Draft Infrastructure Framework for a Generic Repository Development Organization

Fuel Cycle Research & Development

Prepared for
U.S. Department of Energy
Used Fuel Disposition Campaign

Sandia National Laboratories
September 16, 2016
FCRD-USED-2016-000079
SAND2016-9091 R

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

Sandia National Laboratories

Sandia National Laboratories is a multi-mission laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Abstract

This document is milestone M2FT-16SN080503021: Generic Organizational and Procedural Framework for DOE-Managed HLW and SNF Licensing, the result of efforts under work package FT-16SN08050302 “Establish organizational framework to meet regulator expectations – SNL.” The objective of this effort was to develop this document identifying and summarizing the principal elements of an infrastructure organizational framework for a generic repository development organization with the responsibility to site, characterize, design, license, construct and operate a repository for the disposal of high-level radioactive waste (HLW) and spent nuclear fuel (SNF) managed by the U.S. Department of Energy. This organizational framework contemplates an organization structured to facilitate compliance with U.S. Nuclear Regulatory Commission (NRC) expectations and American Society of Mechanical Engineers NQA-1 quality standards, and other internal DOE practices.

This report presents a generic framework of an organization needed and the functions of the organizational elements necessary to execute a generic repository development effort. This report is supported by another milestone report (M4FT-16SN080503032) which identifies the procedures that need to be developed for a generic repository development organization to perform its functions.

This document describes the framework for a generic organization with the responsibility to site, characterize, design, license, construct and operate a repository for the disposal of high-level radioactive waste (HLW) and spent nuclear fuel (SNF) managed by the Department of Energy (DOE). The organizational framework suggested is independent of the facility location and disposal medium. It is assumed that the facility is to be licensed under U.S. Nuclear Regulatory Commission (NRC) regulations with DOE as the applicant (licensee). Detailed organizational elements reflect a workforce functional composition and practices that facilitate compliance with NRC expectations and the American Society of Mechanical Engineers (ASME) NQA-1 2015 Quality Assurance Requirements for Nuclear Facility Applications standard.

Table of Contents

Figures

Tables

Acronyms

ADAMS	Agency wide Documents Access and Management System
AEA	Atomic Energy Act of 1954, as amended
ASME	American Society of Mechanical Engineers
CAP	Corrective Action Program
CEQ	Council on Environmental Quality
CFR	Code of Federal Regulations
COTS	Commercial off the Shelf Software
DoD	U.S. Department of Defense
DOE	U.S. Department of Energy
EA	Environmental Assessment
ECP	Employee Concerns Program
EIS	Environmental Impact Statement
EPA	U.S. Environmental Protection Agency
EVMS	Earned Value Management System
FEDRAMP	Federal Risk and Authorization Management Program
FEIS	Final Environmental Impact Statement
GIS	Geographic Information System
HIPAA	The Health Insurance Portability and Accountability Act of 1996 (Pub. Law. 104–191)
HLW	High-Level Radioactive Waste
HPC	High Performance Computing
HR	Human Resources
IaaS	Infrastructure as a Service
IT	Information Technology
LSN	Licensing Support Network
MOW	Members of the Workforce
NARA	National Archives and Records Administration
NEPA	National Environmental Protection Act
NIST	National Institute of Standards and Technology
NOC	Network Operations Center

NQA-1	American Society of Mechanical Engineers Quality Standard for Nuclear Facilities
NRC	U.S. Nuclear Regulatory Commission
NSC	Nuclear Safety Culture
NUREG	NRC Regulatory Guide
NWPA	Nuclear Waste Policy Act of 1982
PaaS	Platform as a Service
PEIS	Program Environmental Impact Statement
PII	Personally Identifiable Information
QA	Quality Assurance
QAM	Quality Assurance Manager
RAIDS	Request for Additional Information Development System
RD&D	Research, Development, and Demonstration
RDO	Repository Development Organization
SaaS	Software as a Service
SAN	Storage Area Network
SCWE	Safety Conscious Work Environment
SNF	Spent Nuclear Fuel
SNL	Sandia National Laboratories
YM	Yucca Mountain

Draft Infrastructure Framework for a Repository Development Organization

ES-1 Executive Summary

In March 2015, the President found in a Presidential Memorandum for the Secretary of Energy (Obama 2015) that "the development of a repository for the disposal of high-level radioactive waste resulting from atomic energy defense activities only is required." The presidential finding is supported by the March 2015 *Report on Separate Disposal of Defense High-Level Radioactive Waste* (DOE 2015). .

This document describes a framework for a generic organization with the responsibility to site, characterize, design, license, construct and operate a repository for the disposal of high-level radioactive waste (HLW) and spent nuclear fuel (SNF) managed by the Department of Energy (DOE). The organizational framework suggested is independent of the facility location and disposal medium. The effort will be conducted under applicable DOE Orders and regulations of the U.S. Environmental Protection Agency (EPA) and the NRC. It is assumed that the facility is to be licensed under U.S. Nuclear Regulatory Commission (NRC) regulations with DOE as the applicant (licensee). The detailed organizational elements described herein reflect a workforce functional composition and practices that facilitate compliance with NRC quality assurance requirements, assumed here to be equivalent to implementing the ASME NQA-1 2015, Quality Assurance Requirements for Nuclear Facility Applications standards.

Successful implementation of a plan to develop a repository will require an effective organization and infrastructure designed to execute the effort in compliance with DOE and regulatory expectations. The discussions in this report are based on the statutory and regulatory framework existing in 2016. Notably, the context in which the organization's work will be conducted differs substantially from that of the typical research, development and demonstration (RD&D) environment. First, there are work elements that are not customarily included in RD&D work, such as regulatory compliance, a corrective action program, and requirements / commitment management. Secondly, the rigor with which organizational assurance and quality assurance functions need to be applied and practiced is significantly greater than usually necessary in the RD&D environment.

The organization's scope of responsibility is extensive, and will take decades to accomplish. Recognizing that substantial changes will occur over such a long timeframe, this report focuses on identifying the roles and responsibilities of organizational elements that are needed to standup the organization (startup phase) and to initiate the work (initiation phase). These two phases overlap somewhat and include establishing processes and systems that will support the scientific and engineering endeavors necessary to accomplish the siting, characterization, design and licensing of the disposal facility under consideration.

The organizational elements identified in this report reflect a workforce composition and level of practice that facilitates compliance with NRC expectations and in compliance with NRC quality assurance requirements. One often all-to-frequently overlooked component of a compliance-oriented endeavor is the importance of having an outcome-aware management, technical support, and business process organization. A high-quality, regulation-aware, and technically savvy science and engineering team is of course essential; however, it is equally important that the technical team be supported by an experienced, proficient non-technical infrastructure. Ultimately, this team of professionals provides management with the means to extend policy across the organization, as well as providing the context in which operational decisions are implemented. Technical support, business, and quality processes need to be requirements- and assurance-based, as well as quality assurance-informed.

Throughout this report, several principles, concepts, and term usage are applied for clarity. 'Policies' are promulgated by RDO Management to provide overall direction to the organization. Organizational elements perform their function(s) in accordance with policy direction. In most cases, organizational

elements also perform their function(s) in accordance with a function-specific ‘Management Plan’ that is produced consistent with policy and is approved by RDO Management (e.g., Information Management Plan). If necessary, procedural controls are identified in the plan for activities that require a more rigorous level of workflow definition. Procedures are used to define processes (workflows), as discussed herein and further described in a related report (SNL 2016). The electronic information technology (IT) tools that support or facilitate the processes are referred to as ‘Systems’.

Also, this report applies a convention to distinguish specifically between the usage of the terms ‘process’ and ‘system’. Processes are essential workflows designed by an organizational element to accomplish its functional responsibilities. A ‘system’ is an IT solution that is designed to support the process, or processes, for a particular organizational element’s function(s). As an example, Information Management is an essential organizational element/function. The ‘process’ for submittal, recording, processing and retention of records is a workflow that is outlined in an Information Management Plan and may be described in detail in a Records Management Procedure. The IT solution(s) that facilitates this workflow is an Information / Records Management ‘System’ or ‘Service.’ In the report’s discussions distinguishing between an organization’s functional processes and the electronic systems or IT services that facilitate compliance with a defined process is important to avoid confusion.

A schematic timeline is shown in Figure 3 to illustrate the overall timeframe. The ‘Startup’ and ‘Initiation’ phases include most of the activities discussed in this report. This underscores that the initial focus is on establishing the overall direction, support infrastructure, and consent-based siting activities as opposed to the science and engineering organizational elements. The coincidence of the Startup and Initiation phases accommodates proceeding with consent-based siting activities in parallel with the initial development of the organization and its infrastructure.

Establishing a coherent and integrated organization necessary to begin to function in a controlled and systematic fashion aligned with enterprise objectives may take most of the first two to three years of effort. Nonetheless, progress can be made right from the start by assembling a small organization focused on its initial functions, including planning and development of the future organization. As with most similar efforts, the organization will grow from a core set of personnel focused primarily on higher level functions, customarily leveraging talents and skills from personnel in other organizations to help build the basic framework that will allow it to consolidate functions and incubate distinct organizational elements. The effort to assemble, train, and enable early participants will consume a substantial part of the core group’s time.

In such a long-term effort the initial organization and its subsequent variations will need to function with demonstrable continuity for decades. The license amendment for permanent closure (10 CFR 60.51) will likely be 50 or more years from the beginning of the effort. Also, the closure license may rely on information gathered very early in the effort such as “tests, experiments, or analyses pertinent to the long-term isolation of emplaced wastes within the geologic repository” (10 CFR 60.51(a)(4)). The duration of this effort will span two to three workforce generations and significant changes in direction, the implementing organization, and the workforce is to be expected. The organizational evolution description that follows should be viewed as progressively more indefinite, the further it is projected into the future.

Figures 4 through 8 illustrate a possible development sequence for the organization over time. The Startup Organization (Figure 4) has the fundamental elements to foster two important high-level objectives in parallel: (a) systematically begin to build the organization; and, (b) conduct foundational work such as consent-based siting. Note that the organizational elements identified in Figure 4 do not initially require the level of staffing necessary later in the effort. There are more than 25 functions shown in Figure 4; however, these functions can be initiated by about 10 to 15 persons in the first 3 to 6 months of operation. The principal work of leadership personnel is to establish the policy basis for the organization, rough out a fundamental plan, and acquire personnel to fill-out the organization.

Section 4 describes the Organizational Elements needed to execute the activities. Generally, for each organizational element, the respective section addresses its principal:

- Functions, roles and responsibilities;
- Importance in the context of enterprise and regulatory requirements; and,
- Observations based on previous experience, as appropriate.

RDO Management provides the vision, the management approach, enterprise policies and identifies procedures for the assembly and overall operation of the organization. The entire organization's activities need to be conducted in accordance with Nuclear Safety Culture (NSC) principles reflected in a Safety Conscious Work Environment (SCWE) and an effective Quality Assurance (QA) program that is consistent with DOE expectations, and those of the regulator. Table 1 lists the RDO Management Functional Elements.

