Systems Engineering Management Plan

for

CS672 Systems Engineering Methods

Version 5.0

Prepared by Lisa Ross

Colorado Technical University

09/19/2016

EXECUTIVE SUMMARY

This Systems Engineering Management Plan (SEMP) outlines the engineering processes that the PetroChem, Inc. engineer teams will follow to develop a more secure network system to meet the SEC's Sarbanes Oxley (SOX) requirements for all publicly traded companies. Systems engineering is needed for all components and services that depend on the network and security system. This includes adding systems security engineering techniques, methods, and practices into those systems and software engineering processes. The goal of this plan is to use established engineering processes to ensure security needs are met and addresses sustainably throughout the life cycle of the system. This SEMP describes the in place controls and outlines the roles and responsibilities of each engineering team. The cost-effective security protection systems engineering plan (SEP) includes input from various managers and stakeholders responsible for information system security. The approved systems engineering plan (SEP) by stakeholders and the CFO and are the foundation of the SEMP.

Specifications have been elaborated on and approval has been given on the following foundation. The architectural team designed a working product based on the engineering design that integrates all IT departments. The steering committee determined the funding was appropriate to meet the IT goals. The privacy and information security officers made sure that data, system and network security was analyzed and evaluated. The CISO was ultimately responsible for ensuring the security of the system and data as designed by the engineers and developed by the architecture teams. The project management office maintained successful communication to meet project standards. The head of IT operations has trained support engineers as defined in this SEMP. This department will also ensure all IT issues are addressed promptly.

DOCUMENT HISTORY

DOCUMENT REVISION HISTORY			
Ver. #	Approved	Description of Change(s)	Created/Updated by
1	08/22/2016	Document overview/Project Schedule	Lisa Ross
2	08/29/2016	Key Teams/Process Modeling/Decision making	Lisa Ross
3	09/05/2016	Requirements/Functional Analysis/Design	Lisa Ross
4	09/12/2016	Reliability/Security/Maintainability/Safety	Lisa Ross
5	09/19/2016	Elaborate Executive Summary updated to include elaborated procedures.	Lisa Ross

Table of Contents

1. INTRODUCTION

1.1. Company Structure Summary

PetroChem, Inc. is a global corporation based in Houston, Texas with 27 locations worldwide. The company specializes in petroleum consulting services, interpretation and processing services, real-time data services, and well-engineering project management. These collective services maximize a company's petroleum reservoir performance. An acquisition

PetroChem's company structure is overseen by a Board of Directors which consists of an audit committee and which the CEO and CFO report to for advising. Under the CEO and CFO are three main departments: Business Development, Engineering and Administration.

PetroChem, Inc. company infrastructure has been reviewed for security compliance. A security system engineering plan has been approved for better security controls. The security controls will meet the regulatory requirements based on the Sarbanes-Oxley Act.

To be Sarbanes-Oxley compliant three levels of security will be addressed: General IT processes, Application and data-owner controls, and Configurable Application Controls. Below is a breakdown of the three levels that will be addressed to meet public trade compliance requirements.

1.1.1. General IT processes

- Security administration
- Application change control
- Data backup and recovery
- System development life cycle (SDLC)

1.1.2. Application and data-owner controls

- Segregation of security roles and administration
- Controls for applications and reports that modify financial data files and critical reports
- Control over critical transactions and data
- Change controls for business owners

1.1.3. Configurable Application Controls

- Automated process controls
- Manual process controls
- End-user comupting (EUC) controls
- Reporting controls
- Application security controls
- General IT controls

2. PURPOSE

This Systems Engineering Management Plan (SEMP) describes the engineering practices employed in maintaining and developing a secure network system for PetroChem, Inc. to meet the SOX requirements. This document serves as a guideline for the general procedures that the engineering and development teams must follow; however, it does not define specifics on how each procedure will be accomplished. The engineer or development team leads may tailor this SEMP to their system needs.

2.1. Document Overview

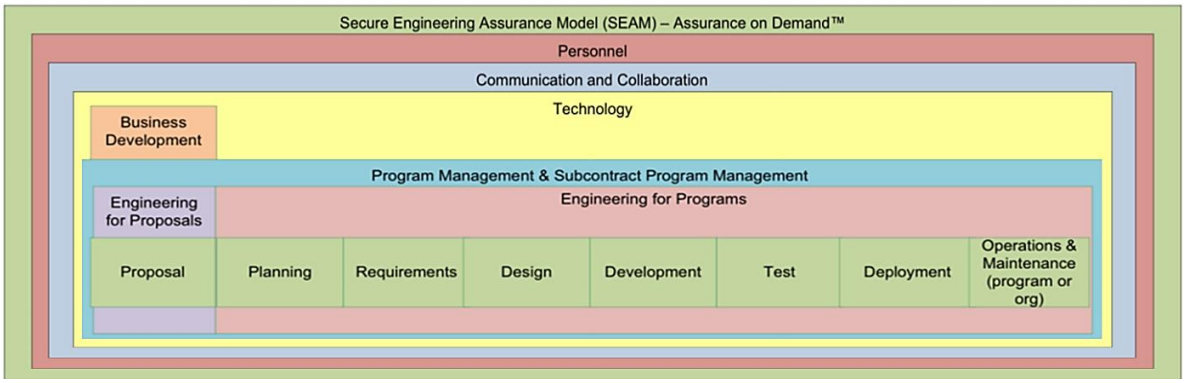
The following provides a summary of each section contained within this SEMP.

- **Introduction**: Identifies, describes the purpose, introduces the objectives and summarizes the contents of the document, and provides a project schedule;
- **Systems Engineering Processes**: Gives the project organization, defines the environments, explains the decision making process, provides a system engineering model, and covers verification and validation;
- **Specialty Engineering**: Describes the integration and coordination of the program which includes the reliability, maintainability, safety and security.
- **System Deployment**: Discusses the site preparation, system installation, system checkout, user training, and support engineering training.
- **Product Support**: Identifies and discusses the system maintenance, logistic processes associated with maintaining required parts, and disposal processes.

2.2. System Overview

The SEMP is documentation that is a result of additions, deletions, and modifications that will occur during its utilization. Additional configuration activities that are identified and defined during the work processes are included during document updates. This document will be identified with a version number and released through configuration control to all appropriate authorities. (Eisenhart, 2007). The final document will include all design, deployment and support activities identified and defined within. The schedule gives a high level overview of the timeline objectives and is subject to change depending on alterations and additions to the plan per the individual engineering teams.

2.2.1. Figure 1.a Security Engineering Assurance Model



(Lockheed Martin Corporation, 2014)

2.3. Project Schedule

2.3.1. Project Schedule Table 1.a

Design	August 2016 - September 2016
Secure Component Design	
Secure System Design	
Attack Surface Analysis/Reduction	
Development	October 2016 - March 2017
Secure Builds & Configuration	
Static Analysis	
Security Test Planning	
Test	April 2017 - May 2017
Functional System Security Testing	
Dynamic Analysis	
Specialty Security Testing	
Attack Surface Review	
Security Test Results & Discrepancy Mitigation	
SRA Report	
C&A Package	
Deployment	June 2017 - July 2017
Approved Security Baseline Sustainment	
Incident Response Plan	
Observation and Measurements	August 2017 - October 2017
Control Monitoring	
Secure Upgrades	
Security Metrics & Reporting	
Security Reviews, Testing & Scans	
Contingency & DR	
Incident Response	
Security Policy & Plan	
C&A	
SATE	
Retirement	November 2017
Security Retirement and Transition Plan	
Safeguard of System Data	

(Lockheed Martin Corporation, 2014).

