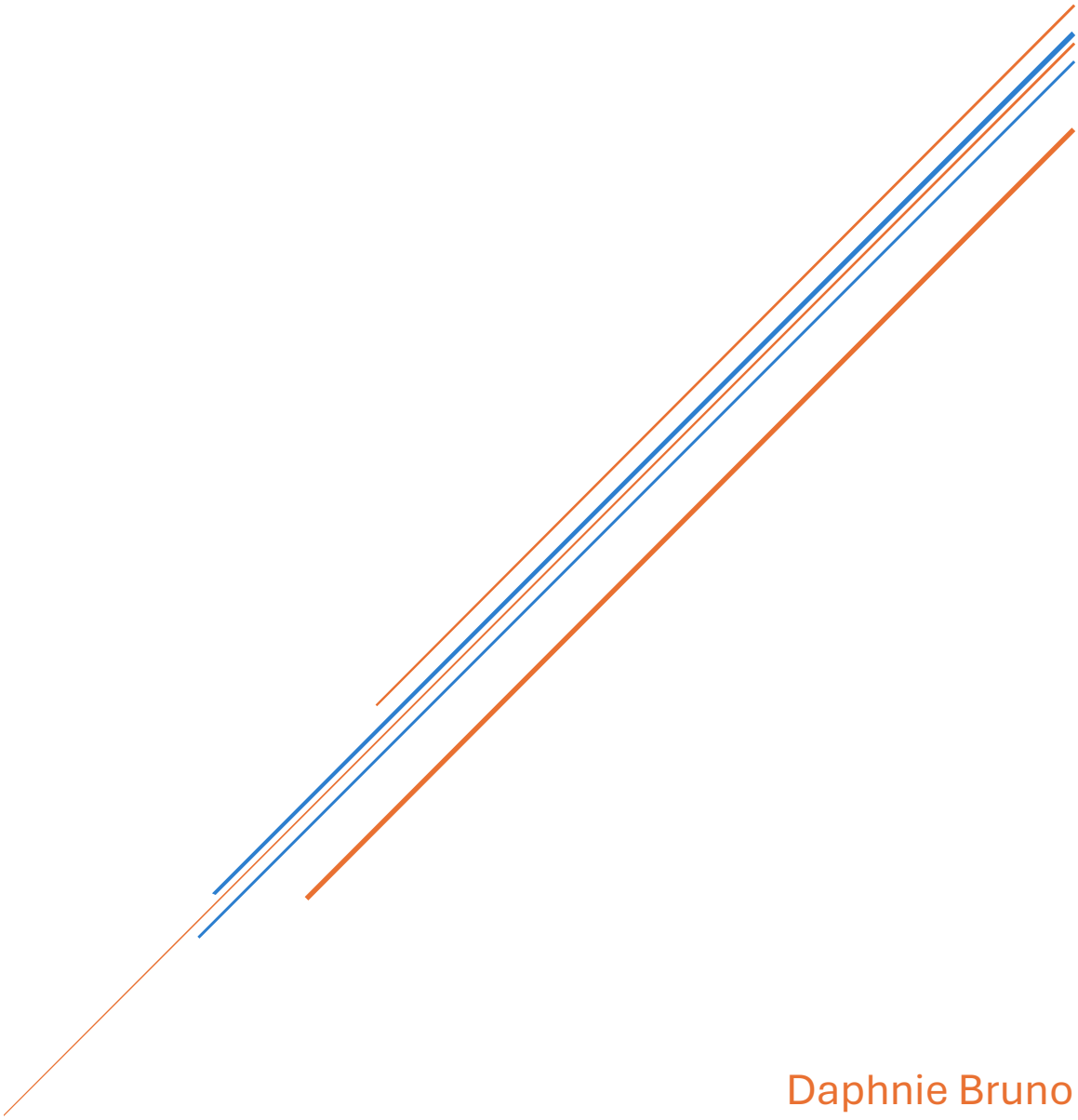
CASE STUDY:
SYSTEM LIFE CYCLE PLAN



Daphnie Bruno
Prof: Bill Moran
March 2025

Priority Order of Planning Phase Processes:

OP.1: Project Planning Process

AQ.1.1: Establish Acquisition Strategy

AQ.1.2: Define System Requirements

OP.2: Risk Management Process

AQ.1.3: Identify Potential Suppliers

AQ.1.4: Develop Solicitation Package

OP.3: Infrastructure Management Process

OP.4: Quality Management Process

OP.5: Decision Management Process

AQ.2.1: Evaluate Supplier Proposals

AQ.2.2: Select Suppliers

AQ.2.3: Award Contracts

RM.1: Risk Monitoring and Assessment

IM.1: Incident Management and Response

QA.1: Quality Assurance and Continuous Improvement

OP.6: Configuration Management Process

OP.7: Information Management Process

VE.1: Verification of System Security and Functionality

VA.2: Vulnerability Assessment and Patch Management

OP.3: Optimization of Performance and Security Controls

MA.4: Maintenance and Corrective Actions

Phase 2 (planning phase) of the Life Cycle and need to review the "Acquisition (AQ)" section of the Framework. For ALL the items in the AQ section, document in priority order all the processes.