Table 1 — RDO Management Functional Elements

Legal Counsel	Provides support to the RDO Manager on the wide variety of legal issues that will inevitably arise.
Quality Assurance	Defines the enterprise level requirements necessary to formulate a high quality and streamlined Quality Assurance program to satisfy ASME NQA-1 2015.
Public Engagement and Consent-Based Siting	Defines, designs and implements processes for public engagement in organization activities include activities that define, design, and implement processes to enable a phased, adaptive, and consent-based approach to siting.
Regulatory/Licensing	Responsible for organization's regulatory support activities regardless of the regulator's identity (e.g., NRC, EPA, or state entities).

Operations Management is the organizational element responsible for the direction, coordination, and oversight the day-to-day functionality of the principal support organizations shown in Table 2. Though discussed in more detail in Section 4, bulleted items in Table 2 represent functions of particular significance in the context of the organizational element's scope.

IT (Information Technology) systems supporting the organization's functions are described in Section 4.2.4. The current IT environment provides marked advantages over those available for use on previous repository development efforts.

Table 2 — Operations Management Functional Elements

Business Management	Defines, designs and implements processes that enable a workforce to accomplish its objectives using established work processes, and business management systems. • Employee Concerns Program (ECP) • Conform procurement processes to the QA program • Training
Organization Assurance	Defines, designs and implements processes to oversee the organization's operational and functional fidelity to ensure integration and appropriate conduct of operations. • Nuclear Safety Culture (NSC) • Safety Conscious Work Environment (SCWE) • Corrective Action Program (CAP) • Requirements Management • Commitment Management • Self-Assessment • Risk Management • Knowledge Management
Information Management	Defines, designs and implements processes that enable the workforce to accomplish its objectives using enterprise-wide information processes and IT systems. • Records Management (including Email) • Correspondence Control • Document Development • Reference Registry • Document Control • Data Management • Software Configuration Management • License Support Network (LSN)
IT Systems	Defines, designs, implements, and maintains IT systems to support the organization's processes and functions.

Science and Engineering is the organizational element responsible for the direction, coordination, performance, and oversight of science and engineering activities. These will include interactions with DOE to formulate direction to mitigate complex issues involving internal and external organizations, present effort-related material to upper management, approve technical and non-technical products and documents, and allocate resources to the performance of regularly scheduled work and rapid response tasks associated with repository sciences and engineering.

As described in Section 3, "The specific configuration and details of the scientific and engineering organizational elements is beyond the scope of this report." The context in which the science and engineering organizational elements will operate has yet to be established. Hence, only general descriptions of the following functions are provided.

1. Introduction

This document is milestone M2FT-16SN080503021: Generic Organizational and Procedural Framework for DOE-managed HLW and SNF Licensing, under work package FT-16SN08050302 “Establish organizational framework to meet regulator expectations – SNL.” The objective of this effort was to develop this draft document identifying and summarizing the principal elements of a generic repository development organization (RDO) infrastructure and organizational framework.

This document describes the framework for a generic organization with the responsibility to site, characterize, design, license, construct and operate a repository for the disposal of high-level radioactive waste (HLW) and spent nuclear fuel (SNF) managed by the Department of Energy (DOE). The organizational framework suggested is independent of the facility location and disposal medium. It is assumed that the facility is to be licensed under U.S. Nuclear Regulatory Commission (NRC) regulations with DOE as the applicant (licensee). Detailed organizational elements reflect a workforce functional composition and practices that facilitate compliance with NRC expectations and the American Society of Mechanical Engineers (ASME) NQA-1 2015 Quality Assurance Requirements for Nuclear Facility Applications standard.

The discussion herein is based on the statutory and regulatory framework existing in 2016. DOE’s 2015 report on defense waste disposal *Report on Separate Disposal of Defense High-Level Radioactive Waste* (DOE 2015) clearly indicates a preference, if not a requirement, for pursuing public acceptability using a ‘phased, adaptive, consent-based siting approach’. The Nuclear Waste Policy Amendments Act of 1987 Section 8(b)(3) renders a ‘repository for the disposal of high-level radioactive waste resulting from atomic energy defense activities only’ (i.e., a defense waste repository) subject to NRC’s licensing authority. Under the current regulatory framework, a defense waste repository will need to comply with 10 CFR Part 60 and by reference 40 CFR Part 191.

The context in which the organization’s work will be conducted differs substantially from that of the typical research, development and demonstration (RD&D) environment. First, there are work elements that are not customarily included in RD&D work, such as regulatory compliance, a corrective action program, and requirements / commitment management. Secondly, the rigor with which organizational assurance and quality assurance functions need to be applied and practiced is significantly greater than usually necessary in the RD&D environment.

2. Background

In March 2015, the President found in a Presidential Memorandum for the Secretary of Energy (Obama 2015) that “the development of a repository for the disposal of high-level radioactive waste resulting from atomic energy defense activities only is required.” The presidential finding is supported by the March 2015 *Report on Separate Disposal of Defense High-Level Radioactive Waste* (DOE 2015), which concluded considering the President’s finding, that

> “…the Secretary may develop a Defense HLW Repository under his Atomic Energy Act of 1954 authority. In developing a Defense HLW Repository, the Secretary would be subject to U.S. Nuclear Regulatory Commission (NRC) licensing authority, but would not be subject to the NWPA’s siting provisions, apart from the State and tribal participation provisions specified in Section 101 of the NWPA” (DOE 2015, p. 2).

Additional support for the 2015 decision was provided in a 2014 DOE report, *Assessment of Disposal Options for DOE-Managed High-Level Radioactive Waste and Spent Fue*l (DOE 2014) that evaluated technical options for the permanent disposal of HLW and SNF managed by DOE. The report drew heavily on a national laboratory report titled *Evaluation of Options for Permanent Geologic Disposal of Used Nuclear Fuel and High-Level Radioactive Waste Inventory in Support of a Comprehensive National Nuclear Fuel Cycle Strategy* (SNL 2014), which summarized the inventory of both commercial and DOE-managed radioactive wastes requiring geologic disposal.

The Administration’s 2013 *Strategy for the Management and Disposal of Used Nuclear Fuel and High-Level Radioactive Waste* (DOE 2013) and subsequent documents (DOE 2014 and DOE 2015) endorse a phased, adaptive, and consent-based approach to implement a flexible waste management system incrementally to ensure safe and secure operations, gain trust among stakeholders, and adapt operations based on lessons learned (DOE 2013). On December 23, 2015 the DOE issued an Invitation for Public Comment to Inform the Design of a Consent-Based Siting Process for Nuclear Waste Storage and Disposal Facilities in the Federal Register (80 FR 79872) thereby initiating the development of its consent-based siting process.

The infrastructure elements and their functions for a generic repository development organization are described this report. The principal operating procedures necessary for a functional and compliant repository development organization (RDO) are identified and summarized in a companion document (SNL 2016).

3. Purpose and Scope

The purpose of this draft report is to identify and summarily describe the principal elements of an organizational framework for a generic RDO and is independent of type of geologic media, or the location of the disposal facility. This document elaborates on the roles and responsibilities (functions) for individual organizational elements.

Successful implementation of a repository development effort will require an effective organization and infrastructure designed to execute work in compliance with DOE and regulatory expectations. The effort will be conducted under applicable DOE Orders and regulations of the U.S. Environmental Protection Agency (EPA) and the NRC. It is assumed that the repository will be licensed by NRC with the DOE as the applicant (licensee). Work will be conducted in compliance with applicable NRC quality assurance requirements, assumed here to be equivalent to implementing the ASME NQA-1 2015, *Quality Assurance Requirements for Nuclear Facility Applications* standards.

Activities and roles described for organizational elements throughout this report will be essential components of the DOE-managed effort. Additional activities may also be required, and the list of organizational elements and functions presented here should be viewed as a comprehensive, but not necessarily complete set, of the full suite of organizational elements and associated activities. Also, a complete identification of statutes, regulations, and directives applicable to this organization is far beyond the scope of this report. However, requirements such as these are mentioned to provide context for the responsibilities of the various organizational elements.

The scope of responsibility for the organization described in this report is to site, characterize, design, license, construct and operate a repository for the disposal of DOE-managed HLW and SNF. This scope is extensive, and will take decades to accomplish. Recognizing that substantial changes will occur over such a long timeframe, this report focuses on identifying the roles and responsibilities of organizational elements that are needed to standup the organization (startup phase) and to initiate the work (initiation phase). These two phases overlap somewhat and include establishing processes and systems that will support the scientific and engineering endeavors necessary to accomplish the siting, characterization, design and licensing of the disposal facility under consideration.

The elements that are the focus of this report are unshaded in Figure 1 and referred to as the 'Management' and 'Support Group' elements in the rest of the report. Based on previous experience, the nature of these management, administrative, business, and technical support functions are well enough understood to define with some detail and will need to be firmly established as early as possible in the effort to support emerging consent-based siting, science, engineering, and regulatory compliance activities. The specific configuration and details of the scientific and engineering organizational elements is beyond the scope of this report, and are expected to evolve as planning proceeds in the first year or two.

The organizational elements identified herein reflect a workforce composition and level of practice that facilitates compliance with NRC expectations. It is assumed that the work will be conducted in compliance with NRC quality assurance requirements. One often overlooked component of a compliance-oriented endeavor is the importance of having an outcome-aware management, technical support, and business process organization. A high-quality, regulation-aware, and technically savvy science and engineering team is of course essential; however, it is equally important that the technical team be supported by an experienced, proficient non-technical infrastructure. The unshaded portions of Figure 1 illustrate the professional non-technical (not science and engineering) team elements needed to provide support and business process management to ensure success of a geologic repository development effort. Figure 2 shows the support organization elements and their associated functions. The organizational elements discussed herein are organized in this context.

Ultimately, this team of professionals provides management with the means to extend policy across the organization, as well as providing the context in which operational decisions are implemented. Technical support, business, and quality processes need to be requirements- and assurance-based, as well as quality assurance-informed.