3. SYSTEM ENGINEERING PROCESSES

3.1. Organization

Stakeholder: a person with an interest or concern with PetroChem

Shareholders: any person, company or other body that owns at least one share of PetroChem's stock.

Board of Directors: A group of individuals elected by the PetroChem, Inc. stakeholders to establish company policies and to make decisions on major company issues.

Audit Committee: Select members of the PetroChem's board of directors that oversee financial reporting and disclosure.

Chief Executive Officer (CEO): Oversees the management of the entire corporation and ultimately responsible for the business' success or failure.

Chief Financial Officer (CFO): Develops annual budgets, manages cash flow, and oversees financial reporting and compliance.

Chief Information Security Officer (CISO): Responsible for ensuring the security of enterprise systems and data.

Chief Operating Officer (COO): Senior manager who is responsible for managing the company's day-to-day operations and reporting them to the CEO.

Business Executives: Responsible for running an organization

Business Process Owner: Define, Measure, Analyze, Improve and Control to successfully manage processes of a project.

Strategy Executive Committee: Review the overall strategy recommended by CEO and exam particular strategic transactions and initiatives.

Steering (Programs/Projects) Committee: Decides the overall level of IT spending and how costs will be allocated.

Project Management Office (PMO): A department within the enterprise that defines and maintains standards for project management within the organization.

Value Management Office (VMO): Oversees corporate governance, organizational change, quality, compliance and process management.

Chief Risk Officer (CRO): A corporate executive responsible for assessing and mitigating significant competitive, regulatory and technological risks.

Architecture Board: Responsible for facilitating architectural discussions and agreements between the core network architecture/engineering team, network operations, and security.

Enterprise Risk Committee: Appointed by the board of directors responsible for review and approval of risk management policies and oversight of the company's risk-management framework.

Head of Human Resources (HR): Responsible for directing all personnel in accordance with Corporate policies and practices.

Compliance: Ensures compliance with all applicable laws, rules and regulations.

Chief Information Officer (CIO)/IT Manager: Senior executive in an enterprise responsible for the information technology and computer systems that support enterprise goals.

Head Architect: Centralizes IT functions so that departments across the company can work together seamlessly.

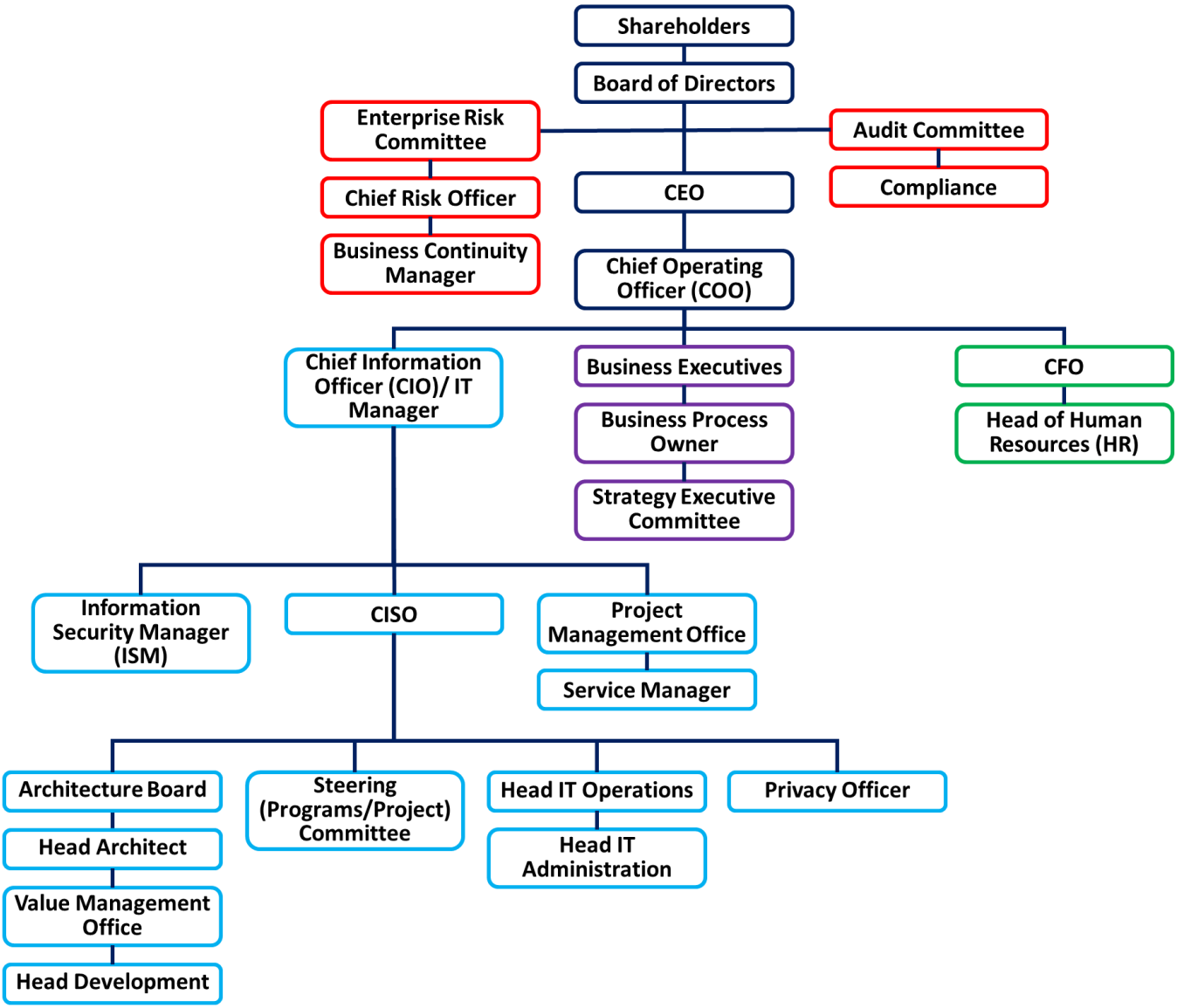
Information Security Manager (ISM): Provide analysis, network evaluation and security vulnerability guidance. Manage security systems such as anti-virus, firewalls, patch management, intrusion detection, and encryption.

Business Continuity Manager: Creates plans to keep a company functioning after disruptive events such as natural disasters, terrorism, crime and computer and human error.

Privacy Officer: Develop and implement policies to protect employee and customer data from unauthorized access.

See Chart 3.a Security System Engineering Team Organization Chart for the hierarchical levels of management for each department involved in the security systems engineering plan.

