# ASSIGNMENT 2.5

# Case Study: System Life Cycle Plan

Donald Doss

Gabriel Hernandez

Michael Kohronas

Xavier Rivera Maysonet

Michael Vazquez

**You and your team are in 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 (i.e., the items that are AQ-#.#), document in priority order all the processes. Your list should include the designation and the numbers in priority order in which you will address each process. (Highest Priority at the top and Lowest at bottom)**

| | |
|---|---|
| AQ-1 | PREPARE FOR SECURITY ASPECTS OF THE AQUISITION |
| AQ-1.1 | Define the security aspects for how the acquisition will be conducted. |
| AQ-1.2 | Prepare a request for a product or service that includes the security requirements. |
| AQ-2 | ADVERTISE THE ACQUISITION AND SELECT THE SUPPLIER TO CONFORM WITH THE SECURITY ASPECTS OF THE ACQUISITION |
| AQ-2.1 | Communicate the request for a product or service to potential suppliers consistent with security requirements. |
| AQ-2.2 | Select one or more suppliers that meet the security criteria. |
| AQ-3 | ESTABLISH AND MAINTAIN THE SECURITY ASPECTS OF AGREEMENTS |
| AQ-3.1 | Develop an agreement with the supplier to satisfy the security aspects of acquiring the product or service and supplier acceptance criteria. |
| AQ-3.2 | Identify and evaluate the security impact of necessary changes to the agreement. |
| AQ-3.3 | Negotiate and institute changes to the agreement with the supplier to address identified security impacts. |
| AQ-4 | MONITOR THE SECURITY ASPECTS OF AGREEMENTS |
| AQ-4.1 | Assess the execution of the security aspects of the agreement. |
| AQ-4.2 | Provide data needed by the supplier in a secure manner in order to achieve timely resolution of issues. |
| AQ-5 | ACCEPT THE PRODUCT OR SERVICE |
| AQ-5.1 | Confirm that the delivered product or service complies with the security aspects of the agreement. |
| AQ-5.2 | Accept the product or service from the supplier or other party, as directed by the security criteria in the agreement |

**Describe (100 words or more) why you selected the processes in the order you documented.**

When reviewing SnowBe's requirements and the current state of their processes, it becomes clear that they need to follow all parts of the Acquisition portion of the NIST framework. SnowBe is aiming to strengthen its supply chain, and this framework ensures that security is integrated throughout the process. Although they currently have nothing set up, the steps in the document already follow a logical order. SnowBe must first prepare the security aspects of the acquisition, establishing guidelines before any further action. Next, they need to communicate their security requirements to potential suppliers, followed by establishing and maintaining security agreements. Continuous monitoring of these agreements is essential to ensure ongoing compliance and effectiveness. Finally, SnowBe should accept and implement the product or service, ensuring all security standards are met. This order ensures SnowBe can secure its supply chain and keep it well-protected as it expands its business.

**You and your team are in phase 2 (planning phase) of the Life Cycle. Using the processes in the "ORGANIZATIONAL PROJECT-ENABLING PROCESSES" section, specifically the LM, IF, and HR processes, document in priority order only the processes you will address specifically for the planning phase. Your list should include the designation and the numbers in priority order in which you will manage each process. The processes you select from each section should be merged so there is only one list with all items in priority order.**
**(High Priority on top to Low on bottom)**

| | |
|---|---|
| LM-1.1 | Establish policies and procedures for process management and deployment that are consistent with the security aspects of organizational strategies. |
| HR-1.1 | Identify systems security engineering skills needed based on current and expected projects. |
| IF-1.1 | Define the infrastructure security requirements. |
| HR-2.1 | Establish a plan for systems security engineering skills development. |
| LM-1.2 | Define the security roles, responsibilities, and authorities to facilitate implementation of the security aspects of processes and the strategic management of life cycles. |
| HR-1.2 | Identify existing systems security engineering skills of personnel. |
| IF-1.2 | Identify, obtain, and provide the infrastructure resources and services that provide security functions and services that are adequate to securely implement and support projects. |
| LM-1.3 | Define the security aspects of the business criteria that control progression through the life cycle. |
| LM-1.4 | Establish the security criteria of standard life cycle models for the organization. |

**Describe (100 words or more) why you chose the processes in the order you documented.**

When reviewing the LM, IF, and HR processes, key aspects become apparent in their planning phase. Starting with LM-1.1, which involves establishing essential policies and procedures, this guides the entire security process for SnowBe. Following this, HR-1.1 and IF-1.1 address critical personnel and infrastructure needs, effectively aligning security with business operations. HR-2.1 ensures any skill gaps regarding employees' roles are addressed. Next, LM-1.2 and HR-1.2 define roles and assess existing personnel skills, ensuring everyone is properly prepared. IF-1.2 then confirms that infrastructure resources meet security requirements. Finally, LM-1.3 and LM-1.4 establish criteria for lifecycle progression and consistency. This structured approach ensures comprehensive planning and security integration from the outset and throughout the system.