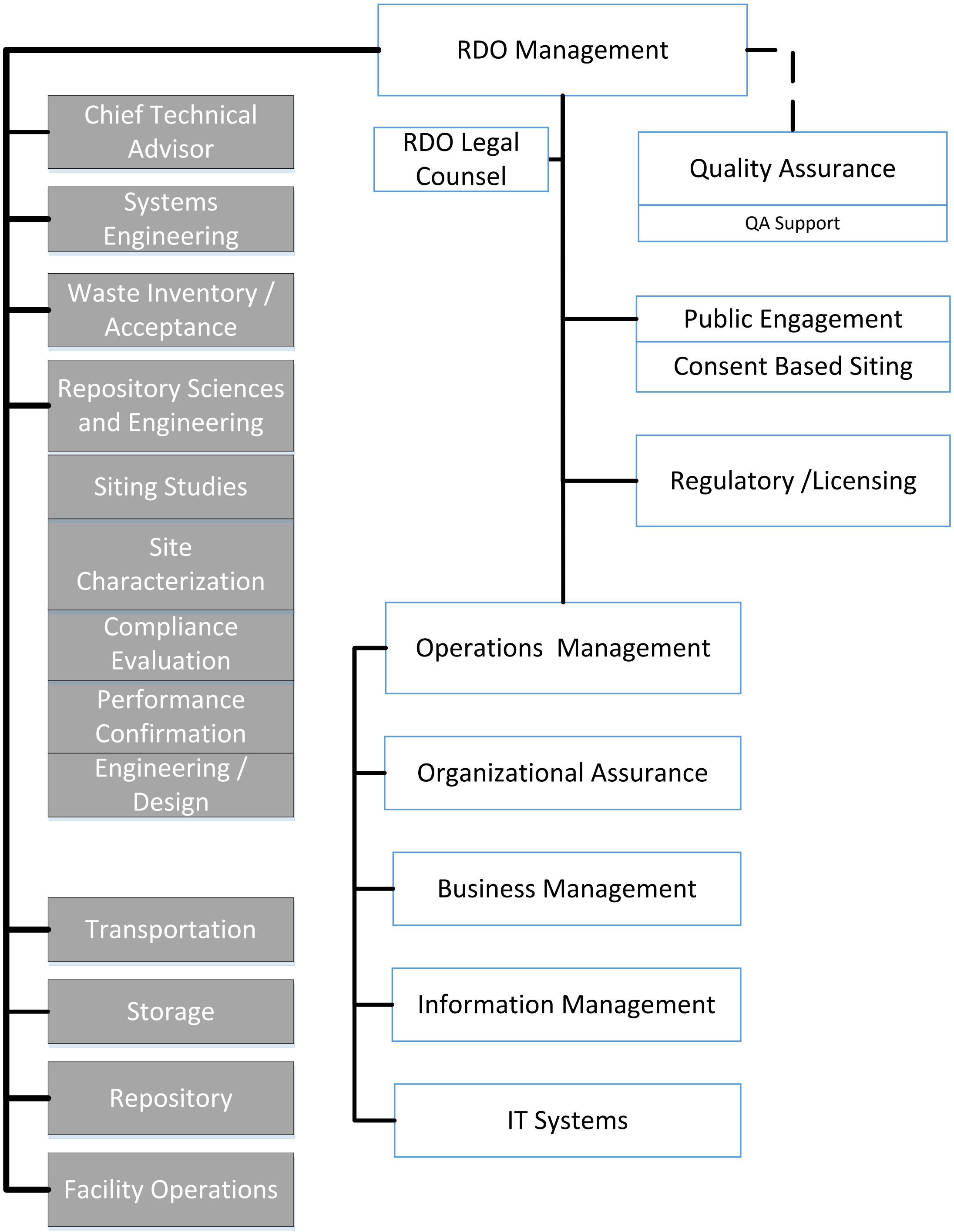


Figure 1 — RDO Organizational Elements

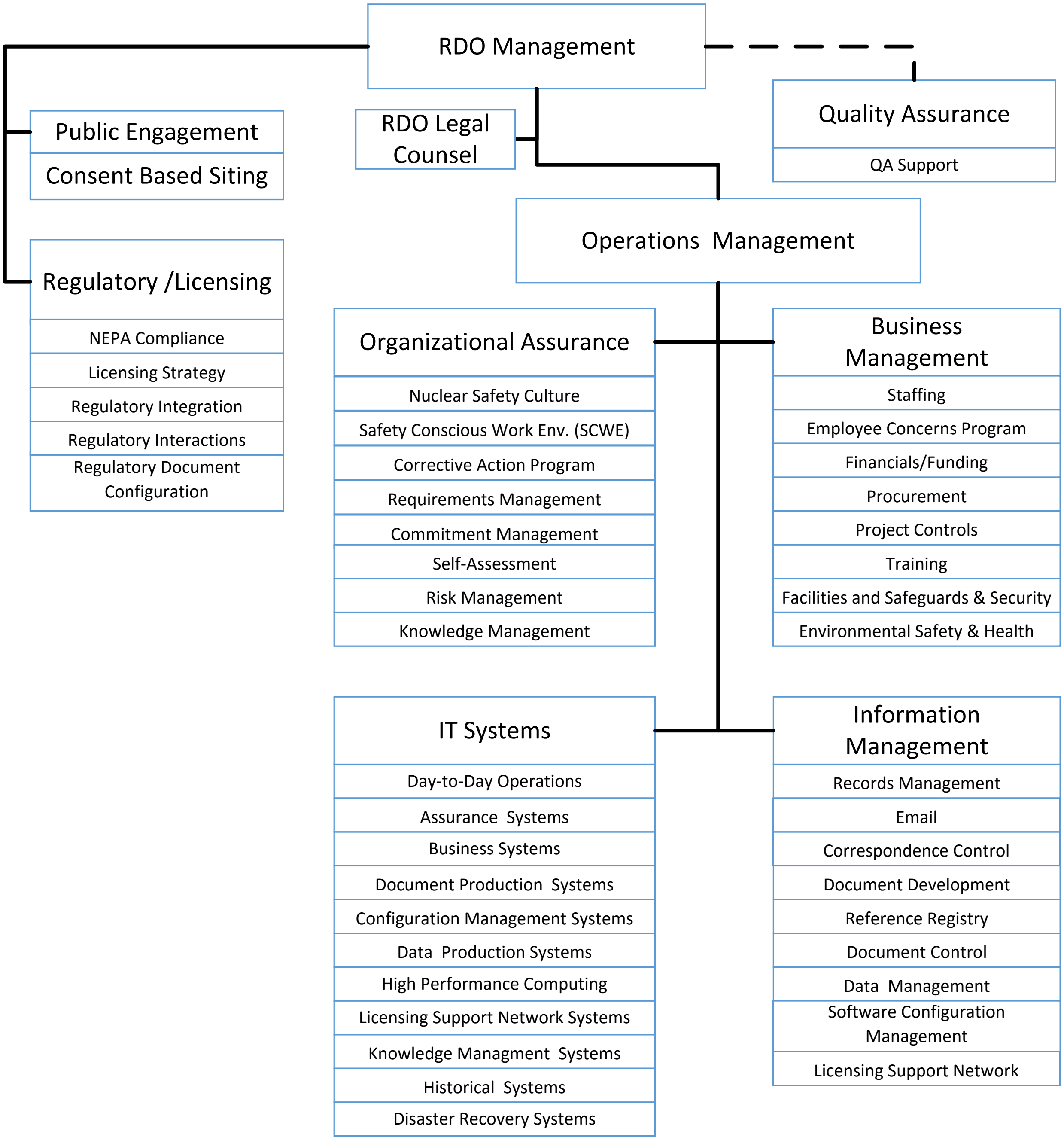


Figure 2 — Support Organization Elements Showing Functions

3.1 Principles, Concepts, and Terms

For clarity, several principles, concepts, and term usage are applied throughout this report. ‘Policies’ are promulgated by RDO Management to provide overall direction to the organization. Organizational elements perform their function(s) in accordance with policy direction. In most cases, organizational elements also perform their function(s) in accordance with a function-specific ‘Management Plan’ that is produced consistent with policy and is approved by RDO Management (e.g., Information Management Plan). If necessary, procedural controls are identified in the plan for activities that require a more rigorous level of workflow definition. Procedures are used to define processes (workflows), as discussed herein and further described in a related report (SNL 2016). The electronic information technology (IT) tools that support or facilitate the processes are referred to as ‘Systems’.

Also, this report applies a convention to distinguish specifically between the usage of the terms ‘process’ and ‘system’. Processes are essential workflows designed by an organizational element to accomplish its functional responsibilities. A ‘system’ is an IT solution that is designed to support the process, or processes, for a particular organizational element’s function(s). As an example, Information Management is an essential organizational element/function. The ‘process’ for submittal, recording, processing and retention of records is a workflow that is outlined in an Information Management Plan and described in detail in a Records Management Procedure. The IT solution(s) that facilitates this workflow is an Information / Records Management ‘System’ or ‘Service.’ In the following discussions distinguishing between an organization’s functional processes and the electronic systems or IT services that facilitate compliance with a defined process is important to avoid confusion.

3.2 Timeframe

The schematic timeline shown in Figure 3 illustrates the overall effort’s timeframe. The ‘Startup’ and ‘Initiation’ phases include most of the activities discussed in this report. This underscores that the initial focus is on establishing the effort’s overall direction, support infrastructure, and consent-based siting activities as opposed to the science and engineering organizational elements. The coincidence of these phases accommodates proceeding with consent-based siting activities in parallel with the initial development of the organization and its infrastructure.