3.1.1. Chart 3.a Security System Engineering Team Organization Chart



As identified by systems engineering management team lead (Lisa Ross)

3.2. Environments

Project enablers are processes and resources that contribute to the success of a project. COBIT 5 model has seven enablers which include: Principles, Policies and Frameworks; Processes; Organizational Structures; Culture, Ethics and Behavior; Information; Services, Infrastructure and Applications; and People, Skills and Competencies. Enablers are factors that both individually and collectively influence enterprise IT governance and management. See Table 3.a COBIT 7 Enablers

3.2.1. Table 3.a COBIT 7 Enablers

Enabler	Description
Processes	Sets of practices and activies performed to meet objectives and produce an output of overall IT-related goals.
Organizational structures	An orginazations key decision making entities.
Culture, ethics and behavior	Governance and management of individuals and of the organization
Principles, policies and frameworks	Define desired behavior into guidance for day-to-day management
Information	Output prevalent throughout the organization and used by the enterprise. A key product of the enterprise.
Services, infrastructure and applications	The hardware and software that provide the enterprise with information technology processing and services
People, skills and competencies	Vital to successful completion of activities and decision making for corrective actions

The seven enablers are interconnected achieve the main objectives with a complete governance and management. Enablers depend on the input of other enables in order to be fully effective. Output deliverables benefit other enablers and improve process efficiency. The scope common to all enables include: Entity interaction management, facilitate successful enabler outcomes, and provide simple and structured processes to deal with enablers.

3.3. Decision-Making Process

A portfolio investment approach uses a cost/benefit/risk assessment for decision making. Throughout the development life cycle the portfolio investment tool reduces risks and maximizes benefits of operations. The tool assesses the costs of continued funding of current operations versus new development with greater performance capabilities. Some SOX-mandated management controls include: benchmarking, activity cost accounting, software license audits, incident response capabilities and cost/benefit analysis. (ITIL Help, 2005).

A series of guidelines, laws and regulations provide resources and controls necessary for successful security development. The Information Technology Infrastructure Library(ITIL) is a collection of good practices and knowledge/skill for operations of infrastructure. The ITIL enables stable and high quality operation of IT infrastructure. It also provides a clear indicator of Return on Investment (ROI) for IT operation. The Sarbanes Oxley Act (SOX), is a United States federal law enacted on July 30, 2002 following the Enron as well as other publicly traded company scandals. SOX directs the SEC to enact rules protecting shareholders and the economy. The rules mandate honest financial reporting, placing corporate leaders accountable, and using audits to ensure compliance.

Leadership, organizational structures and processes make up IT governances. The organization structure of the IT Strategy Committee and the IT Steering Committee ensure that PetroChem's information technology align with the company's strategies and objectives in decision making. The IT Strategy Committee focuses on current and futures strategic IT issues. They are responsible for advising the board and management of an appropriate IT strategy. The IT Steering Committee oversees the IT spending budget, assist executive in IT strategy realization and focus on implementation.

Communication keeps all stakeholders on the same page, can be done through meetings or reports and is key in the decision making process. Workgroups meet to maintain quality and consistency. Individuals bring their work to meetings to submit to other teams for compilation and testing. The results will be reported and can then be reviewed and analyzed. Time considerations are also important in decision making. A Gantt chart provides both task duration and milestones which can identify where time is wasted or efforts should be refocused. Other tools vital to decision making include a Balanced Scorecard, the COBIT 5 Framework and Service Level Agreements (SLA).

Because PetroChem, Inc. is a publicly traded company, major decisions must be approved by the board of directors. Case arguments identified by the portfolio investment tool are presented to the board by each team lead. These arguments are considered and the board returns their decision based on what they feel is in the best interest of the company and its stakeholders.

3.4. System Engineering Model

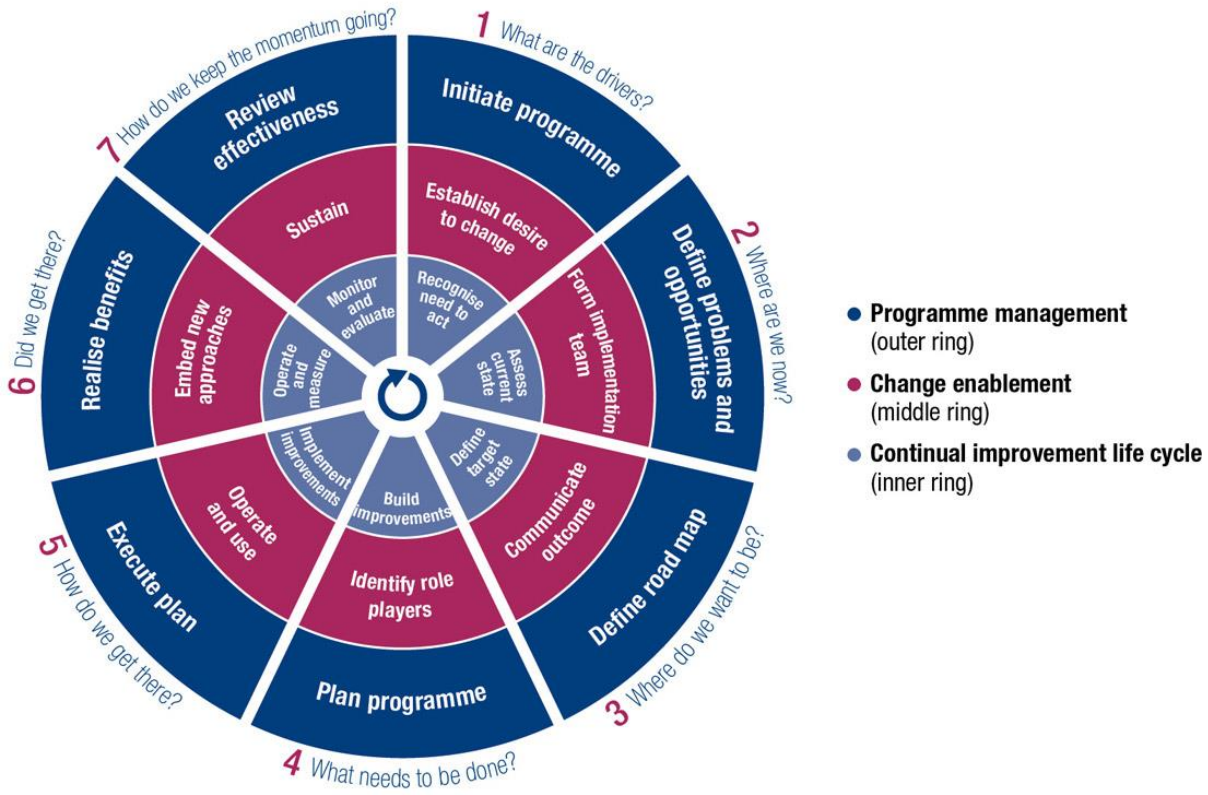
There are several models used in systems engineering today. Some examples of systems engineering models include: Waterfall, Rapid application development (RAD), Spiral, Agile, Iterative and V-Shaped. Engineering projects vary in needs and so too does the most appropriate model for development. Before choosing a model, all aspects of its design should be considered for effectiveness.

