**ROGER MCNULTY**

**Business Systems Analyst, IT & Security**

**PROFESSIONAL PORTFOLIO | 2026** **Business**

**CORE COMPETENCIES**

Requirements Engineering in Regulated Environments

System Dependency and Workflow Analysis

Operational Risk Reduction and Continuity Planning

Configuration and Change Enablement

IT Service Management and Compliance Alignment

**QUALIFICATIONS & EDUCATION**

Top Secret Clearance

ECBA (In Progress)

MBA – Business Analytics (In Progress)

**Purpose of This Portfolio:**  
This portfolio presents my work supporting IT and Security organizations in regulated and classified environments. The materials demonstrate how I clarify requirements, document undocumented systems, reduce operational risk, and support-controlled change in mission-critical programs.

All company names, system identifiers, and sensitive details have been anonymized to protect confidentiality. Each case study reflects real analytical and operational work performed in defense and regulated settings, with a focus on continuity, compliance, and risk management rather than visibility or scale.

**How to Use This Portfolio:**  
This portfolio is designed for hiring managers, technical leaders, and IT & Security partners who want to understand how I operate in high-consequence environments. It includes:

Case studies show how I translate business and operational needs into clear system requirements, map dependencies, eliminate single points of failure, and support disciplined change in regulated programs.

Selected artifacts that demonstrate documentation quality, requirements clarity, and continuity planning, including SOPs, workflow diagrams, user stories, and risk-aware process models.

The portfolio can be reviewed sequentially or referenced selectively based on role focus, whether that is requirements engineering, service management, system behavior analysis, or compliance-driven process improvement.

**Table of Contents**

[About Me 2](#_Toc219414029)

[Project Index 4](#_Toc219414036)

Project Case Studies

[Case Study 1: IT Service Impact Analysis 5](#_Toc219414037)

[Case Study 2: Data Center Dependency Mapping 7](#_Toc219414038)

[Case Study 3: Asset Management And Audit Readiness 9](#_Toc219414039)

[Case Study 4: Asset Management And Audit Readiness 11](#_Toc219414040)

[Case Study 4: Legacy Sme Knowledge Capture 14](#_Toc219414041)

[Case Study 5: CMDB Modernization 16](#_Toc219414042)

Exhibits & Artifacts

[Exhibit A — Service Impact & Capacity Analysis 18](#_Toc219414043)

[Exhibit B — System Shutdown & Startup Operations Guide 19](#_Toc219414044)

[Exhibit C — Continuity & Knowledge Transfer Framework 20](#_Toc219414045)

[Exhibit D — CMDB User Stories, Use Cases & Requirements 23](#_Toc219414046)

[Exhibit E — Program Tracker / Project Tracking System 24](#_Toc219414047)

# About Me

|  |
| --- |
| Linkedin Profile ImageI specialize in bringing structure to complex, regulated systems where continuity, compliance, and security cannot be compromised. My work centers on documenting what is undocumented, clarifying ownership where it is unclear, and partnering with engineering and cybersecurity teams to reduce operational risk and make change safer.  Across defense and enterprise IT environments, I have supported mission-critical systems by mapping dependencies, reverse-engineering legacy workflows, and formalizing procedures that previously relied on tribal knowledge. This approach strengthens audit readiness, improves service reliability, and ensures that modernization efforts do not introduce unnecessary exposure.  My background includes military leadership and years of experience in classified environments, which shape a disciplined, detail-oriented approach to business systems analysis. I focus on being a trusted partner to IT and Security leadership, translating business priorities into clear requirements and helping organizations deploy compliant, resilient, and sustainable capabilities. |

| **Detail** | **Description** |
| --- | --- |
| **Education** | MBA – Business Analytics (in progress) |
| **Primary Focus** | Infrastructure and operations analysis  Requirements gathering in regulated environments  Risk identification and continuity planning  Process documentation and workflow modeling  Configuration and change management support |

Business Analysis Competency Summary  
My experience as a Business Systems Analyst has been shaped by work in classified and highly regulated environments where clarity, accuracy, and reliability are essential.

# **Requirements Engineering**

I gather and validate business and system requirements through stakeholder interviews, workflow observation, and technical analysis. I document functional and non-functional requirements using BRDs, FRDs, user stories, and acceptance criteria to support controlled, predictable development.

# **Systems and Workflow Analysis**

I reverse-engineer undocumented processes, map end-to-end workflows, and analyze system dependencies to expose risk, clarify constraints, and support modernization decisions.

# **Process Documentation and Continuity**

I develop SOPs, lifecycle guides, and system maps that eliminate reliance on tribal knowledge and support training, sustainment, and operational readiness.