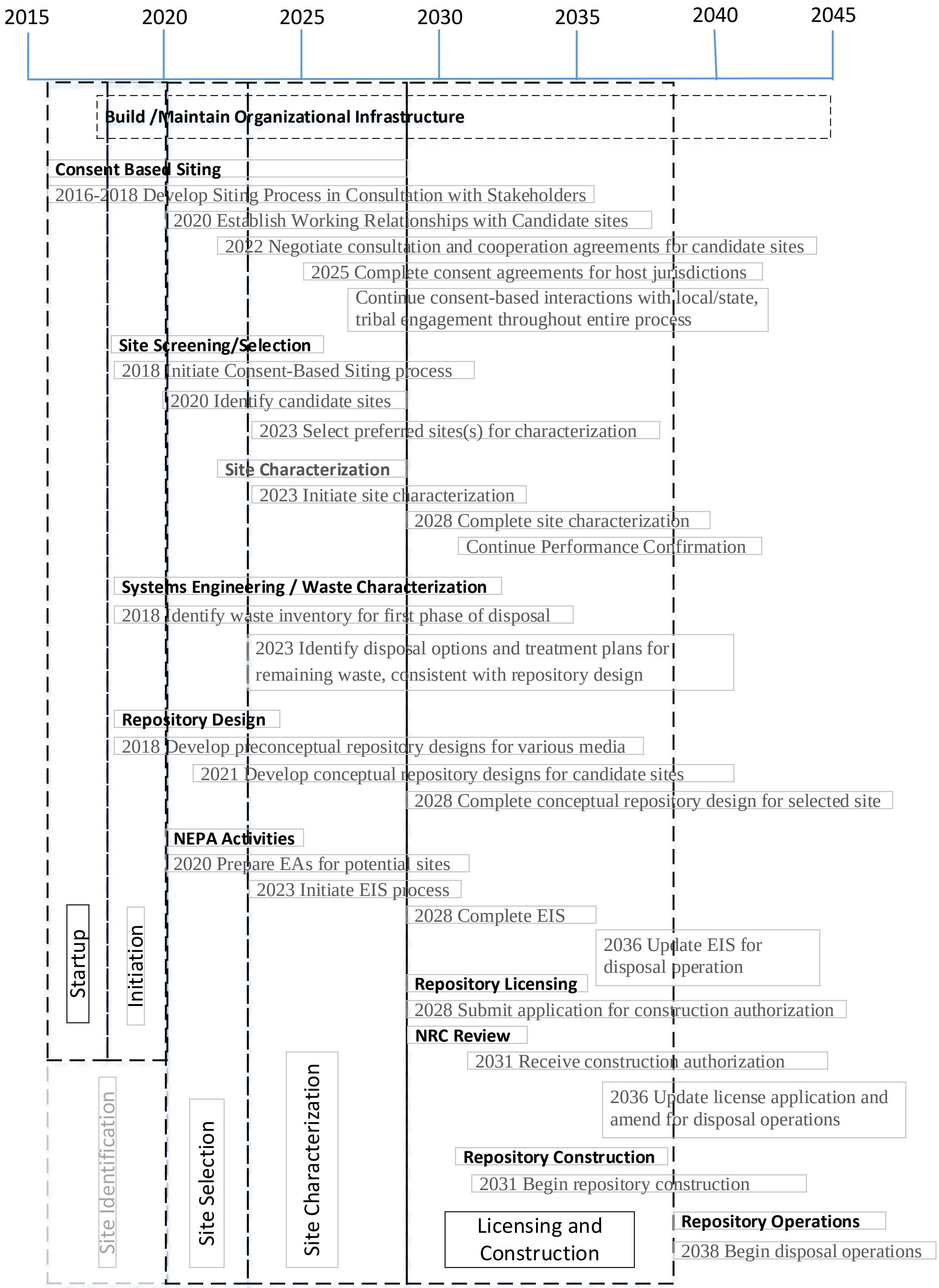

2015
2020
2025
2030
2035
2040
2045
Build /Maintain Organizational Infrastructure
Consent Based Siting
2016-2018 Develop Siting Process in Consultation with Stakeholders
2020 Establish Working Relationships with Candidate sites
2022 Negotiate consultation and cooperation agreements for candidate sites
2025 Complete consent agreements for host jurisdictions
Continue consent-based interactions with local/state, tribal engagement throughout entire process
Site Screening/Selection
2018 Initiate Consent-Based Siting process
2020 Identify candidate sites
2023 Select preferred sites(s) for characterization
Site Characterization
2023 Initiate site characterization
2028 Complete site characterization
Continue Performance Confirmation
Systems Engineering / Waste Characterization
2018 Identify waste inventory for first phase of disposal
2023 Identify disposal options and treatment plans for remaining waste, consistent with repository design
Repository Design
2018 Develop preconceptual repository designs for various media
2021 Develop conceptual repository designs for candidate sites
2028 Complete conceptual repository design for selected site
NEPA Activities
2020 Prepare EAs for potential sites
2023 Initiate EIS process
2028 Complete EIS
2036 Update EIS for disposal operation
Repository Licensing
2028 Submit application for construction authorization
NRC Review
2031 Receive construction authorization
2036 Update license application and amend for disposal operations
Repository Construction
2031 Begin repository construction
Repository Operations
2038 Begin disposal operations
Startup
Initiation
Site Identification
Site Selection
Site Characterization
Licensing and Construction

Figure 3 — Schematic Timeline

3.3 Organizational Development with Time

Establishing a coherent and integrated organization necessary to begin to function in a controlled and systematic fashion aligned with enterprise objectives may take most of the first two to three years of effort. Nonetheless, progress can be made right from the start by assembling a small organization focused on its initial functions, including planning and development of the future organization. As with most similar efforts, the organization will grow from a core set of personnel focused primarily on higher level functions, customarily leveraging talents and skills from personnel in other organizations to help build the basic framework that will allow it to consolidate functions and incubate distinct organizational elements. The effort to assemble, train, and enable early participants will consume a substantial part of the core group’s time.

In such a long-term effort the initial organization and its subsequent variations will need to function with demonstrable continuity for decades. The license amendment for permanent closure (10 CFR 60.51) will likely be 50 or more years from the beginning of the effort. The closure license may rely on information gathered very early in the effort such as “tests, experiments, or analyses pertinent to the long-term isolation of emplaced wastes within the geologic repository” (10 CFR 60.51(a)(4)). The duration of this effort will span two to three workforce generations and significant changes in direction, the implementing organization, and the workforce is to be expected. The organizational evolution description that follows should be viewed as progressively more indefinite, the further it is projected into the future.

Figures 4 through 8 illustrate a possible development sequence for the organization over time. The Startup Organization (Figure 4) has the fundamental elements to foster two important high-level objectives in parallel: (a) systematically begin to build the organization; and, (b) conduct foundational work such as consent-based siting. Note that the organizational elements identified in Figure 4 do not initially require the level of staffing necessary later in the effort. There are more than 25 functions shown in Figure 4; however, these functions can be initiated by about 10 to 15 persons in the first 3 to 6 months of operation. The principal work of leadership personnel is to establish the policy basis for the organization, rough out a fundamental plan, and acquire personnel to fill-out the organization.

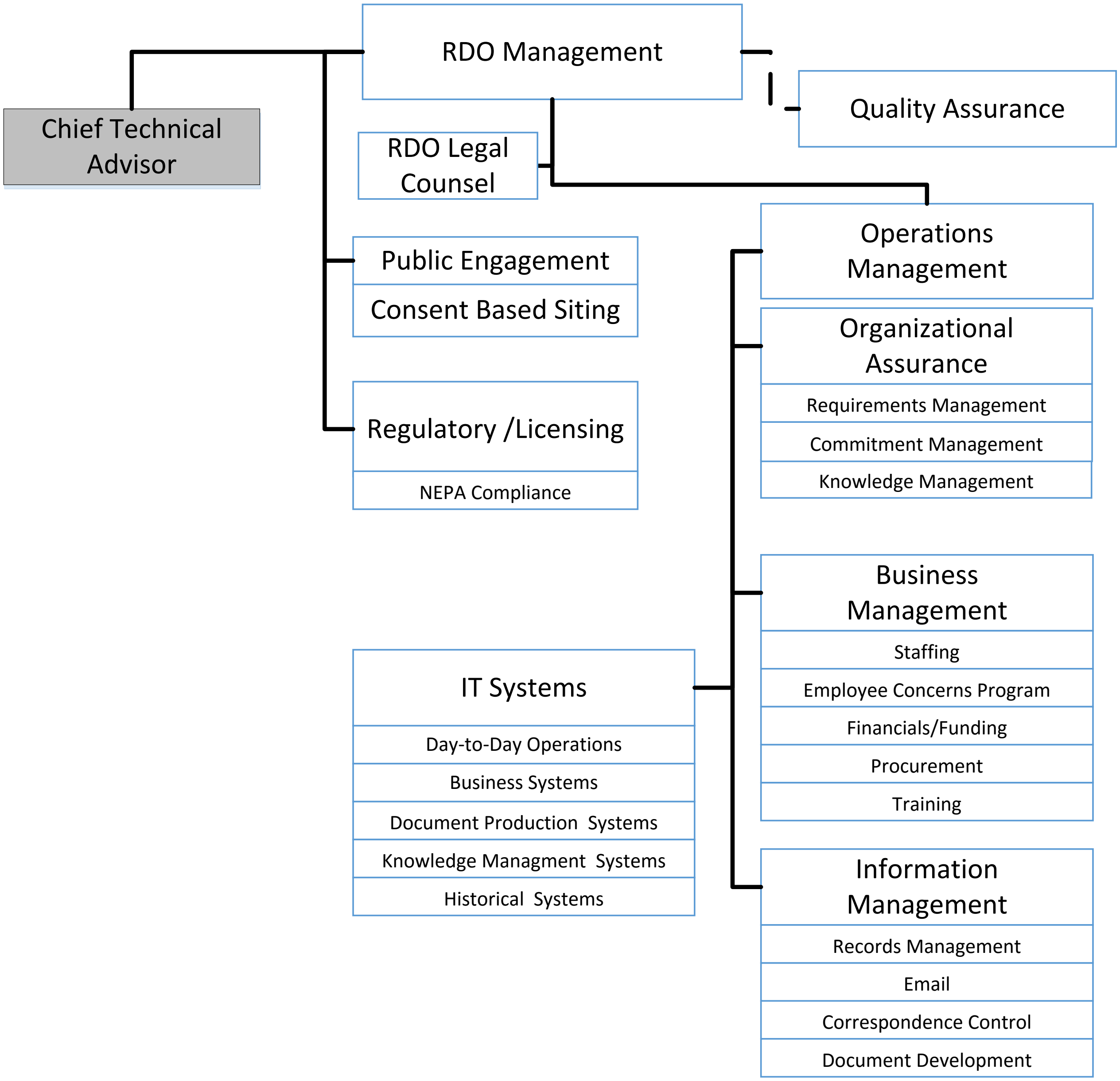


Figure 4 — Startup Phase Organization

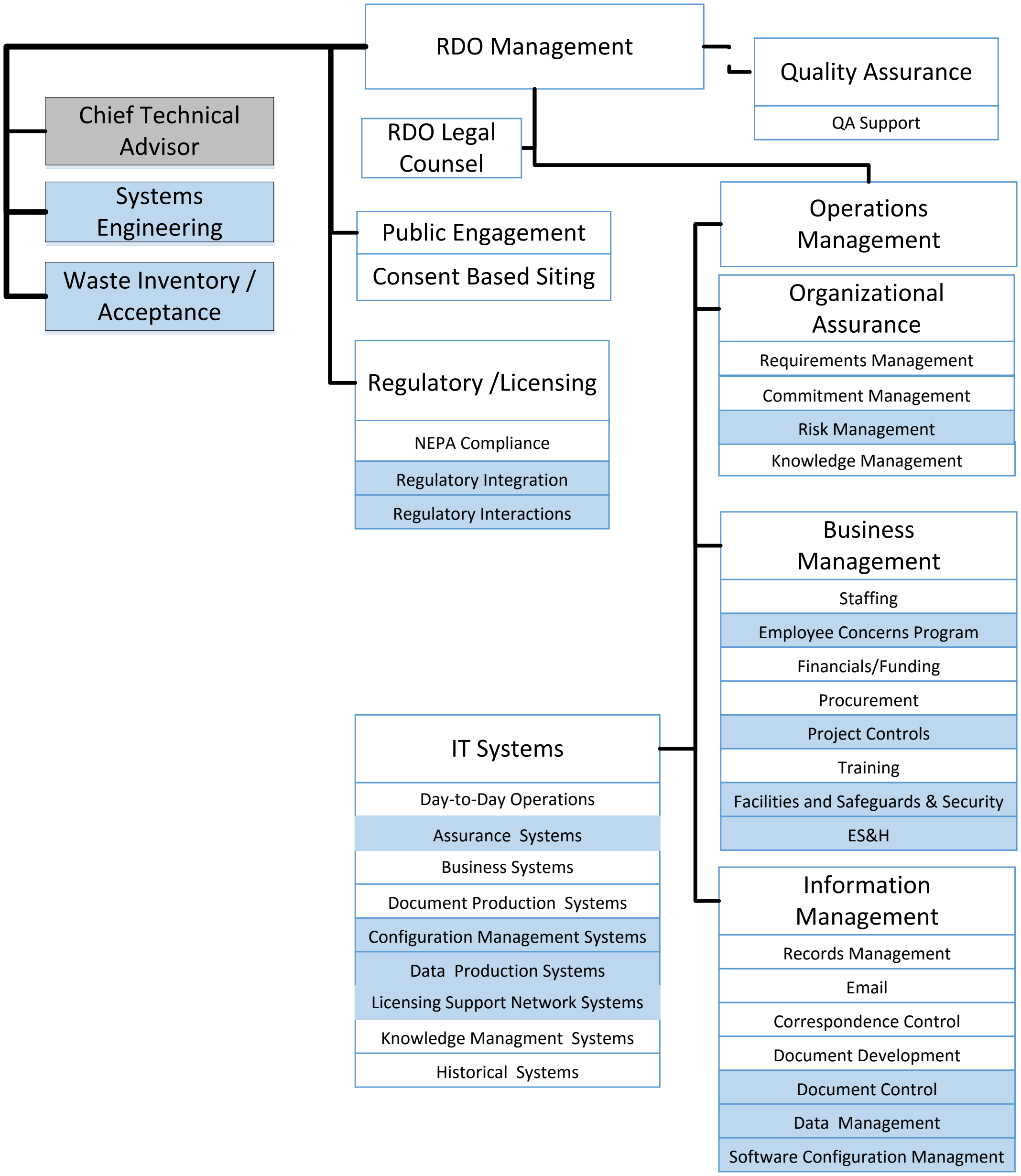


Figure 5 — Initiation Phase Organization

Note: functional elements added to support a particular phase are shaded (filled) to highlight their addition.