One of the models considered by PetroChem, Inc. system engineers was the Waterfall model. The scope limitations are just one of several issues with the waterfall model. The model assumes that there is a well-defined set of requirements up front and that few modifications to the system will be needed. This model does not accommodate change well because there is a huge gap in time from the definition to delivery. You cannot predict how smooth systems integration will be based on architecture and planning. This model does not consider software innovation, new system specifications and testing necessary. The model does not keep the stakeholders involved at each stage in order to make modifications. Feedback only comes after all stages of development are complete. This model is insufficient for the PetroChem, Inc. systems engineering project.

The Agile model addressed many of the waterfall model shortcomings but would need modifications to address the SEC public company security compliance. PetroChem, Inc. is a publicly traded company and as such must meet the SECs guidelines in accordance with the Sarbanes-Oxley Act (SOX). This is to ensure accurate financial information disclosure and requires the organization to produce an internal control report. COBIT 5 has an internal control framework that is designed to meet IT SOX compliance.

The COBIT 5 Implementation Model has three life cycles: Program Management, change enablement, and continual improvement. See Figure 3.a COBIT 5 Implementation Model for how the three life cycles are interrelated and Table 3.b Seven Phases of the Implemetnation Life Cycle for a description of each phase. (Zororo, 2016).

3.4.1. Figure 3.a COBIT 5 Implementation Model



(Zororo, 2016).

3.4.2. Table 3.b Seven Phases of the Implemetnation Life Cycle

The 7 phases of the implementation life cycle – Creating the Appropriate Environment	Programme management	Change enablement	Continual Improvement Life Cycle
What are the drivers?	Initiate programme	Establish desire to change	Recognise need to act
Where are we now?	Define problems and opportunities	Form implementation team	Assess current state
Where do we want to be?	Define road map	Communicate outcome	Define target state
What needs to be done?	Plan programme	Identify role players	Build improvements
How do we get there?	Execute	Operate and use	Implement improvements
Did we get there?	Realise benefits	Embedded new approaches	Operate & Measure
How do we keep the momentum going?	Review effectiveness	Sustain	Monitor & Evaluate

(Zororo, 2016).

3.5. Systems Engineering Processes

The security systems engineering processes is based on five core COBIT 5 principles: Meeting Stakeholder Needs, Covering the Enterprise End-to-End, Applying a Single, Integrated Framework, Enabling a Holistic Approach and Separating Governance from Management. **Principle 1**. Meeting Stakeholder Needs means that the enterprise exists to create value for stakeholders. This requires negotiation between stakeholders that hold value in different interests while still weighing the benefits, resources and risk.

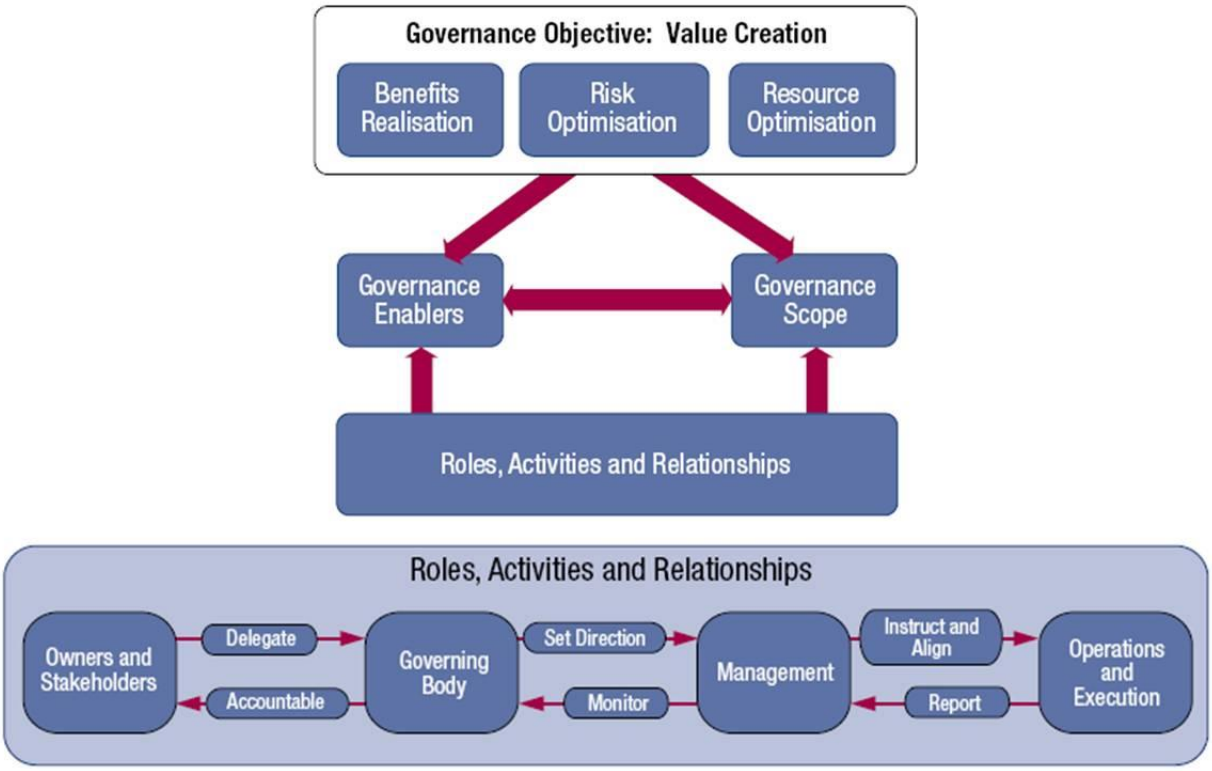
Principle 2. Covering the Enterprises End-to-end addresses all functions and processes within an enterprise and treats information and related technologies as assets.

Principle 3. Applying a Single Integrated Framework facilitates COBIT user mapping of practices and activities and allows management framework integration.

Principle 4. Enabling a Holistic Approach focus on enablers describe in the COBIT 5 seven category framework. Enablers provide individual or collective results that determine the functionality of processes and activities.

Principle 5. Separating Governance from Management clearly distinguishes governance from management by defining their individual purpose, types of activities and differing organizational structure. Board of directors are responsible for governance where the executive management is under the leadership of the CEO. See Figure 3.b System Engineering Process Chart for how governance objectives, roles, activities, relationships and enables are interrelated.

3.5.1. Figure 3.b System Engineering Process Chart



(Zororo, 2016).

3.6. Configuration Management

Change management begins with technical reviews. During a technical review, requirements, design, code and other developments are presented to stakeholders for comments and approval. This is done at each phase of the project and must be approved before moving onto the next phase. Walkthroughs are similar to reviews but done with other team members. The goal is to identify any errors in interface, logic, data and syntax. The COBIT 5 model includes a review checklist as a guideline for determining the effectiveness of the system. The model also includes quality metrics for measuring completeness and presenting a case for recommendations.

COBIT 5 uses a Process Capability Model and Levels based on ISO/IEC 15504 to measure the functionality level of processes. Levels are rated from 0 to 5. Table 3.a Process Capability Model and Levels provides a summary of the six levels. (ITIL Help, 2005).

