ROGER MCNULTY

Business Systems Analyst, IT & Security

PROFESSIONAL PORTFOLIO | 2026

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

I 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

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.

Approach	Details
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.

Approach	Details
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

Approach	Details
	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

Approach	Details
	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

Case Study 5: 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.

Approach	Details
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 6: 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.

Approach	Details
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

Strategic Modernization Assessment: Governance-Led Decision Matrix

This exhibit demonstrates a governance-aligned approach to infrastructure modernization. By evaluating technical debt, cybersecurity exposure, and FTE capacity alongside ROI, the analysis justifies a strategic pivot away from high-complexity custom integrations. The result is a transition toward native, low-debt solutions that strengthen service delivery and ensure long-term operational stability in a regulated IT environment.

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

Critical System Restoration: Shutdown & Startup Sequence 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 C — Continuity & Knowledge Transfer Framework

Knowledge Transfer Tracker: Eliminating Operational Dependency

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

Foundational Project Charter: Mitigating 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.

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.

Strategic SME Transition Framework & 24-Month Roadmap

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 — Configuration Management & Requirements Lifecycle Framework

This exhibit presents a comprehensive requirements lifecycle for a Configuration Management Database (CMDB) modernization initiative. By integrating strategic business objectives with granular technical specifications and validation testing, these materials demonstrate a disciplined, "BSA Playbook" approach to eliminating tribal knowledge, reducing operational risk, and strengthening audit readiness in mission-critical and classified IT environments.

Business Requirements Document (BRD)

Below is a high-level Business Requirements Document (BRD) for Case Study 6: CMDB Modernization. This document is structured to bridge high-level business goals with regulated IT environment constraints.

1. Executive Summary

The objective of this initiative is to modernize the current Configuration Management Database (CMDB) to eliminate reliance on undocumented "tribal knowledge" and manual tracking. By standardizing asset intake and establishing automated lifecycle alerts, the organization will reduce operational risk, improve audit readiness, and ensure that mission-critical IT infrastructure is maintained according to strict security standards.

2. Business Objectives & Success Criteria

- **Audit Compliance**: Achieve 100% visibility into the "Capital ID" and "Classification" of hardware assets to support regulatory and financial audits.
- **Risk Mitigation**: Proactively identify and flag software reaching "End-of-Life" (EOL) to prevent security vulnerabilities within classified environments.
- **Data Integrity**: Implement automated schema validation for bulk inventory updates to reduce manual entry errors by 40%.
- **Security Governance**: Enforce Role-Based Access Control (RBAC) to ensure only authorized personnel can modify status levels for sensitive assets.

3. Stakeholder Profiles

Stakeholder	Role	Responsibility
IT & Security Leadership	Project Sponsor	Provides strategic direction and risk-balanced decision support.
Engineering / Cyber Teams	Subject Matter Experts	Defines technical dependencies, system behavior, and security constraints.
Asset / Software Managers	Primary Users	Responsible for day-to-day inventory updates and software lifecycle tracking.
Finance / Audit Partners	Compliance Oversight	Validates that the system meets capital asset reporting and regulatory standards.

4. High-Level Business Requirements

ID	Requirement Name	Description	Priority
BR-01	Mandatory Capital Tracking	The system must require a unique "Capital ID" for all hardware assets to ensure auditability.	High 🔴
BR-02	Automated EOL Alerts	The system must automatically compare software dates and trigger visual alerts for upcoming EOL milestones.	High 🔴
BR-03	Bulk Upload Validation	The system must validate the schema of CSV/Excel uploads to prevent "dirty data" from entering the CMDB.	Medium 🟡
BR-04	RBAC Enforcement	The system must restrict "Status" and "Classification" edits to users with the 'Asset Manager' role.	High 🔴

5. Constraints & Assumptions

- **Network Environment:** The system must be capable of operating within air-gapped or restricted classified networks.
- **Regulatory Alignment:** All requirements must align with NIST 800-171 and ITIL service management frameworks.
- **Existing Infrastructure:** Assumes the solution will integrate with existing procurement and shipping/receiving workflows

User Stories & Acceptance Criteria

Drawn from stakeholder workshops and operational gap analysis, these stories translate human needs into functional objectives. They ensure that specific roles—such as Asset Managers and Security Analysts—have the exact capabilities required to maintain baseline management and inventory tracking.

REQ-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** 
REQ-04	Security & Access Governance	As a Security Administrator, I want to restrict "Status" and "Classification" edits to authorized roles only, so that I can prevent unauthorized changes to sensitive configuration items.	Access is restricted via Role-Based Access Control (RBAC). Non-authorized users receive a 403 Forbidden error. All attempts to modify classification levels are logged in the security audit trail.	**High** 

Requirements Traceability Matrix (RTM)

Drawn from stakeholder workshops and operational gap analysis, these stories translate human needs into functional objectives. They ensure that specific roles—such as Asset Managers and Security Analysts—have the exact capabilities required to maintain baseline management and inventory tracking.