The Initiation Phase Organization (Figure 5) adds support system functions that will be needed to underpin work done in the Siting Phase. By the time the technical siting work begins, the Management, Consent-Based Siting, and Support Groups functions are fundamentally operational. A readiness review should be conducted in the latter half of the Initiation Phase to confirm this. The Systems Engineering and Waste Inventory/Acceptance elements begin their work in this phase, and continue throughout the effort. It should be kept in mind that refinement in established organizational elements is expected, and an element’s plans, processes, and procedures will continue to develop over time.

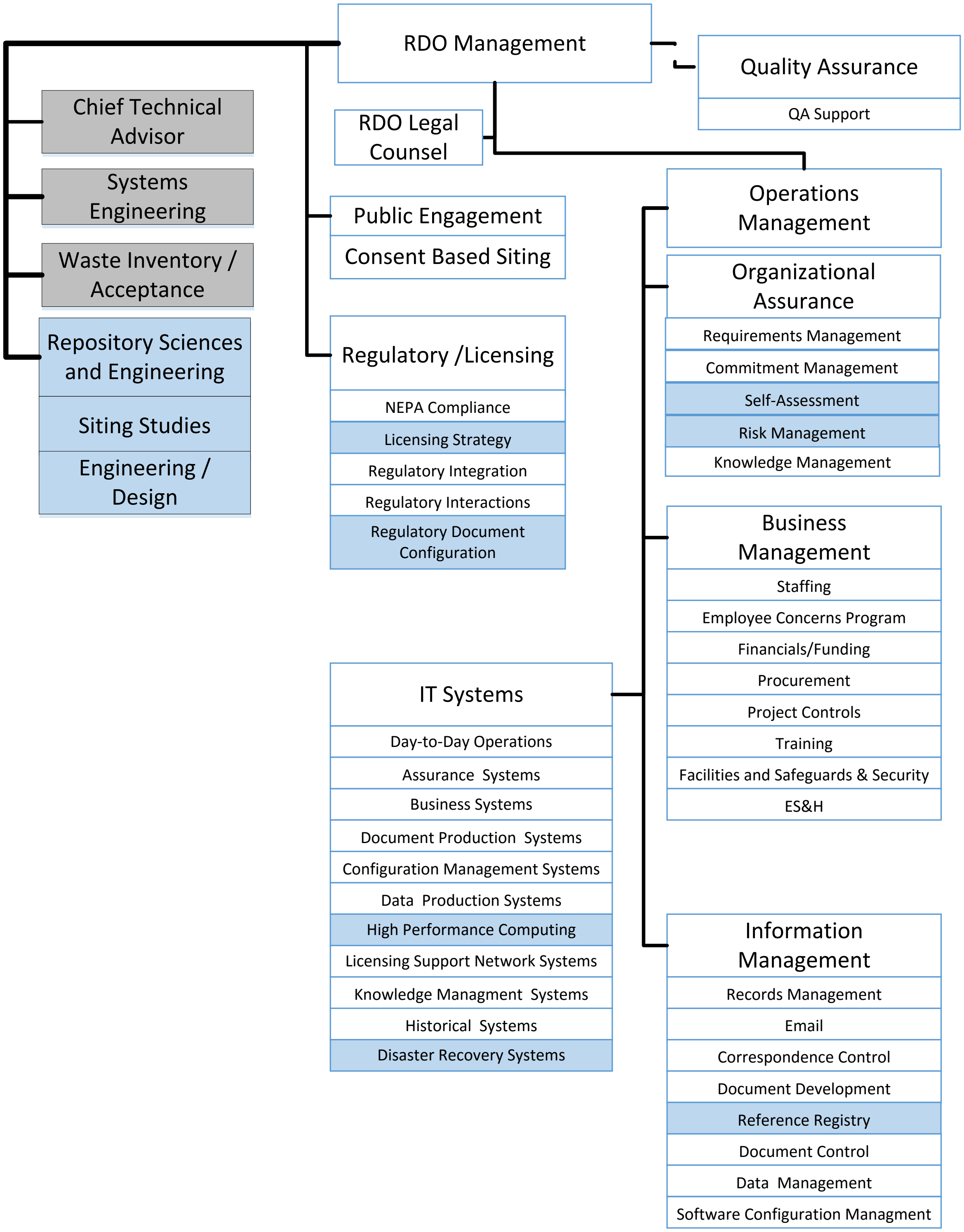


Figure 6 — Siting Phase Organization

Note: functional elements added to support a particular phase are shaded (filled) to highlight their addition.

The Siting Phase Organization (Figure 6) adds technical work elements to support the development of National Environmental Policy Act (NEPA) Environmental Assessments prepared during this phase to assess the potential impacts of site characterization and begin the NEPA documentation processes ultimately leading to an EIS.

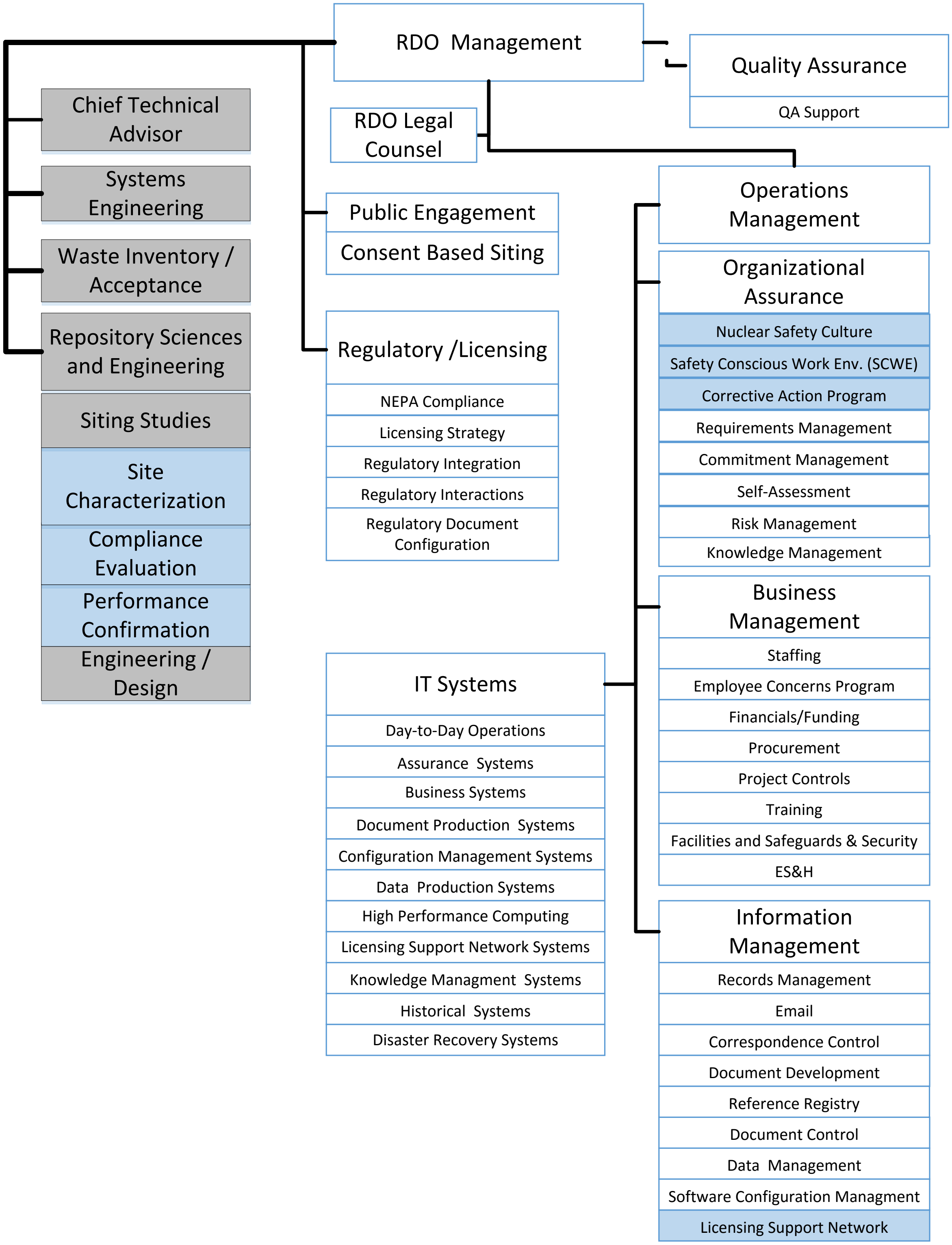


Figure 7 — Site Characterization Phase Organization

Note: functional elements added to support a particular phase are shaded (filled) to highlight their addition.

The Site Characterization Phase Organization (Figure 7) adds technical and Nuclear Safety Culture (NSC) elements as the effort begins to migrate to the technical work that will support the license application. As an example, site characterization begins to define the technical aspects of the site to be licensed, which will require demonstrated compliance with 10 CFR Part 60, including Subpart F, Performance Confirmation Program. "Performance Conformation means the program of tests, experiments, and analysis which is conducted to evaluate the accuracy and adequacy of the information used to determine with reasonable assurance that the performance objectives for the period after permanent closure will be met" (10 CFR 60.2). By regulation "The program shall have been started during site characterization and it will continue until permanent closure" (10 CFR 60.140(b)).

Strict compliance with Licensing Support Network rules at the beginning of the Site Characterization phase is prudent because the effort is nominally investigating the site for which it will eventually be submitting a license application.

The Licensing Phase Organization (Figure 8) has the same functional elements as the Site Characterization Phase Organization; however, there is a shift in work emphasis from the technical (Site Characterization and preliminary engineering design) efforts to the regulatory and compliance evaluation efforts (preclosure and postclosure safety). It is during this phase that the license application is finalized based on the characterization results and a preliminary engineering design. This information is also integral to the Final Environmental Impact Statement (FEIS).