3.6.1. Table 3.a Process Capability Model and Levels

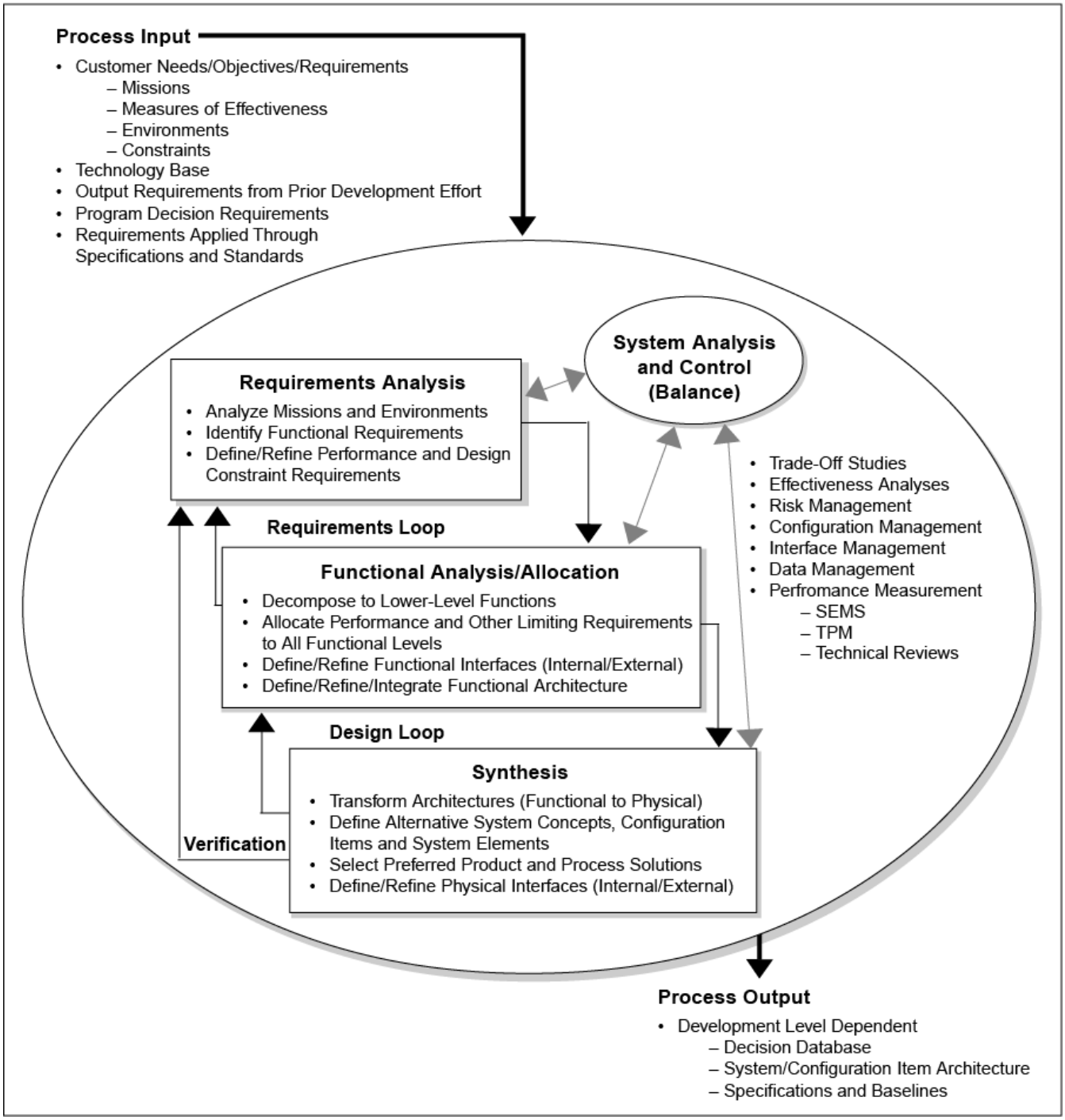
Level	Process capability status
0	Incomplete. The process is not implemented or fails to achieve its purpose.
1	Performed (Informed). The process is implemented and achieves its purpose.
2	Managed (Planned and monitored).The process is managed and results are specified, controlled and maintained.
3	Established (Well defined). A standard process is defined and used throughout the organization.
4	Predictable (Quantitatively managed). The process is executed consistently within defined limits.
5	Optimizing (Continuous improvement). The process is continuously improved to meet relevant current and projected business goals.

Following a review and walkthrough the results are reviewed by the technical review lead. Each team in the organization has a technical review lead who is responsible for documenting findings, decisions and recommendations throughout the life cycle of the systems development. The documentation is then reviewed collaboratively with other team managers and field experts. Team managers respond to the recommendations. (ITIL Help, 2005).

3.7. Requirements Engineering/Functional Analysis

The requirements engineering and functional analysis is best explained visually. See Figure 3.c Requirements and Functional Analysis for how process inputs are analyzed and defined to provide meaningful process output. Customer needs/requirements, technology assets, decision requirements, and specification/standard requirements are some of the process input needed from analysis. Considerations for process output include tradeoffs, effectiveness, management types (risk, configuration, interface and data), and performance measurements. The process output provides engineers with information necessary for decision making. (IT Governance Ltd, 2001).

3.7.1. Figure 3.c Requirements Engineering and Functional Analysis



(IT Governance Ltd, 2001).

3.8. Design

PetroChem, Inc. uses enterprise resource planning (ERP), customer service management (CRM), exchange email, LAN/WAN and the internet. The engineering and administration departments use the ERP system while the business development department uses the CRM system. All departments and teams utilize the email, network and internet resources. The PetroChem, Inc. home office location network will run on separate domains and the server's application, data, exchange, web and other servers will each reside behind a dedicated firewall. Table 3.b Hardware and Software Design provides a summary of the hardware and software access controls that are in the scope of the design.

3.8.1. Table 3.b Hardware and Software Design

System	Identification/Authentication	Authorization
Building Access	Key Card Entry	Access Control Lists (ACL)
Server Rooms	Electronic Keyless Entry	Physical Control / Network Segregation
Desktops	Active Directory	Role Based Access Control (RBAC)
Laptops	Cryptosystem (Syncronous) 1. Data encryption 2. Token	Technical (Locigal) Control
WiFi	LDAP	Nondiscretionary Access Control (NAC)

3.9. Development

The development process includes build management, software/hardware development and systems integration. Table 3.c Responsible, Assist, Consulted, Informed (RACI) Chart provides a list of all processes used to create, manage, and transmit the build. The table defines the roles and responsibilities of the key decision makers in the engineering processes. The COBIT RACI chart is used to identify who is involved in each process and to what level. A RACI chart assigns four levels of involvement: Responsible, Assist, Consulted and Informed. (IT Governance Ltd, 2001).