# **Testing and Validation**

I support functional testing and User Acceptance Testing to ensure system changes meet operational and security requirements before deployment.

# **Service Management and Improvement**

I apply IT service management principles to incident, change, and continuity practices, helping organizations improve reliability while maintaining compliance and security posture.

# **Cross-Functional Collaboration**

I work closely with engineering, cybersecurity, operations, facilities, and leadership teams to ensure shared understanding and alignment across technical and non-technical stakeholders.

# Project Index

**IT Service Impact Analysis**

**System Dependency Mapping for Data Center Operations**

**Asset Management Workflow Redesign for Compliance and Accountability**

**Legacy System Knowledge Capture and Continuity Planning**

**CMDB Modernization, Requirements and Workflow Modeling**

Selected artifacts include SOPs, dependency diagrams, requirements packages, user stories, and continuity documentation that demonstrate disciplined analysis in regulated environments.

# Case Study 1: IT Service Impact Analysis



**Project Overview**

Evaluated a proposed endpoint-management automation initiative in a regulated IT environment to assess long-term service sustainability, cybersecurity exposure, and workforce impact. The objective was to support IT & Security leadership with a risk-aware, ITIL-aligned analysis that ensured modernization improved service delivery without introducing hidden operational or compliance risk.

| **Approach** | **Details** |
| --- | --- |
| **Requirements elicitation** | Partnered with engineering, cybersecurity, and service owners to clarify functional needs, security constraints, and long-term support expectations. |
| **Service impact analysis** | Assessed the proposal through the lens of IT service management, focusing on change enablement, service continuity, and operational resilience rather than feature delivery alone. |
| **Capacity and workforce assessment** | Analyzed long-term maintenance and support requirements to understand FTE impact, technical debt accumulation, and sustainability of the proposed solution. |
| **Option comparison** | Evaluated alternative implementation approaches, including a lean scripting model that preserved functionality while reducing complexity and security exposure. |
| **Decision-support documentation** | Translated technical risk into operational impact through a structured briefing for IT & Security leadership, supporting informed, risk-balanced decision making. |

| **Outcome** |
| --- |
| ▪ Enabled IT & Security leadership to make a risk-informed modernization decision balancing efficiency with long-term service sustainability.  ▪ Supported a pivot to a solution that met operational needs while reducing maintenance burden and cybersecurity exposure.  ▪ Strengthened alignment between service delivery goals and security posture.  ▪ Reinforced disciplined change governance using ITIL-aligned service impact analysis. |

| **Key Deliverables** |
| --- |
| ▪ Service Impact & Risk Assessment Summary  ▪ Capacity and Workforce Impact Analysis  ▪ Comparative Implementation Options Matrix  ▪ Change Enablement & Risk Considerations Brief |
| *Supporting documentation for this procedure is provided in Exhibit A.* |

# Case Study 2: Data Center Dependency Mapping



**Project Overview**

Analyzed and documented the shutdown and startup dependencies of a classified data center environment to eliminate tribal knowledge, reduce operational and hardware risk, and establish a standardized, repeatable workflow across engineering, cybersecurity, operations, and facilities teams.

| **Approach** | **Details** |
| --- | --- |
| **Requirements elicitation** | Interviewed engineering, cyber, operations, and facilities teams to identify technical dependencies, functional constraints, and non-functional requirements (data integrity, safety, timing). |
| **Workflow modeling** | Reverse-engineered undocumented steps and developed clear workflow and dependency diagrams illustrating system relationships and required pre-conditions. |
| **Gap analysis** | Identified inconsistencies in execution, lack of documentation, and risk caused by sequence variation across teams. |
| **Process documentation** | Authored standardized SOPs and a condensed sequencing checklist to ensure repeatable, auditable execution. |
| **Cross-functional alignment** | Facilitated validation sessions with engineers and cyber teams to confirm sequence accuracy and risk controls. |

| **Outcome** |
| --- |
| ▪ Eliminated reliance on tribal knowledge through clear, system-focused documentation.  ▪ Reduced hardware and data-integrity risk during maintenance events.  ▪ Improved communication and shared understanding across all technical teams.  ▪ Established a repeatable, approved workflow supporting future modernization efforts. |

| **Key Deliverables** |
| --- |
| ▪ Shutdown/Startup SOP  ▪ Sequencing Checklist  ▪ System Dependency Diagram  ▪ Risk & Control Summary |
| *Supporting documentation for this procedure is provided in Exhibit B.* |

# Case Study 3: Asset Management and Audit Readiness



**Project Overview**

Led requirements gathering and functional analysis to support a cost-efficient modernization of end-user devices across a distributed enterprise environment. The goal was to reduce long-term hardware costs, improve reliability, and ensure device selections aligned with operational needs.