Operationally oriented elements (Transportation, Storage, Repository, and Facility Operations) are added to the organization in anticipation of the Post-Licensing Phase. These elements begin preparation for repository construction following NRC issuance of a Construction Authorization; and full repository operations after NRC authorizes a license to receive and possess the waste (10 CFR 60.41).

During the licensing phase, NRC will focus on confirming that the prospective licensee demonstrates a proactive Nuclear Safety Culture, and demonstrable Safety Conscious Work Environment. Emphasis will be directed at the management, use, and resolution of technical and procedural issues (for both science and engineering) using the Corrective Action Program and associated IT system (NRC 2004b).

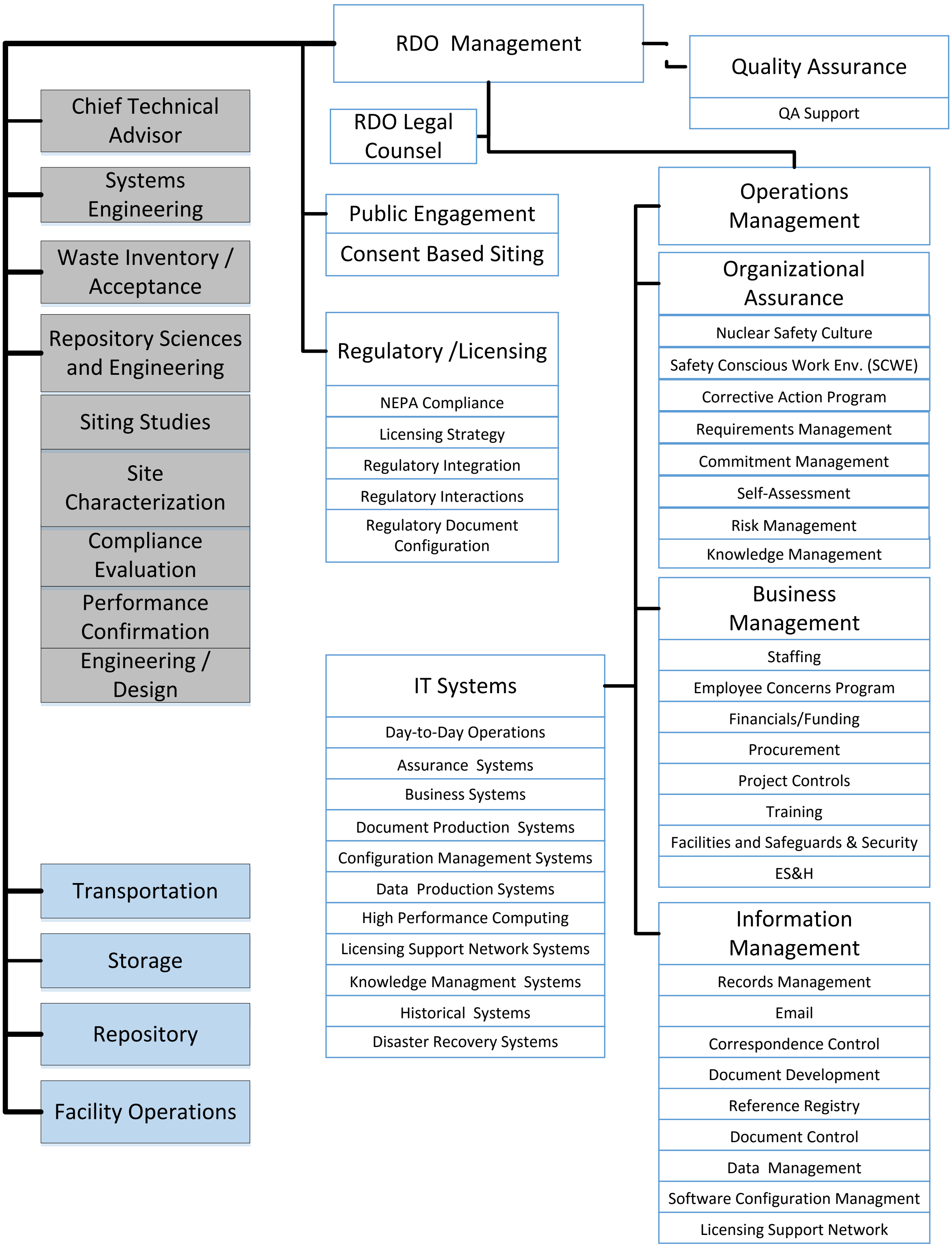


Figure 8 — Licensing Phase Organization

Note: functional elements added to support a particular phase are shaded (filled) to highlight their addition.

4. Organizational Elements

This section describes the Organizational Elements needed to execute the activities needed for repository development. Generally, for each organizational element, the respective section addresses its principal:

- Functions, roles and responsibilities;
- Importance in the context of enterprise and regulatory requirements; and,
- Observations based on previous experience, as appropriate.

4.1 RDO Management

RDO Management provides the vision, the management approach, enterprise policies and identifies procedures for the assembly and overall operation of the organization. The entire organization's activities need to be conducted in accordance with NSC principles reflected in a Safety Conscious Work Environment (SCWE) and an effective Quality Assurance (QA) program that is consistent with DOE expectations, and those of the regulator.

Because of the regulatory compliance orientation of the organization's work products, the organization's approach will be based on centralization of function and responsibility. The organization's focus will be on conscientious planning, work execution monitoring, work performance evaluation and documentation of results in each of the functional areas listed below. The fulfillment of the organization's mission will require interactions and integration with DOE management and operating contractors, National Laboratories, other waste management organizations and various external review and advisory groups, as well as, state, local and tribal governments in addition to the general public. An integrated management system should provide a single framework for the arrangements and processes necessary to address all the goals of the organization. These goals include safety, health, environmental, security, quality and economic elements and other considerations such as social responsibility (IAEA 2006).

RDO management activities that will require particular attention in the first year or two of the effort are:

- Completion of a detailed plan, including full description of the strategy (institutional, technical, regulatory), and of the organizational structure
- Initial staffing of an enterprise management team; and staffing for initial phase of project execution
- Initial development of the consent-based siting process; and full-scale implementation of the consent-based siting process
- Development of an enterprise risk management plan
- Complete development of support functions; including implementation of a QA program
- Waste inventory evaluation; and finalization of a planned inventory including consideration of options for phased disposal
- Initiation of generic repository design concepts for multiple geologic media, consistent with phased disposal of the waste inventory
- Development of a NEPA strategy
- Initial interactions with the EPA and NRC; including development of a regulatory strategy
- Performance of a rigorous readiness review mid-to-late in the initiation phase
- International collaborations

Development of a repository is an earnest undertaking. NRC takes the licensee management's role very seriously, as underscored by these examples:

- The provisions of 10 CFR Part 21 apply to facilities like the repository proposed for this effort licensed under 10 CFR Part 60. Part 21 concerns reporting of defects, in basic components that could create a substantial safety hazard, and which requires immediate notification the Commission upon the identification of such defects. In this context, basic component means a structure, system, or component, or part thereof, that affects their safety function, that is directly procured by the licensee of a facility or activity subject to the NRC regulations and in which a defect or failure to comply with any applicable regulation or license issued by the NRC could create a substantial safety hazard (10 CFR 21.3 (3)). The rule requires identification of a 'Responsible officer' which means the president, vice-president, or other individual in the organization of a corporation, partnership, or other entity who is vested with executive authority over activities subject to 10 CFR Part 21. Failure to comply can result in criminal penalties imposed on the officer.

- NRC requires information provided to the Commission to be "complete and accurate in all material respects" (10 CFR 60.10). The Commission takes this prescription very seriously. Recognizing the importance this specific kind of constraint is what emphasizes the importance of organizational assurance. Once a compliance document is issued, its contents effectively become commitments, which translate into enterprise requirements.

4.1.1 RDO Legal Counsel

Legal Counsel provides support to the RDO Manager on the wide variety of legal issues that will inevitably arise. Counsel also provides a direct interface for the effort with DOE's Office of General Counsel, which is essential to support the organization's and the Agency's regulatory roles with respect to NEPA and repository licensing.

4.1.2 Quality Assurance

The Quality Assurance Manager (QAM) defines the enterprise level requirements necessary to formulate a high quality and streamlined Quality Assurance program to satisfy ASME NQA-1 2015 *Quality Assurance Requirements for Nuclear Facilities Applications*, expected to satisfy NRC licensing rules.

In the context of this discussion, it is assumed that DOE adopts the definition of quality assurance (QA) at 10 CFR 60.150:

> "As used in this part, *quality assurance* comprises all those planned and systematic actions necessary to provide adequate confidence that the geologic repository and its subsystems or components will perform satisfactorily in service. Quality assurance includes quality control, which comprises those quality assurance actions related to the physical characteristics of a material, structure, component, or system which provide a means to control the quality of the material, structure, component, or system to predetermined requirements."

A QA program must be developed and implemented so that it is consistent with this definition and will meet applicable requirements of the NRC (e.g., 10 CFR Part 60, Subpart G) and applicable DOE Orders (e.g., DOE O 414.1d). Where NRC and DOE requirements duplicate or conflict, NRC requirements shall take precedence. The QA program will apply to structures, systems and components important to safety, to design and characterization of barriers important to waste isolation, and to related activities, and it will be implemented throughout site characterization, repository design, licensing, construction, and operations. Requirements of the QA program will apply to DOE and DOE contractors, as appropriate. The need for a transparent, pervasive, and effective QA program cannot be understated.

The QAM serves as the focal point for the organization's QA activities, providing coordination with the DOE to ensure quality-affecting activities are conducted according to DOE policies, guidance and objectives, and in compliance with standards and regulations. The QAM is responsible for identifying overall QA requirements and confirming the satisfactory operation of the QA program through audits and surveillances; however, the workforce itself is responsible for the design and implementation of QA processes to enable implementation of the QA program.

To achieve enterprise-wide quality objectives, it is important that non-quality-affecting activities (e.g., business processes) facilitate and are integrated with QA's interests. The converse of this is also true.

4.1.3 Public Engagement and Consent-Based Siting

Public engagement planning is necessary to define, design and implement processes for public engagement in organization activities. Public engagement is not just for public information dissemination; rather it needs to be directed toward active public involvement throughout the effort. Public engagement activities present opportunities to inform potential stakeholders and engage them intellectually in the operations of the enterprise so that they have the opportunity to become an advocate with direct involvement.

Consent-Based Siting is included in this organizational element. These activities include those necessary to define, design, and implement processes to enable a phased, adaptive, and consent-based approach to siting waste management facilities. Consent-based siting is expected to focus siting considerations based on the interests of communities, gain trust among stakeholders, and adapt operations based on lessons learned, consistent with national goals.

The lead for this element is responsible for coordination of consent-based siting activities among the different organizational elements, and with the DOE. They will provide RDO and DOE Management with technical and integration recommendations regarding consent-based siting. These activities will include interactions with DOE to formulate direction, mitigate complex issues involving internal and external organizations, present effort-related material in upper management forums, approve technical and non-technical products and documents, and allocate resources to the performance of regularly scheduled work and rapid response tasks associated with consent-based siting.