3.9.1. Table 3.c Responsible, Assist, Consulted, Informed (RACI) Chart

	Board of Directors	Chief Executive Officer (CEO)	Chief Financial Officer (CFO)	Chief Operating Officer	Business Executives	Business Process Owner	Strategy Executive Committee	Steering (Programs/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer (CISO)	Architecture Board	Enterprise Risk Committee	Head of Human Resources (HR)	Compliance	Audit Committee	Chief Information Officer (CIO)/IT Manager	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager (ISM)	Business Continuity Manager	Privacy Officer
Develop and maintain the program plan			C	C	A	C		R	R	R	C					C	C	C	C	C	C		C	C	C	C
Launch and execute the program			C	C	A	R		R	R	I	C					C	C	R	R	R	R		C	C	C	C
Monitor, control and report on the program outcomes					A	C	I	R	R	R	C					C	R	R		C	C			C		
Identify and classify problems					I	C					I	I				I	I	R	C	R	R		A	C		
Investigate and diagnose problems											I	I							C	C	A		R	R		
Raise known errors																					A		R	R		
Resolve and close problems					I	C					I	I				C	C	I	C	C	R		A			
Perform proactive problem						C													C	C	R		A			
Protect against malware						R	I				C	A			R	C	C	C	I	R	R		I	R		
Manage network and connectivity security						I					C	A				C	C	C	I	R	R		I	R		
Manage endpoint security						I					C	A				C	C	C	I	R	R		I	R		
Manage user identity and logical						R					C	A			I	C	C	C	I	C	R		I	R		C
Manage physical access to IT						I					C	A				C	C	C	I	C	R		I	R	I	
Manage sensitive documents and output devices											I					C	C	A			R					
Monitor the infrastructure for security-related events				I		C					I	A				C	C	C	I	C	R		I	R	I	I
Evaluate the governance system	A	R	C	C	R		R				C		C	C	C	C	C	R	C	C	C					
Direct the governance system	A	R	C	C	R	I	R	I	I	I	C	I	I	I	I	C	C	R	C	I	I	I	I	I	I	I
Monitor the governance system	A	R	C	C	R	I	R	I	I	I	C	I	I	I	I	C	C	R	C	I	I	I	I	I	I	I
Monitor internal controls		I	C	I	C	R			R		R					R	R	A	I	R	R	R	R	R	R	R
Review business process controls effectiveness	I	I	R	I	A	R	I				I	I				R	R	C			C		C	C	C	
Perform control self-assessments		I	C	I	C	R			R		R					R	R	A	I	R	R	R	R	R	R	R
Identify and report control		I	C	I	C	R			R		I	I				R	R	A	I	R	R	R	R	R	R	R
Identify external compliance					A	R										R	R	R								R
Optimise response to external requirements		R	R	R	A	R	I		R							R	R	R	I	R	R	R	R	R	R	R
Confirm external compliance	I	R	R	R	R	R	I	I	C							A	I	R	C	C	C	C	C	C	C	R

(IT Governance Ltd, 2001).

	Board of Directors	Chief Executive Officer (CEO)	Chief Financial Officer (CFO)	Chief Operating Officer	Business Executives	Business Process Owner	Strategy Executive Committee	Steering (Programs/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer (CISO)	Architecture Board	Enterprise Risk Committee	Head of Human Resources (HR)	Compliance	Audit Committee	Chief Information Officer (CIO)/IT Manager	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager (ISM)	Business Continuity Manager	Privacy Officer
Define the organization structure		C	C	C	C		I		C						R	I	I	A	C	C	C	R	C	C	C	
Establish roles and responsibilities						C			C						C	C	C	A	C	C	C	R	C	C	C	C
Maintain the enables of the management system	C	A	C	R	C	C	I				C					C	C	R				R				
Communicate management objectives and direction		A	R	R	R	I	R	I	I	I	R	R	I	I	I	I	I	R	I	I	I	I	I	I	I	I
Optimise the placement of the IT		C	C	C	C		A		C						C	C	C	R	C	C	C	R	C	C	C	
Define Information (data) and system ownership		I	I	C	A	R									C	C	C	C	C						C	C
Manage continual improvement of processes				A		R			R				C		I	C	C	R	R	R	R	R	R	R	R	
Maintain tcompliance policies and procedures		A				R			R				R		R	C	I	R	R	R	R	R	R	R	R	
Identify IT Services		C		R	R	R	C		I							I	I	R	I	C	C	C	A	I	I	
Catalog IT-enabled services					I	I			I							I		R	I	C	C	R	A	I	I	
Define and prepare service					R	C			C		C					C		R		C	R	R	A	C	C	
Monitor and report service levels		I		I	I	R					C							I		I	I	I	A			
Review service agreements and					A	C			C		C					C	C	R		C	R	R	R	C	C	I
Collect data		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R
Analyze risk		I				R			C		R	C		I		R	R	A	C	C	C	C	C	C	C	C
Maintain a risk profile		I				R			C		A	C		I		R	R	R	C	C	C	C	C	C	C	C
Articulate risk		I				R			C		R	C		I		C	C	A	C	C	C	C	C	C	C	C
Define a risk management action		I				R			C		A	C		I		C	C	R	C	C	C	C	C	C	C	C
Respond to risk		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R
Establish and maintain an ISMS		C		C	C	I	C	I	I		C	A	C	C		C	C	R	I	I	I	R	I	R	C	C
Define and manage an informaiton security risk treatment plan		C		C	C	C	C	I	I		C	A	C	C		C	C	R	C	C	C	R	C	R	C	C
Monitor and review the ISMS					C	R	C		R			A				C	C	R	R	R	R	R	R	R	R	R
Maintain a standard approach for program and project management	I	A	C	C	R		R		C		C					C	C	R								
Initiate a program	I	R	C	C	A	R	R	R	R									C	C	C	C		C	C	C	C
Manage stakeholder engagement		A	C	R	R	R	C	R	I	I								R	C	C	C		C	C	C	C

(IT Governance Ltd, 2001).

	Board of Directors	Chief Executive Officer (CEO)	Chief Financial Officer (CFO)	Chief Operating Officer	Business Executives	Business Process Owner	Strategy Executive Committee	Steering (Programs/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer (CISO)	Architecture Board	Enterprise Risk Committee	Head of Human Resources (HR)	Compliance	Audit Committee	Chief Information Officer (CIO)/IT Manager	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager (ISM)	Business Continuity Manager	Privacy Officer
Obtain assurance of external compliance	I	I	I	I	C	C	I		C							C	A	R	C	C	C	C	C	C	C	C
Build IT strategic plan		A	C		C	I			I							C	C	R	C	C	C	C		C		
Build IT tactical plan		C	I			C			R							I	I	A	C	C	C	C		I		
Analyze program portfolios and manage project and service		C	I		I	R			C							I	I	A	C	R	R	C		I		
Build project charters, schedules quality plans, budgets and communication and risk					C	C		A/R								C	C	C	C	C	C	C		C		
Identify, asses and mitigate supplier			I						C							C	C	A		R	R	R		C		
Regularly test the IT continuity plan						I			I							I	I	I	C	C	A/R	C		I		
Conduct regular vulnerability assessments			I			I										R	R	A		C	C			R		
Identify and collect measureable objectives that support the business objectives.		C	C		C	R												A		R	R					
Review, endorse, align and communicate IT performance, IT strategy and resource and risk managment with business strategy	A	R	I		R											C	C							C		

R: Responsible — Those responsible for the performance of the task.
A: Assists — Those who assist completion of the task
C: Consulted — Those whose opinions are sought; and with whom there is two-way communication.
I: Informed — Those who are kept up-to-date on progress; and with whom there is one-way communication.

