Configuration Database, so that I can proactively manage software lifecycle, plan upgrades, and maintain compliance.
ACCECPTANCENCE CRITERIA	* The CMDB administrator can add and update EOL dates for all recorded software baselines. * The EOL date must be selected from a date-picker or dropdown menu to ensure consistent data format and reduce entry errors.

2. DATA MANAGEMENT AND USABILITY

BULK UPLOAD CAPABILITY

USER STORY	As an IT Asset Manager, I want the ability to perform bulk uploads of hardware and software data, so that I can efficiently populate and maintain the CMDB after large deployments or inventory refreshes.
ACCECPTANCENCE CRITERIA	* A bulk upload feature is available for authorized users to upload data (e.g., CSV, Excel). * Access controls are in place to restrict the feature to authorized personnel only. * Validation checks are performed during the upload process to ensure data quality and consistency. * A comprehensive log and audit trail is created for all bulk uploads.

3. FINANCIAL AND PROJECT GOVERNANCE

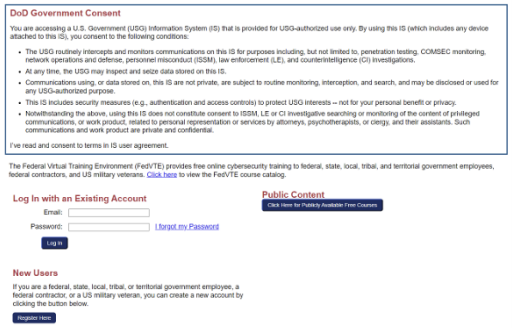
CAPITAL ASSET TRACKING AND OVERSIGHT

USER STORY	As a Finance & Asset Inventory Manager, I want to assign a Capital ID tag to hardware that requires special tracking, so that I can maintain accurate asset accounting and comply with financial reporting and regulatory requirements.
ACCECPTANCENCE CRITERIA	* A dedicated Capital ID field is available and distinct from the standard Asset Tag field. * Immediate notifications (e.g., email alerts) are sent to designated Finance stakeholders whenever any change is made to a capital asset's status or location. * Reports are available to view the status, location, and history of all capital assets based on their Capital ID.

Exhibit E — Federal Virtual Training Environment Skills Development

This exhibit demonstrates ongoing professional development through the FedVTE platform, which provides government-backed training in cybersecurity, incident response, cloud security, risk management, and forensics. The coursework strengthens foundational security knowledge and aligns with CompTIA, CISSP, CEH, and other industry frameworks, directly supporting the Business Analyst role's expectations for security-conscious process design, compliance awareness, and collaboration with IT and security engineering stakeholders.

WHAT IS FEDVTE?



- FedVTE is a free online platform providing virtual training environments for government employees and partners.
- Specifically, the FedVTE access policy states that the following individuals are eligible to access the platform:
  - Federal government employees
  - Members of the U.S. military
  - Non-federal users sponsored by a federal agency or organization
  - State and local government personnel sponsored by a federal agency
  - Employees of private companies that contract with the federal government, sponsored by their government customer
- It offers a wide range of IT and Cyber Security courses, labs, and resources.

2

ADVANTAGES FOR RECERTIFICATION

FedVTE Training Courses

Training approved in this document is based on the exam objectives:

- A+ 220-1001 and 220-1001
- Network+ N10-008
- Security+ SY0-601
- Linux+ XK0-004
- Cloud+ CV0-002
- PenTest+ PT0-002
- CySA+ CS0-003
- CASP+ CAS-004

Activity name to use when uploading CEUs into a certification record:

Complete a Training Course

CEU Required Documentation

The certified professional must upload a certificate of completion into their certification record as proof of attendance.

Completion Certificate

- Your name
- Name of the course
- Name of the training provider
- Date the course was completed
- Number of hours

- Convenient online access
- Wide range of courses for various certifications
- Cost-effective way to earn CEUs
- Enhance your skills and stay up-to-date
- Self-paced learning at your convenience
- Hands-on virtual labs for practical experience
- Access to the latest course materials and resources
- Tracking and reporting tools for CEU credits
- Aligns with industry-recognized certification requirements
- Supports continuous professional development

5

Exhibit F — Program Tracker / Project Tracking System

This exhibit presents a comprehensive program-tracking system designed to improve accountability and communication across closed-area IT programs. Features include a timestamped working log, administrative procedures, troubleshooting guides, reference libraries, and new-hire onboarding modules. This centralized tracking approach reflects the Business Analyst's responsibility to enhance documentation quality, manage workflows, improve visibility for leadership, and streamline communication channels across technical and operational teams.

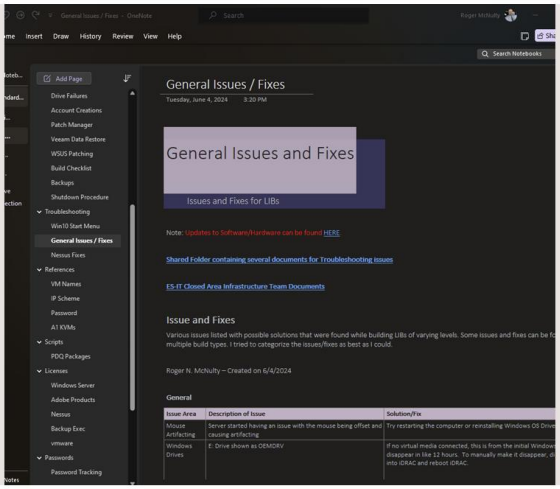
2

Introduction

A comprehensive OneNote solution for managing and tracking Program in Closed Areas

Key features:

- Working Log
- Administrative
- Procedures
- Troubleshooting
- References
- Checklists
- New Hires Information



4

Existing Challenges

- Lack of centralized documentation and communication.
- Difficulty in tracking what tasks have been completed and by whom.
- Difficulty tracking task completion and accountability.
- Lack of visibility into program status and progress.
- Lack of accountability due to non-standardized task tracking.
- Poor communication between team members in closed areas.