On December 23, 2015, the DOE issued an Invitation for Public Comment to Inform the Design of a Consent-Based Siting Process for Nuclear Waste Storage and Disposal Facilities in the Federal Register (80 FR 79872), thereby initiating the development of its consent-based siting process. Public meetings were held across the country to hear from the public and interested stakeholders on what matters to them as DOE moves forward in developing a consent-based process to be documented in a draft report late in 2016. The content of the resultant report and the subsequently developed definition of a consent-based process will have great effect subsequent activities.

4.1.4 Regulatory/Licensing

This element is responsible for the activities necessary to manage the regulatory support activities conducted by the organization, regardless of the regulator's identity (e.g., NRC, EPA, or state entities). Regulatory activities will include interactions with DOE to formulate direction, mitigate complex issues involving internal and external organizations, present work-related material in upper management forums, approve technical and non-technical products and documents, and allocate resources to the performance of regularly scheduled work and rapid response tasks associated with regulatory matters. The strategic response development for regulatory issues as well as the planning for and preparation of witnesses during the licensing hearing is managed from this element. Working with RDO Management, this element ensures consistency and coordination among other organizational elements for producing regulatory materials and during regulatory proceedings.

The regulatory/licensing element will be responsible for meeting requirements in two broad regulatory regimes: NEPA, and NRC licensing. NEPA will require attention first with NRC licensing following during site characterization (Figure 3). These regimes are inter-related as an EIS must be submitted with a license application to NRC.

4.1.4.1 NEPA Compliance

This element is responsible for the activities necessary to manage the RDO's compliance with NEPA. DOE is subject to the Council on Environmental Quality (CEQ) regulations that implement NEPA and to its own implementing regulations (10 CFR Part 1021). Under 10 CFR Part 1021, it is expected that selection of a final site for a repository for DOE-managed waste requires preparation of an EIS, developed during detailed site characterization. Appendix D to Subpart D of 10 CFR Part 1021, which discusses classes of actions that normally require preparation of an EIS, specifically identifies "Siting, construction, operation, and decommissioning of major treatment, storage, and disposal facilities for high-level waste and SNF, including geologic repositories…" among such actions. Preparation of the EIS would begin at the time candidate sites are selected for detailed characterization, and the EIS would include as alternatives, other sites that were considered before the final choice of a site for licensing and development. A Final Environmental Impact Statement (FEIS) is submitted in conjunction with the NRC license application.

DOE could decide that an agency action of this magnitude requires a Programmatic EIS (PEIS), as well as the required site specific EIS, and related supplements, if necessary. A PEIS is a broad-scope EIS that identifies and assesses the environmental impacts of a DOE program and identifies and assesses the individual and cumulative impacts of ongoing and reasonably foreseeable future actions at a DOE site or program, (10 CFR Part 1021). Recent guidance from the CEQ encourages use of programmatic NEPA reviews and may be advantageous in the context of the flexible, phased, and consent-based process being applied to this effort. "Effective programmatic NEPA [processes] should present document reviewers with the agency's anticipated timing and sequence of decisions, which decisions are supported by the programmatic NEPA document and which decisions are deferred for some later time, and the time-frame or triggers for a tiered NEPA review" (CEQ 2014).

While not explicitly required by DOE's implementing regulations (10 CFR 1021.312), it is assumed here that EAs will be prepared for sites that passed the initial qualifying screening and are considered as serious candidates for characterization. This will serve to evaluate the impacts of proposed site characterization activities and begin the analyses used in the EIS to provide a consistent basis for comparison of the initial candidates to support selection of those to be characterized in depth.

4.1.4.2 Licensing Strategy

The effort is expected to be subject to NRC licensing under 10 CFR 60. The regulatory organizational element will be actively engaged in tracking and understanding NRC's anticipated rulemaking process to align 10 CFR 60 with the risk-informed, performance-based approach in 10 CFR Part 63, which will also involve EPA, to ensure the organization's ability to comply. In issuing 10 CFR Part 63, NRC acknowledged that its new more risk-informed, performance-based approach provides a better regulatory framework for geologic disposal of HLW and SNF than the earlier approach in 10 CFR Part 60. NRC stated that the "generic Part 60 requirements will need updating if applied to sites other than Yucca Mountain" (66 FR 55732). The NRC has not yet begun rulemaking to effect this update (Rubenstone 2012). The licensing element will formulate licensing and compliance strategies based on the outcome of this rulemaking, developing strategic responses for regulatory issues, and planning and preparing for license application development and submittal and license defense activities.

4.1.4.3 Regulatory Integration and Interactions

This element will be responsible for the two typical functions in the regulatory area: regulatory integration; and regulatory interactions. While the functions apply to both the NEPA and NRC regimes interactions are most prominent in the latter. Regulatory integration entails coordination of regulatory activities among the enterprise's various organizational elements (e.g., systems engineering, transportation and storage) and with the DOE regulatory affairs. Both RDO Management and DOE will receive technical and integration recommendations regarding regulatory matters from this source. Regulatory interactions provide the interface with and support DOE regulatory affairs, in interactions with regulators and responses to regulatory requests. The Regulatory Interactions lead is also responsible for supporting DOE regulatory affairs, meetings with NRC, the regulator's onsite representative, and the associated inspection program as it relates to the organization's scope of work. Regulatory interactions are most likely to begin during the Site Characterization phase.

4.1.4.4 Regulatory Document Configuration Management

This element addresses development and implementation of the organization's regulatory document configuration management process. Its purpose is to facilitate and maintain rigorous configuration management for formal regulatory document submittals. This is a special case of document development and control. Official documents produced by the organization should be managed and produced via the document development element. For regulatory documents (e.g., EAs, EISs, license applications, etc.) meticulous attention must be paid to their composition and configuration. In effect, such documents generally represent precise documentation of the satisfaction of requirements, and often contain the explication of significant numbers of commitments. As an example of how seriously one regulator considers the contents of a licensee's responses, NRC requires information provided to the Commission to be "complete and accurate in all material respects" (10 CFR 60.10). Violating this prescription may be the basis for adverse regulatory enforcement actions.

4.2 Operations Management

Operations Management is the organizational element responsible for the direction, coordination, and oversight of the Business Management, Organizational Assurance, Information Management, and IT Systems elements. Reporting directly to the RDO Manager, Operations Management is responsible for the day-to-day functionality of the principal support organizations.

4.2.1 Business Management

Business Management includes the activities that enable a workforce to accomplish its objectives using established work processes, and business management systems. The work force and financial controls are supplied via prescribed business management processes. It is most likely that the business management practices and systems for the enterprise will be DOE's or a DOE Contractor's and therefore well established.

Nonetheless, certain aspects of enterprise requirements will influence customary practices. For example, addition of Employee Concerns Program (ECP) elements to customary Human Resources (HR) processes is an obvious complication. Also, Training program requirements and documentation, as well as, procurement processes will need to conform to the QA program, which may result in the development of separate processes or system interfaces with existing parent organization programs. Given that existing practices in a diverse parent organization may be firmly established and resistant to change, such changes to conform to external requirements can be complicated.

4.2.1.1 Staffing (HR)

Handling the on-boarding and off-boarding of personnel to and from the enterprise is essential to its existence, functionality, and changing emphasis over the term of the effort. At least a thousand (maybe two thousand depending on the scope) persons will be needed to execute an effort of this magnitude, based on Yucca Mountain (YM) experience. Many HR protocols are straightforwardly transferrable from a parent organization (e.g., Equal Opportunity Employment, drug-free workplace, etc.) However, as indicated in Section 4.2.1, existing processes for HR business practices may be influenced by enterprise specific requirements. An important consideration for HR processes and systems is that much of the information gathered and used by this function may contain Personally Identifiable Information (PII) that requires rigorous protection. Also, there should be an effective interface between HR and Knowledge Management so that there are records maintained documenting individuals engaged in the effort, their background and expertise, and the areas in which they were involved. This information could prove essential in restoring the organization after unanticipated interruptions.

4.2.1.2 Employee Concerns Program

ECP is tied closely to the SCWE program and the broader concept of an NSC, because it provides the means by which Members of the Workforce (MOW) can express a concern without fear of retaliation. Well implemented SCWE, ECP, and a persistent NSC are essential for NRC's acceptance of the licensee's activities. The ECP will also need to conform to DOE's directive on employee concerns programs in DOE Order 442.1A *Employee Concerns Program*. Information maintained by the ECP also requires rigorous protection as it will contain particularly sensitive information related to individuals and their perceptions, perhaps about other individuals. Confidentiality breaches would endanger the strict compact between the individual and the ECP, potentially endangering the program's effectiveness.

ECP should also manage the process for addressing Differing Professional Opinions (DPOs) since it requires a similar level of confidentiality as that of ECP matters. These processes need to be consistent with DOE Order 442.2, *Differing Professional Opinions for Technical Issues Involving Environmental, Safety, and Health Technical Concerns*, and to the extent practicable with observations and guidance in NUREG-1763 (NRC 2002) and NRC's 2014 *Differing Professional Opinions Program Assessment* (NRC 2014).

4.2.1.3 Financials/Funding

This function provides for annual budgeting, including cost estimating, and fund management, as well as, receiving and verifying the Approved Funding Program to meet government requirements. This element will be responsible for the substantial task of compliance with the broad range of Federal/DOE financial/funding rules.

4.2.1.4 Procurement

The need to acquire material or services is obviously critical in the execution of an effort of this scale and scope. These functions are necessary to ensure that procurements are conducted in accordance with the applicable Federal and agency specific rules. There is also a very direct connection between QA and procurement when it comes to acquiring quality-affecting items or services (NQA-1 Requirement 4, Procurement Document Control). An initial review of a procurement must include a determination of whether it involves quality-affecting items or services. Contracts for services affecting quality must include appropriate QA provisions. Early establishment of a qualified suppliers list will avoid much effort later on.

A substantial effort may be required to integrate enterprise QA requirements with an existing conventional procurement process. It will likely be necessary to dedicate a number of personnel to ensure that procurements made are compliant with enterprise QA requirements. Quotation of selected requirements from NQA-1 Requirement 4, Procurement Document Control are provided below to illustrate the point.

- "Section 202 Technical Requirements - Technical requirements shall be specified in the procurement documents. These requirements shall be specified, as appropriate by reference to specific drawings, specifications, codes, standards, regulations, procedures, or instructions, including revisions thereto that describe the items or services to be furnished. The procurement documents shall identify appropriate test, inspection, and acceptance criteria for determining acceptability of the item or service.
- Section 203 Quality Assurance Program Requirements - Quality assurance program requirements shall be specified in the procurement documents. These requirements shall be consistent with importance and/or complexity of the item or service being procured. The procurement documents shall require the Supplier to incorporate appropriate quality assurance program requirements in sub-tier procurement documents.
- 300 Procurement Document Review - A review of the procurement documents and changes thereto, shall be made and documented prior to award to ensure that documents transmitted to

prospective Supplier(s) include appropriate provisions to ensure that items or services will meet the specified requirements. Technical or quality assurance program changes made as a result of bid evaluations or negotiations shall be incorporated into the procurement documents prior to their issuance to the Supplier. Procurement document review shall be performed by personnel who have access to pertinent information and who have an adequate understanding of the requirements and intent of the procurement documents.