(IT Governance Ltd, 2001).

3.10. Verification & Validation

Verification tests whether a system and/or software meets the expressed requirements and user needs. COBIT 5 uses a four-point rating scale to assess each process to see if it has met its requirements. The four-points rating scale is identify by the letters N, P, L, F. An N or Not achieved is given if 0 – 15% of the requirement are met. Achievements between 15 – 50 % are given a P for Partially achieved. A process is given an L for Largely achieved if it has successfully achieved between 50 – 85% of the requirements. Anything over 85% is given a F rating for Fully achieved requirements. This scale identifies areas that need to be revisited or are incomplete. (IT Governance Ltd, 2001).

Once the processes have met the requirements defined and user needs the system is then tested for compliance and security. Fraunhofer SIT is a research lab dedicated to providing the most comprehensive security system testing and analysis available. The company ties together various tools including automated or semi-automated testing tools, complex applications testing tools and other interface and operation testing tools. Their approach uses human testing, sensors and actuators. The mission of Fraunhofer SIT is to test the network security with the intent of breaking the systems in order to identify weaknesses that need to be addressed. ("Fraunhofer SIT - Security Test Lab - About Us," n.d.).

4. SPECIALTY ENGINEERING

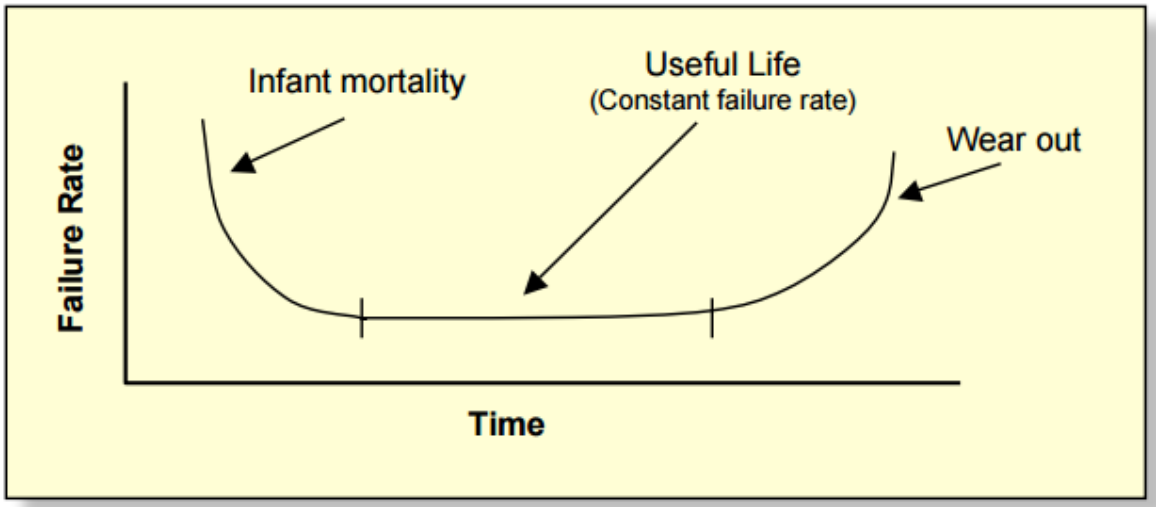
The systems of system (SoS) defined in this SEMP will meet SOX requirements as defined by the SEC. The SoS is a set of independent systems that are integrated to produce a larger system with greater capabilities. In order to evaluate functional or system requirements, quality attributes known as “ilities” are used throughout the life cycle and beyond the systems initial use. (Software Architecture Notes, n.d.). While it is hard to deduce the most important ilities for a system design, this SEMP places high importance on the following: reliability, maintainability, security and safety.

An ility characterizes a systems ability to respond to change. This includes changes that are foreseen and unforeseeable. Emphasis is placed on longer term consistency over the entire life cycle of the system. During the life cycle of a system or SoS, many operational environmental changes take place. Ilities take into account future change needs. The purpose of an ility is to describe how a system should be rather than what the system should do. (Ricci, Fitzgerald, Ross, & Rhodes, 2014).

4.1. Reliability

A reliable system will meet performance requirements for a period of defined time under specified operating conditions. Reliability measures the average potential failure rate for a system, SoS or components. At infancy the rate of failure will continue to reduce as modifications are made during its development life cycle. At the point of release the rate of failure should remain very low for the systems expected life. This is referred to as the Mean Time between Failures (MTBF). See Figure 4.a SoS MTBF. Rate of failure should only increase at the end of the systems life or point of disposal. (Raytheon Learning Institute, n.d.).

4.1.1. Figure 4.a SoS MTBF



The role of a Reliability Engineer is to develop a failure, analysis and corrective action systems (FRACAS) document. This document is included in the SEMP and will cover requirements analysis, design guidelines, critical items and risks and hazard tracking. Reliability engineers must be proficient in fault avoidance, fault tolerance and functional redundancy. (Raytheon Learning Institute, n.d.).

Various tools aid engineers in testing and identifying points of failure. A reliability model is a tool that allows engineers to predict reliability of alternatives by performing component stress analysis and assessment. A fault tree is another tool that engineers can use to graph fault combinations that lead to the top-level fault. (Raytheon Learning Institute, n.d.).

4.2. Maintainability

Maintainability is the ability to keep the system working and the ease, safety and minimal cost of restoring operation in the event of failure. Maintainability engineers focus on maintenance downtime, work hours per operating hour, and annual maintenance cost. Maintainability engineers are responsible for developing and refining the systems main functions.

The maintainability engineer is responsible for design criteria, design handbooks, checklists and lessons learned, and guidelines and policies. They also establish, allocate and verify maintainability requirements. By identifying maintainability design deficiencies, engineers are able to refine systems maintenance and create a maintainability program plan. A functional flow block diagram (FFBD), maintainability models and problem/failure reports are useful tools for maintainability engineers. (Raytheon Learning Institute, n.d.).

4.3. Security

System security is the task of preventing sensitive information and documentation located in the system from being compromised. System Security Engineer identify the system security vulnerabilities and needed protection measures within the scope of the system. They are responsible for defining security requirements and processes. (Dutcher, 2010).

4.4. Safety

System Safety Engineers ensure that dangerous or hazardous conditions are eliminated or controlled. Safety engineers identify safety critical items, conduct safety tests and evaluations and develop safety plans and guidelines. Health hazards are also important to safety engineers. Occupational health hazard assessments and operating and support hazard analysis is key in ensuring environment safety and health (ESH). See Figure 4.b System safety focus during the system life cycle. (Office of the Deputy Assistant Secretary of Defense, 2016).

4.4.1. Figure 4.b System safety focus during the system life cycle

Concept Stage		Development Stage		Production Stage	Utilization Stage / Support Stage		Retire-ment Stage
Establish Safety Objectives	Initial Hazard Analysis	Update Hazard Analysis	Safety Verifi-cation	Sys Safety Assessment & Certification	Maintenance of Safety Baseline	Mishap Investigation and Correction	Safe Disposal

5. SYSTEM DEPLOYMENT

During system deployment, a system is installed in an operational environment. At this phase of the life cycle, the system moves development to on site operation. System deployment includes site preparation, system installation, system checkout, user training and support engineer training. At this point in the development life cycle the SoS has been integrated, verified and is ready for installation.