| **Approach** | **Details** |
| --- | --- |
| **Requirements elicitation** | Interviewed administrators, faculty, and technical staff to identify workflows, performance expectations, application needs, and usability requirements. |
| **Functional evaluation** | Compared device models based on lifespan, maintenance requirements, compatibility with enterprise tools, and user experience feedback. |
| **Workflow assessment** | Analyzed current provisioning and onboarding processes to determine inefficiencies, training gaps, and points of friction. |
| **Documentation** | Produced clear deployment workflows, readiness checklists, and user onboarding materials to standardize rollout and reduce support demand. |

| **Outcome** |
| --- |
| **▪**  Reduced total cost of ownership through targeted device selection informed by functional requirements and lifecycle analysis.  **▪**  Improved end-user reliability and performance by aligning device capabilities with real operational needs.  **▪**  Standardized provisioning and onboarding workflows, decreasing downtime and ensuring consistent adoption across the organization.  **▪**  Enhanced transparency for leadership through concise cost-benefit documentation and recommendations. |

| **Key Deliverables** |
| --- |
| **▪** Functional Requirements Summary  **▪** Cost Comparison & Analysis Report  **▪** Deployment Workflow Diagram  **▪** End-User Onboarding Guides |

# Case Study 4: Asset Management and Audit Readiness



**Project Overview**

Conducted a full assessment and redesign of asset management workflows across storage, shipping/receiving, and tracking functions. The objective was to restore accountability, improve audit readiness, eliminate undocumented processes, and create a scalable, standardized asset lifecycle model supporting mission-critical IT infrastructure.

| **Approach** | **Details** |
| --- | --- |
| **Requirements elicitation** | Engaged infrastructure, operations, logistics, security, and program teams to identify pain points, compliance needs, lifecycle gaps, and system constraints. |
| **Workflow analysis** | Mapped as-is processes for intake, tagging, reconciliation, storage, staging, and shipping to identify inefficiencies, bottlenecks, and points of failure. |
| **Product redesign** | Developed to-be workflows that improved traceability, clarified responsibilities, aligned cross-team handoffs, and supported compliance requirements. |
| **Documentation** | Created SOPs, process maps, lifecycle models, and reconciliation tools to eliminate reliance on tribal knowledge and ensure consistent execution. |
| **Asset Lifecycle improvement** | Implemented a structured asset-tracking register that provided visibility into status, location, and movement history for all tracked hardware. |

| **Outcome** |
| --- |
| **▪**  Established clear, standardized end-to-end asset processes used across multiple teams.  **▪**  Improved accuracy and audit readiness through reliable lifecycle tracking and documentation.  **▪**  Reduced risk tied to undocumented workflows and single-person SME reliance.  **▪**  Enhanced operational coordination and reduced processing timelines.  **▪**  Provided leadership with visibility into inventory status and workflow performance. |

| **Key Deliverables** |
| --- |
| **▪** Asset Management Lifecycle Workflow Maps  **▪** Centralized Asset Tracking Register  **▪** Shipping & Receiving SOP  **▪** Workspace Organization & Labeling System |
| *Supporting documentation for this procedure is provided in Exhibit B.* |

# Case Study 4: Legacy SME Knowledge Capture



**Project Overview**

Captured undocumented system knowledge and reconstructed operational logic for a legacy, mission-critical environment previously dependent on single-point SMEs. The goal was to analyze system behavior, document command sequences, and create clear reference materials enabling sustainment, onboarding, and continuity for future technical staff.

| **Approach** | **Details** |
| --- | --- |
| **Knowledge extraction** | Conducted structured interviews and shadow sessions with outgoing SMEs to capture operational steps, system logic, dependencies, and critical nuances not documented elsewhere. |
| **System logic analysis** | Reverse-engineered workflows and command sequences to clarify what the system does, why specific steps are required, and how components interact. |
| **Workflow documentation** | Developed detailed, step-by-step procedures and high-level logic diagrams describing data flow, system triggers, and operational states. |
| **Risk identification** | Analyzed failure modes related to incorrect sequencing, missing prerequisites, or improper parameter use; defined controls to mitigate operator error. |
| **Training enablement** | Produced onboarding materials and process explanations enabling new engineers to understand, operate, and troubleshoot the system safely and consistently. |

| **Outcome** |
| --- |
| **▪**  Eliminated reliance on tribal knowledge linked to retiring SMEs.  **▪**  Improved sustainment readiness by providing engineering-grade documentation.  **▪**  Reduced operational risk by clarifying required sequencing, dependencies, and failure points.  **▪**  Enabled faster, more structured onboarding for new analysts and engineers.  **▪**  Strengthened continuity planning across classified programs. |

| **Key Deliverables** |
| --- |
| **▪** System Logic Diagram & Dependency Map  **▪** Operator Workflow Guide  **▪** SME Knowledge Capture Notes  **▪** Risk / Failure Mode Summary |
| *Supporting documentation for this procedure is provided in Exhibit C.* |