<table>
<tr><td colspan="2"><b>You and your team are in 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, and IM processes, document in priority order only the processes you will address specifically for the maintenance AND evaluation phase. Your list should include the designation and the numbers in priority order in which you will manage each process. The processes you select from each section should be merged so there is only one list with all items in priority order.</b></td></tr>
<tr><td>RM-5.1</td><td>Continually monitor all risks and the security risk management context for changes and evaluate the security risks when their state has changed.</td></tr>
<tr><td>RM-5.2</td><td>Implement and monitor measures to evaluate the effectiveness of security risk treatments.</td></tr>
<tr><td>IM-2.4</td><td>Securely archive designated information.</td></tr>
<tr><td>IM-2.2</td><td>Securely maintain information items and their storage records, and record the security status of information.</td></tr>
<tr><td>RM-5.3</td><td>Monitor on an ongoing basis, the emergence of new security risks and sources of risk throughout the lifecycle.</td></tr>
<tr><td>RM-3.1</td><td>Identify security risks in the categories described in the security risk management context.</td></tr>
<tr><td>RM-3.2</td><td>Estimate the likelihood of occurrence and consequences of each identified security risk.</td></tr>
<tr><td>IM-2.1</td><td>Securely obtain, develop, or transform the identified information items.</td></tr>
<tr><td>IM-2.3</td><td>Securely publish, distribute, or provide access to information and information items to designated stakeholders.</td></tr>
<tr><td>RM-3.3</td><td>Evaluate each security risk against its security risk thresholds.</td></tr>
<tr><td>RM-3.4</td><td>Define risk treatment strategies and measures for each security risk that does not meet its security risk threshold.</td></tr>
<tr><td>IM-2.5</td><td>Securely dispose of unwanted or invalid information or information that has not been validated.</td></tr>
<tr><td colspan="2"><b>Describe (100 words or more) why you chose the processes in the order you documented.</b></td></tr>
<tr><td colspan="2">This prioritized order starts with continuous monitoring (RM-5.1 and RM-5.2) to promptly detect changes or new risks, ensuring system integrity. Secure archiving (IM-24) and maintaining information (IM-2.2) follow, preserving essential data and records. Ongoing risk monitoring (RM-5.3) helps us stay ahead of emerging threats. Identifying (RM-3.1) and estimating (RM-3.2) risk lay the groundwork for evaluating (RM-3.3) and defining strategies (RM-3.4). Managing information securely (IM-2.1, IM-2.3) supports operational efficiency and stakeholder’s access. Addressing risk thresholds (RM-3.3, RM-3.4) and disposing of invalid data (IM-2.5) ensures a comprehensive security posture. This structure prioritizes proactive risk management while maintaining data integrity and operational efficiency. Overall, this order was picked to ensure that all information and risks are evaluated and maintained securely.</td></tr>
</table>

**You and your team are in 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 VA and OP processes, document in priority order only the processes you will address specifically for the maintenance AND evaluation phase. Your list should include the designation and the numbers in priority order in which you will manage each process. The processes you select from each section should be merged so there is only one list with all items in priority order.**

| | |
|---|---|
| OP-2.3 | Monitor the security aspects of system operation. |
| OP-2.4 | Identify and record when system security performance is not within acceptable parameters. |
| OP-2.5 | Perform system security contingency operations, if necessary. |
| VA-3.1 | Record the security aspects of validation results and any security anomalies encountered. |
| VA-3.2 | Record the security characteristics of operational incidents and problems and track their resolution. |
| OP-3.1 | Record results of secure operation and any security anomalies encountered. |
| OP-3.2 | Record the security aspects of operational incidents and problems and track their resolution. |
| OP-3.3 | Maintain traceability of the security aspects of the operations elements. |
| VA-2.2 | Perform security validation procedures in the defined environment. |
| VA-2.3 | Review security-focused validation results to confirm that the protection services of the system that are required by stakeholders are available. |
| VA-3.4 | Maintain traceability of the security aspects of validated system elements. |
| OP-4.1 | Provide security assistance and consultation to customers as requested. |
| OP-4.2 | Record and monitor requests and subsequent actions for security support |
| OP-4.3 | Determine the degree to which the delivered system security services satisfy the needs of the customers. |

**Describe (100 words or more) why you chose the processes in the order you documented.**

The VA and OP processes are crucial during SnowBe's maintenance and evaluation phases. OP 2.3, 2.4, 2.5 focus on monitoring system security, identifying performance issues, and executing contingency operations, vital for maintaining real-time system integrity. VA-3.1 and 3.2 ensure that validation results, anomalies, and incidents are properly recorded and tracked. OP 3.1, 3.2, 3.3 address secure operation results and maintain traceability. VA 2.2, 2.3, 3.4 perform security validation in the operational environment. Finally, OP 4.1, 4.2, 4.3 handle customer support, ensuring that security needs are met and tracked. This order was chosen to enhance SnowBe's risk and operational management effectively, ensuring customer trust and secure operations.

| **Describe (100 words or more) 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 is critical for ensuring the development and maintenance of secure systems. It offers a comprehensive methodology to incorporate security at every stage of the systems engineering process, from initial concept to final disposal. Adhering to these guidelines enables SnowBe to systematically identify and mitigate risks, ensuring that their rapid growth is not compromised by security vulnerabilities. The 9-step life cycle offers a structured approach to system maintenance and evaluation. Each phase-from concept and development through deployment, operation, and decommissioning-requires meticulous attention to security. By following this life cycle, SnowBe ensures continuous monitoring, evaluation, and enhancement for their security posture. This proactive approach is essential for maintaining operational integrity and addressing vulnerabilities efficiently. It is critical for a company like SnowBe, which is transition to more controlled environment while sustaining its growth trajectory. |