Req ID	Business Requirement	Functional Requirement	Technical Component	Test Case / Validation	Status
REQ-01	Maintain 100% audit readiness for capital assets.	System must provide a mandatory "Capital ID" field for hardware.	DB Table: Asset_Master Field: Cap_ID_Primary.	TC-101: Validate field cannot be null on save.	Pass
REQ-02	Manage software security vulnerabilities.	System must display "Software EOL Date" with automated alerts.	UI Logic: Date_Compare() Alert: CSS_Risk_High.	TC-102: Verify asset turns red 30 days prior to EOL.	Pass
REQ-03	Ensure data integrity during bulk updates.	System must perform schema validation on CSV/Excel uploads.	Module: Bulk_Import_Handler (Python/SQL).	TC-103: Attempt upload with invalid data format; verify rejection.	Pass
REQ-04	Prevent unauthorized status changes.	Restrict "Status" field edits via Role-Based Access Control (RBAC).	API: /v1/asset/status Auth: JWT_Claims.	TC-104: Attempt edit with 'Standard User' role; verify 403 Forbidden.	Pass

Software Requirements Specification (SRS) & Data Dictionary

This technical specification defines the exact data types, validation logic, and error-handling protocols for the system. It ensures data integrity by preventing "dirty data" from entering the environment and mandates strict adherence to security classification standards (e.g., CUI, Secret, TS).

Field Name	Data Type	Mandatory?	Validation Logic / Constraints	Security/Audit Note
Asset_Tag	Alphanumeric	YES	Format: AT-XXXXX (5 digits). Must be unique in the database.	Primary Key for hardware tracking.
Capital_ID	String	YES	Minimum 8 characters. Must	Essential for financial audit readiness.

			match Finance Dept. regex pattern.	
Software_EOL	Date	NO	Format: YYYY-MM-DD. Must not be a date in the past.	Triggers automated "Risk" alerts in UI.
Owner_Role	Dropdown	YES	Values: Engineering, Cyber, Operations, Admin.	Defines access permissions for the CI.
Classification	String	YES	Values: Unclassified, CUI, Secret, TS.	Crucial: Directs asset storage in secure zones.

Risk & Control Matrix (RACM)

This matrix outlines the specific safeguards built into the CMDB to ensure security and compliance.

Risk ID	Risk Description	Control Activity (Mitigation)	Control Type	Validation (Test Case)
RSK-01	Unauthorized Change: Unprivileged users modify a system's security classification.	RBAC Enforcement: The Classification and Status fields are restricted to the "Security Admin" role via JWT-based authorization.	Technical	TC-104: 403 Forbidden error logged for non-authorized edits.
RSK-02	"Dark" Assets: Hardware enters the environment without a Capital ID, causing audit gaps.	Mandatory Schema Validation: The Bulk Import Handler rejects any record missing a valid, unique Asset_Tag or Capital_ID.	Technical	TC-103: System rejects upload with null mandatory values.
RSK-03	Tribal Knowledge Dependency: Single-point-of-failure risk if SMEs depart without documentation.	SME Knowledge Capture: Structured shadowing and standardized SOPs for all legacy workflows.	Admin	Exhibit C: Validated task boards and knowledge transfer frameworks.
RSK-04	Stale Security Posture: Software remains in use beyond its End-of-Life (EOL) date.	Automated EOL Alerting: System triggers visual "Risk" alerts 30 and 60 days prior to EOL milestones.	Technical	TC-102: Verification of CSS-based color coding in asset views.

Lessons Learned & Project Reflection

This modernization initiative served as a practical application of my MBA – Business Analytics coursework and ECBA study, particularly in the areas of stakeholder alignment and data governance.

Key Takeaways

1. **Bridge the Strategic-Technical Gap:** By starting with a BRD, I learned to secure leadership buy-in by focusing on Audit Readiness and ROI before moving into technical implementation.
2. **Eliminating Single Points of Failure:** The transition from tribal knowledge to a formal SRS and Data Dictionary proved that clear documentation is a security control in itself, ensuring continuity even as personnel change.
3. **Data Integrity as a Security Baseline:** Implementing schema validation for Bulk Imports taught me that "clean data" is a prerequisite for accurate security reporting. If the Classification field is unreliable, the entire security posture is compromised.
4. **The Power of Traceability:** Maintaining an RTM reinforced the importance of validation. It ensures that every technical feature built directly serves a business objective, preventing "scope creep" and ensuring the project remains compliant with NIST 800-171 standards.