# Case Study 5: CMDB Modernization



**Project Overview**

Led business and system requirements gathering for the modernization of a cross-functional Configuration Management Database (CMDB). The existing process lacked clarity, produced inconsistent data, and caused friction between infrastructure, operations, and cybersecurity teams. The objective was to define structured requirements, model workflows, and create documentation to support a scalable CMDB redesign aligned with enterprise workflows.

| **Approach** | **Details** |
| --- | --- |
| **Stakeholder interviews** | Engaged engineering, operations, cybersecurity, asset management, and ITSM teams to understand pain points, data inconsistencies, and required capabilities. |
| **Requirements engineering** | Documented functional requirements, non-functional requirements, user roles, data fields, validation rules, and integration expectations. |
| **User story development** | Created clear user stories, acceptance criteria, and data-flow considerations to support backlog refinement and development planning. |
| **Gap analysis** | Built current-state and future-state diagrams illustrating intake, lifecycle updates, attribute validation, approval pathways, and system dependencies. |
| **Cross-functional alignment** | Identified breakdowns in data accuracy, hand-off ambiguity, and inconsistencies between teams entering or consuming CMDB data. |
| **Documentation** | Produced conceptual data models, process maps, and requirements packages used to design a more structured and reliable CMDB. |

| **Outcome** |
| --- |
| **▪** Established a unified requirements baseline across all contributing teams.  **▪** Improved data quality expectations through defined validation logic and ownership responsibilities.  **▪** Provided development teams with actionable requirements, reducing ambiguity and rework.  **▪** Enabled consistent lifecycle tracking and audit-ready data for compliance and reporting.  **▪** Strengthened cross-team communication by clarifying workflow interactions and system behavior. |

| **Key Deliverables** |
| --- |
| **▪** Functional & Non-Functional Requirements Package  **▪** User Stories with Acceptance Criteria  **▪** Current-State & Future-State Workflow Diagrams  **▪** Conceptual Data Model  **▪** CMDB Intake & Update Process Map |
| *Supporting documentation for this procedure is provided in Exhibit D.* |

# Exhibit A — Service Impact & Capacity Analysis

|  |
| --- |
| This exhibit documents the analytical artifacts used to support a risk-informed modernization decision for an endpoint-management initiative in a regulated IT environment. The materials demonstrate how IT service management principles were applied to evaluate service sustainability, cybersecurity exposure, and long-term support impact before authorizing change.  Rather than focusing solely on cost efficiency, the exhibit reflects a governance-aligned approach that balances capacity planning, technical debt, and compliance posture to ensure modernization strengthens service delivery without introducing operational risk. |
| |  |  |  |  | | --- | --- | --- | --- | | Analysis Metric | Proposed | Recommendation | Delta / Variance | | Development Time | 320 Hours (8 Weeks) | 40 Hours (1 Week) | -87.5% Time-to-Value | | FTE Overhead (Annual) | 0.25 FTE (Maintenance/Sec) | 0.05 FTE (Updates) | 80% Lower Labor Debt | | Tech Debt / Complexity | High (Custom Integration) | Low (Native Scripting) | Lower Risk Profile | | Cybersecurity Risk | Significant (New Attack Surface) | Negligible (Standard Controls) | Compliance Alignment | | Estimated Year 1 ROI | -14% (Negative ROI) | +210% (High Yield) | Strategic Pivot Justified | |

# Exhibit B — 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. |
|  |

# Exhibit C — Continuity & Knowledge Transfer Framework

|  |
| --- |
| 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. |
|  |
| 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. |
|  |
| 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. |
|  |

# 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. |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | ID | Feature | User Story | Acceptance Criteria | Priority | | REQ-01 | Inventory Lifecycle Management | As a Software Asset Manager, I want the ability to include End-of-Life (EOL) data for software baselines in the Configuration Database, so that I can proactively manage software lifecycle, plan upgrades, and maintain compliance. | The CMDB administrator can add and update EOL data 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. | **High** | | REQ-02 | Data Management and Useability | 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. | 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. | **Low** | | REQ-03 | Financial and Project Governance | 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. | 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. | **Medium** | |

|  |
| --- |
|  |

# Exhibit E — 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. |
|  |