5.1. Site preparation

To prepare a site for deployment, several key activities must take place. Prior to delivery of the system, facility managers, systems administrators and the development teams must discuss site planning, preparation, and system installation. Engineers must plan for the system installation and transition. Understanding the delivery, configuration, installation and maintenance plan prior to installation will ensure its success. (“CHAPTER 1 – Site Preparation”, n.d.).

Environmental factors must be considered to ensure that the required system components will be operational. This includes airflow, temperature and humidity that could impact mission critical equipment. Configuration issues such as the physical topology and needed peripherals should be considered. Knowing how much power is needed to support the system, distance to power outlets and backup power supply sources are addressed during site preparation. The space needed, mounted racks and the ability to fit equipment through facility doors are also considerations that are important to address. (“CHAPTER 1 – Site Preparation”, n.d.).

Technical data is needed for site preparation. A technical data checklist will include all needed equipment as well as all steps required to avoid misses during installation. Delivery of all systems components must be verified against the compiled checklist. The development of the following is also part of site preparation: system installation and checkout procedure; operating and maintenance instructions; drawings and facility specifications; modification instructions; and inspection procedures. (Ryen, 2008).

5.2. System installation

Hardware configuration of components is the first step in the installation process. Since the system is a SoS and very large, the installation will need to be done in stages. This is to mitigate risks by deploying only the system core and adding features in phases. Phased deployments require an understanding of dependencies between successive deployments. Installation prioritization will be determined based on these dependencies. Following installation, the system will be validated using a series of performance acceptance tests. Validation will confirm that the installed system meets the user’s needs and intended purpose. (Ryen, 2008).

5.3. System checkout

System checkout is the process to make sure the system and personnel are ready to go live. This is the transition to system operation and maintenance. Once the system is fully operational, measurements can be made to test how effective the system is in meeting the originally identified goals. This is done using verification and validation. Verification confirms

that the system meets the specified requirements while validation ensures it fulfills its intended use. The continued iterative process of technical data collection, analysis, reporting and documentation follows throughout the life cycle of the SoS. (Ryen, 2008).

5.4. User and Support engineer training

Section 7.1 of COBIT 5, control objectives, covers training plan development. A training plan is part of every information system development, implementation or modification project. Learning objectives, resources, key milestones, dependencies and critical path tasks that impact the delivery are identified in the training plan. The training plan addresses all impacted groups, including business end users, IT operations, support and IT application development training, and service providers. Alternative training strategies based on business needs are also addressed.

The training plan will also cover necessary training equipment identified during the development phase. Necessary courses on the training equipment will be described for support engineers. Support engineers will support the operation and maintenance.

Training is monitored to obtain feedback that could lead to potential improvements in either the training or the system. The three primary areas for training include: training for personnel, training for confidentiality, training for support engineers responsible for operations and support of the system.

6. PRODUCT SUPPORT

6.1. Maintenance

Once the customer has accepted the SoS, system performance is measured and monitored throughout the rest of the systems life cycle. A systems maintenance plan is a working document of measured results. Any issues, suggested improvements or identified technology upgrades are documented for consideration. As funds become available, system upgrades deemed beneficial to the system baseline will be incorporated. Maintenance is performed over the systems operational life. (Ryen, 2008).

Maintenance processes include providing user support, system operation data collection, changes or upgrades to the system and maintaining configuration control of the system. Operations and maintenance plan reviews are conducted and maintenance procedures are developed at this stage. Maintenance processes provide system performance reports, operation logs, maintenance records and are used to identify defects. (Ryen, 2008).

6.2. Logistics support

A supply or logistics support system is used to meet life cycle cost goals and support operational availability. Providing the most cost-effective logistics support is done using a level-of-repair analysis. This is a mathematical analysis model used to determine cost effectiveness of repairing or replacing a faulty part. Logistics support includes all spares, repair parts, consumables, special supplies, and related inventories needed for system support. This includes supporting mission-oriented equipment; software; testing and support equipment; transportation and handling equipment; training equipment; and facilities.

Forecasts of replenishment and spare part that will support the system for the entire life cycle should be identified. Packaging, storage and transportation of parts should also be considered as part of logistics support.

6.3. Disposal

An assessment of the operations of the SoS is performed periodically to determine the systems efficiency. Once the cost to operate and maintain the system exceed the cost to develop a new system, considerations for replacing the existing system should be taken. As equipment approaches the end of usefulness, certain steps must be taken for system disposal. This includes: taking an audit of disposed hardware and software inventory; capturing final software images; archiving all system documentation; and closing contracts associated with the system being disposed. (Ryen, 2008).

.

7. REFERENCES

Dutcher, B. (2010, March 15). Determining the role of the IA/Security Engineer. Retrieved from https://www.sans.org/reading-room/whitepapers/leadership/determining-role-ia-security-engineer-33508

Eisenhart, B. (2007). *System engineering management plan - TMDD SEMP*. Retrieved from Institution of transportation engineers website: http://library.ite.org/pub/e28147b5-2354-d714-5141-a649eb30f140

Fraunhofer SIT - Security Test Lab - About Us. (n.d.). Retrieved from https://testlab.sit.fraunhofer.de/content/testlab/

IT Governance Ltd. (2001). *COBIT - an IT governance framework*. Retrieved from http://www.itgovernanceusa.com/cobit.aspx
COBIT 5 Toolkit collection download

ITIL Help. (2005). *COBIT IT assessment/audit tool*. Retrieved from Bestpracticehelp.com website: http://www.bestpracticehelp.com/COBIT_IT_Assessment_Audit_Tool.pdf

Lockheed Martin Corporation. (2014). *Systems security engineering*. Retrieved from National Defense Industrial Association website: http://www.ndia.org/Divisions/Divisions/SystemsEngineering/Documents/Rodgers_LM%20Tom%20Rodgers%20SystemSecurityEngineering%205-20-2014.pdf

Office of the Deputy Assistant Secretary of Defense. (2016, September 1). Systems engineering: Initiatives. Retrieved from www.acq.osd.mil/se/initiatives/init_safety.html

Raytheon Learning Institute. (n.d.). *Specialty engineering: Principles of systems engineering*[PDF]. Retrieved from http://www-edlab.cs.umass.edu/cs491m/slides/lecture13.pdf

Ryen, E. (2008). *Overview of the systems engineering process*. Retrieved from North Dakota Department of Transportation website: https://www.dot.nd.gov/divisions/maintenance/docs/overviewofsea.pdf

US Department of Transportation Federal Highway Administration. (2013, April 17). California Division | Federal Highway Administration. Retrieved from https://www.fhwa.dot.gov/cadiv/segb/views/document/sections/section3/3_6_4.cfm

Zororo, T. (2016, April). *Implementing governance of enterprise IT (GEIT) using COBIT 5: A business driven approach*. Paper presented at COBIT Conference, New Orleans, LA. Retrieved from http://www.isaca.org/Education/Conferences/Documents/COBIT/COBIT-NA-2016/2.pdf