Priority Order:
AQ.1.1: Establish Acquisition Strategy
AQ.1.2: Define System Requirements
AQ.1.3: Identify Potential Suppliers
AQ.1.4: Develop Solicitation Package
AQ.2.1: Evaluate Supplier Proposals
AQ.2.2: Select Suppliers
AQ.2.3: Award Contracts
AQ.3.1: Monitor Supplier Performance
AQ.3.2: Manage Supplier Relationships

I picked AQ.1.1 Establish Acquisition Strategy as my first priority because it sets the foundation for obtaining what is needed by determining the strategy with budget, timelines, risk, and compliance in mind. With a defined strategy, there will be an alignment with business goals and the creation of a foundation for all acquisition activities. Second is AQ.1.2 Define System Requirements in ensuring potential suppliers are clear on functional specifications, performance criteria, security controls, and regulatory compliance. Clearly defined requirements offer the standard by which proposal evaluations are measured and prevent future misalignment. Having determined system requirements, the following task is AQ.1.3 Identify Potential Suppliers by evaluating vendor capability, financial soundness, and security compliance. A detailed supplier identification process provides us with a competitive and feasible pool of candidates. Then, after potential suppliers have been identified, AQ.1.4 Develop Solicitation Package is next, creating detailed RFPs or RFQs that will provide vendors with the information necessary to develop accurate proposals. The package must include specifications, evaluation criteria, and contract terms for transparency and proper organization. After proposals are received, AQ.2.1 Evaluate Supplier Proposals ensures objective assessment based on predefined criteria, allowing the best options to be considered. AQ.2.2 Select Suppliers follows, focusing on vendors that offer the best balance of cost, technical capability, and strategic fit. Once the best supplier(s) are chosen, AQ.2.3 Award Contracts finalizes the agreement, establishing clear deliverables, timelines, and compliance expectations. Once the contract is in place, AQ.3.1 Monitor Supplier Performance ensures vendors adhere to their contractual obligations through periodic reviews and key performance tracking. Finally, AQ.3.2 Manage Supplier Relationships fosters collaboration, conflict resolution, and long-term engagement to support the success of the project.

By following this structured acquisition process, SnowBe ensures an efficient, compliant, and security-focused strategy that aligns with NIST SP 800-160 guidelines.

Phase 2 (planning phase) of the Life Cycle. They need to plan the processes in the "ORGANIZATIONAL PROJECT-ENABLING PROCESSES" section, document in priority order only the processes you will address specifically for the planning phase.

Priority Order:

OP.1: Project Planning Process
OP.2: Risk Management Process
OP.3: Infrastructure Management Process
OP.4: Quality Management Process
OP.5: Decision Management Process
OP.6: Configuration Management Process
OP.7: Information Management Process

The Project Planning Process (OP.1) is placed first as it establishes the foundation for the project scope, objectives, and deliverables according to business needs and security requirements. The Risk Management Process (OP.2) follows as it identifies, analyzes, and resolves potential security and operational risks before development. Next, the Infrastructure Management Process (OP.3) ensures that the necessary tools, platforms, and network resources are in place to support development. (OP.4) Quality Management would follow because it is incorporated for maintaining compliance with security and performance standards in the initial stage itself. (OP.5) Decision Management is after we have ensured logical decision-making principles applied to each part of the project. Next, we have version control and change controlling which fall under (OP.6) Configuration Management. Finally, (OP.7) Information Management manages secure handling and governing of the information throughout the life cycle of the system.

My prioritization of Organizational Project-Enabling Processes, SnowBe lays a strong foundation for secure and successful software development. One step leads to another, building a well-formulated and risk-aware project environment. With appropriate planning, active control over risks, good infrastructure, and thorough checks on quality, the project is set for success from the get-go. Furthermore, decision-making, configuration management, and secure information handling force the governance and stability necessary for long-term sustainability of the system. The system not only becomes more efficient and secure but also compliant, adaptable, and resilient, set-up for scalable growth and continued improvement for SnowBe.

Phases 7 and 8 (maintenance and evaluation phases) of the Life Cycle and need to monitor and identify issues with the implemented system. Using the processes in the "TECHNICAL MANAGEMENT PROCESSES " section, specifically the RM, IM, and QA processes, document in priority order only the processes you will address specifically for the maintenance AND evaluation phase.

Priority Order of Processes (RM, IM, QA):

RM.1: Risk Monitoring and Assessment
IM.1: Incident Management and Response
QA.1: Quality Assurance and Continuous Improvement

Risk Monitoring and Assessment (RM.1) is first because staying ahead of potential threats is vital to keeping SnowBe's system security intact. Cyber threats are constantly active, and without continuous monitoring, vulnerabilities might not be identified, and the business will be exposed to attacks that could penetrate sensitive customer data. Through the active identification of risks, the team can implement security controls prior to their development into significant issues.

Next, Incident Management (IM.1) is most important in order to deliver a fast and effective response if a security breach or system failure does actually occur. Since no system is ever completely secure from getting attacked, having a defined plan to contain and minimize the effect of incidents immediately can assist in minimizing downtime, financial loss, and damage to reputation. Any delays in respond may result in extended disruptions in operations, upset customers, and it may affect sales.

Finally, Quality Assurance (QA.1) makes SnowBe's software remain stable, secure, and efficient in the long term. Through continuous evaluation, testing, and improvement, the team can maintain high performance and security levels, not letting minor issues turn into major failures. QA also ensures compliance with industry standards, which keeps SnowBe aligned with security best practices.

Together, these processes create an open-minded security belief where risks are identified early, incidents are handled swiftly, and system quality is maintained. Allowing SnowBe to continue growing without compromising on security or customer trust.

Phases 7 and 8 (maintenance and evaluation phases) of the Life Cycle and need to monitor and identify issues with the implemented system. Using the processes in the "TECHNICAL PROCESSES" section, specifically the VE, VA, OP, and MA processes, document in priority order only the processes you will address specifically for the maintenance AND evaluation phase.

Priority Order:

VE.1: Verification of System Security and Functionality
VA.2: Vulnerability Assessment and Patch Management
OP.3: Optimization of Performance and Security Controls
MA.4: Maintenance and Corrective Actions

The team will need to verify SnowBe's system security and functionality, this is why Verification of System Security (VE.1) is first. Verifying that it is running as anticipated, meeting security requirements, and protecting customer data is key prior to evaluating any other aspect of the system. Without this any hidden vulnerabilities may not be detected, and therefore, breaches may occur.

Once the integrity of the system is confirmed, Vulnerability Assessment (VA.2) will now take top priority to proactively identify and correct vulnerabilities. Cyber-attacks are constantly evolving, so regular vulnerability tests will ensure SnowBe remains in front of the growing security threats. This not only will defend the system against attacks, but it also increases stakeholders' and customers' confidence.

Now we will need Optimization of Performance (OP.3) which will follow the need to enhance the efficiency and security measures so that SnowBe's software runs smoothly. A system may be secure, but if it is slow, then it may become frustrating for the users, hindering productivity. Optimizing performance and security maintains the team confirming users are enjoying a painless experience and still have tough protective measures.

Finally, Maintenance and Corrective Actions (MA.4) enable the system to continually improve itself, get updated, and get corrected. No software ever remains static when new threats are introduced. Through an ongoing maintenance process, SnowBe ensures that its system is solid, secure, and will accommodate as the business grows.

Using this organized procedure, SnowBe is not just addressing security concerns but constructing an environment which is secure, high performance, and sustainable. By validation, vulnerability management, optimization, and regular maintenance, the company is creating a strong technological foundation that supports business growth, customer trust, and long-term success.

Describe the importance of the NIST 800-160 v1 AND the 9 step life cycle as it relates to this assignment.

The NIST 800-160 v1 framework and the 9-Step System Development Life Cycle (SDLC) provide a defined and comprehensive system of secure system development, and therefore security is introduced from the planning stage right through to routine maintenance. The NIST 800-160 v1 framework focuses systems security engineering, mandating best security practices that allow for the design, implementation, and operation of sound software systems. With the addition of the risk principles, SnowBe can build a strong security posture to support industry regulation such as PCI DSS, necessary for handling sensitive financial data. The framework helps SnowBe to identify threats early during the development phase, which enables the company to establish a security focused culture rather than security being an afterthought. In addition, NIST 800-160 v1 gives confidence that security is not a technical add-on but an essential component of the entire software lifecycle, protecting customer transactions, personal data, and company business. 9-Step SDLC complements NIST 800-160 v1 with a structured approach to software planning, development, testing, deployment, and maintenance. Security and risk management are integrated into each step, so attacks are identified, and they're fixed early, not like emergency patches after release. This methodical process minimizes the likelihood of costly security breaches, increases user confidence, and maintains software patches and updates under control. Furthermore, SDLC's continuous monitoring and evaluation phases ensure SnowBe's software is strong, high-performance, and adaptable enough to resist emerging threats. This plan not only improves operational efficiency, but it also will provide a strategic advantage in a todays digital landscape. Security will no longer be an afterthought, as it becomes included into SnowBe's software development lifecycle, allowing the company to modernize and achieve long-term business success.