- 400 Procurement Document Changes - Procurement document changes affecting the technical or quality assurance program requirements shall be subject to the same degree of control as utilized in the preparation of the original documents. Regardless of the nature of the venture, acquisition of property will be necessary to achieve its objectives. The functions of the Facilities element are directed at all the post-purchase (or rental) management needs required to account for the various property."

4.2.1.5 Project Controls

This function establishes a work breakdown structure, which provides the structure for planning, managing, controlling, and monitoring the cost, schedule and performance of the effort consistent with DOE Order 4.13-3B. Typically, this function is also responsible for establishing and certifying an Earned Value Management System (EVMS) for the effort consistent with DOE Guide 413.3-10A.

4.2.1.6 Training

The training function is integrally tied to the enterprise's operations and Quality Assurance (NQA-1 Requirement 2, Quality Assurance Program; Section 200 Indoctrination and Training). MOW must be trained to perform certain functions as a high-quality, regulation-aware business and technical team. Such training applies to both the technical organization that will be performing 'quality affecting' work as well as the support organizational elements. The latter's understanding and awareness of QA requirements can be critical to their ability to provide effective support to the technical organization. Some elements of the support organization will need extensive QA training and detailed familiarity with the QA program to perform their roles.

Providing or arranging for the necessary training from either internal or external sources, and maintaining the related records is key to demonstrating that MOW are qualified to perform specific work. Some of the information gathered and used by this function may be considered PII. Scrupulous maintenance of training records is crucial to satisfying QA requirements as well as providing a positive influence on NRC's perspective of the licensee's activities. Existing processes for training practices may be influenced by enterprise-specific requirements such that separate systems may be necessary for enterprise related training.

4.2.1.7 Facilities and Safeguards & Security

This function will be responsible for managing the facilities eventually needed to accomplish the mission. Such facilities could be in a number of locations including potential site locations. It is likely that the number of facilities and their locations will increase as the effort progresses. This element would also be responsible for the safeguards and physical security at these locations consistent with DOE Orders 473.3A *Protection Program Operations* and 470.4B *Safeguards and Security Program*.

Note that DOE Order 470.4B Section 3(c)(2) Exemption, states

> "Requirements in this Order that overlap or duplicate requirements of the Nuclear Regulatory Commission (NRC) related to radiation protection, nuclear safety (including quality assurance), and safeguards and security of nuclear material, do not apply to the design, construction, operation, and decommissioning of the facilities of the former Office of Civilian Radioactive Waste Management (RW) now managed by the Office of Nuclear Energy. This exemption does not apply to requirements for which the NRC defers to DOE or does not exercise regulatory jurisdiction."

This statement is specific to the previously considered repository at Yucca Mountain, but is anticipated to be applicable to any DOE repository licensed by the NRC. This is also consistent with a similar policy statement in DOE Order 435.1.

4.2.1.8 Environment, Safety & Health

This organizational element will be responsible for managing the efforts to ensure compliance with DOE environmental health and safety provisions. Overall, this work is encompassed by DOE Policy 450.4A, *Integrated Safety Management Policy*; DOE Order 450.2, *Integrated Safety Management*; DOE Guide 450.4-1C, *Integrated Safety Management System Guide*; and 10 CFR Part 851 *Worker Safety and Health Program*. The ultimate objective is to ensure that DOE will continue to have “zero tolerance” for accidents that result in life-threatening injuries or major environmental contamination.

4.2.2 Organization Assurance

Organizational Assurance includes the activities necessary to oversee the organization’s operational and functional fidelity to ensure integration and appropriate conduct of operations, including the concepts and processes listed below. Organizational Assurance has a significant role in the organization. It serves to support a multitude of functions that enable the effort to assert and document that it is a functional quality organization with a persistent Nuclear Safety Culture.

4.2.2.1 Nuclear Safety Culture (NSC)

This aspect of the Organizational Assurance function enables the development and implementation of the organization’s NSC philosophy by:

- Promoting a NSC (Table 1) within the organization similar to that of other high performing nuclear organizations consistent with the expectations of NRC (76 FR 34773; June 14, 2011).
- Developing and guiding implementation of the plan for ensuring and independently verifying that the NSC permeates all organizational elements and monitoring how well the organization exhibits the requisite NSC.

Conformance to NRC’s safety culture policy statement (76 FR 34773) will be necessary for a successful licensing program. The Commission defines Nuclear Safety Culture as the core values and behaviors resulting from a collective commitment by leaders and individuals to emphasize safety over competing goals to ensure protection of people and the environment. Table 1 summarizes NRC’s perspective on the characteristics of a positive Nuclear Safety Culture.

RDO Management will periodically direct Organizational Assurance to survey the workforce to assess the state of the NSC across the enterprise.

Table 3 — Traits of a Positive Nuclear Safety Culture

Traits of a Positive Nuclear Safety Culture	
Leadership Safety Values and Actions	Leaders demonstrate a commitment to safety in their decisions and behaviors.
Problem Identification and Resolution	Issues potentially impacting safety are promptly identified, fully evaluated, and promptly addressed and corrected commensurate with their significance.
Personal Accountability	All individuals take personal responsibility for safety.
Work Processes	The process of planning and controlling work activities is implemented so that safety is maintained.
Continuous Learning	Opportunities to learn about ways to ensure safety are sought out and implemented.
Environment for Raising Concerns	A safety conscious work environment is maintained where personnel feel free to raise safety concerns without fear of retaliation, intimidation, harassment, or discrimination.
Effective Safety Communication	Communications maintain a focus on safety.
Respectful Work Environment	Trust and respect permeate the organization.
Questioning Attitude	Individuals avoid complacency and continuously challenge existing conditions and activities in order to identify discrepancies that might result in error or inappropriate action.

4.2.2.2 Safety Conscious Work Environment

SCWE (NRC 2004b, 2005) is the aspect of Organizational Assurance responsible for development, implementation, and assessing the organization's work environment where:

- Employees are encouraged to raise safety concerns
- Concerns are promptly reviewed,
- Concerns are given the proper priority based on their potential safety significance, and
- Concerns are appropriately resolved with timely feedback to the originator of the concerns and to other employees, as appropriate

NRC licensees and contractors are expected, although not required by regulation, to establish and maintain a SCWE, which is defined by the NRC as an environment in which "employees feel free to raise safety concerns, both to their management and to the NRC, without fear of retaliation" (76 FR 34773; June 14, 2011). The NRC states in its 2005 Guidance for Establishing and Maintaining a Safety Conscious Work Environment (NRC 2004b, 2005)

> "Licensees bear the primary responsibility for the safe use of nuclear materials in their various licensed activities. To carry out that responsibility, licensees need to receive prompt notification of concerns as effective problem identification and resolution processes are essential to ensuring safety. Thus, the Commission expects that each licensee will establish a safety-conscious environment where employees are encouraged to raise concerns and where such concerns are promptly reviewed, given

> the proper priority based on their potential safety significance, and appropriately resolved with timely feedback to employees.
>
> A safety-conscious environment is reinforced by a management attitude that promotes employee confidence in raising and resolving concerns. Other attributes of a work place with this type of an environment may include well-developed systems or approaches for prioritizing problems and directing resources accordingly; effective communications among various departments or elements of the licensee's organization for openly sharing information and analyzing the root causes of identified problems; and employees and managers with an open and questioning attitude, a focus on safety, and a positive orientation toward admitting and correcting personnel errors."

Consistent with best practices among NRC licensees, the DOE will establish an effective ECP, Corrective Action Program (CAP) and undertake other activities, including training and self-assessments to ensure an effective SCWE throughout the effort, including operations of DOE contractors.

4.2.2.3 Corrective Action Program

The CAP function develops and implements the organization's corrective action program and system consistent with current regulatory guidance. Specific areas of review for a licensee's CAP are:

- Policies, programs, and procedures
- Identification, reporting, and documentation of safety and security issues
- Significance classification and causal evaluation of safety and security issues
- Development and implementation of corrective actions
- Assessment of corrective action and program effectiveness

The CAP process is a pivotal element of overall operations, and should be an integral part of enterprise management and effective organizational assurance. It is the vehicle by which the effort demonstrates that problems are being recognized, reported, evaluated for their consequences and extent of condition, and managed to a responsible resolution with a documented conclusion. The CAP system should be robust, easy to use, and oriented toward complete electronic documentation and trending.

The nuclear power industry has vast experience with CAP programs and the program used on the previously considered YM repository project was adopted from power plant operations. It was not a seamless fit for a project mostly concerned with engineering design and materials and geoscience research (i.e., not nuclear plant operations). NEI recognized similar differences in the context of new reactor construction and has offered a modified view of CAP processes in *Corrective Action Processes for New Nuclear Power Plants During Construction* (NEI 2015). Careful consideration should be given to the differences between nuclear plant operations and repository development processes in the development of a CAP system for the RDO, including DOE Guide 414.1-5 *Corrective Action Program Guide*.

4.2.2.4 Requirements Management

Requirements Management develops and implements the organization's requirements management effort and process consistent with current agency guidance and consistent with DOE Order 413.3B, *Program and Project Management for the Acquisition of Capital Assets* and other applicable DOE Orders. Note that DOE Order 435.1 *Radioactive Waste Management* explains at (d)(3) that "Requirements in this Order that duplicate or conflict with requirements of NRC or an Agreement State do not apply to facilities and activities licensed by the NRC or an Agreement State." Requirements Management provides a means to identify record, allocate, implement and track the organization's internal and external requirements independent of their source. The scale of this task will require a sophisticated software tool(s) to be efficient. Care should be taken not to undersize the selected software platform. Initially the software platform will seem oversized for the task, but one must keep in mind that its contents will necessarily grow, and the software platform is likely to be in use over a long term (decades). One of the first tasks for this element will be to identify and allocate responsibility for statutory, DOE, NRC, EPA, and NEPA requirements that apply to the effort.

4.2.2.5 Commitment Management

This function is responsible for the development and implementation of a commitment management process to facilitate the tracking and resolution of the organization's commitments, whether they originate in enterprise policies, administrative directives, or technical or regulatory instruction. It provides a means to record and track resolution of items identified by management. A component of the process could track corrective actions. While this may seem redundant with Requirements Management, it is closely related, but distinctly different. Requirements originate from sources that have established authority over the effort (e.g., the parent DOE organization, NRC, EPA, NEPA, and general statutory or legislative sources). Commitments arise from within the RDO itself (e.g., a commitment to resolve a particular problem in a specified fashion), or between the RDO and an external body (e.g., a commitment to resolve a regulatory issue with NRC, or provide certain information to an oversight or public body). The ability to keep track and manage the resolution of commitments is essential to maintaining a credible and respected reputation.

4.2.2.6 Self-Assessment

The Self-Assessment function is to develop and implement the organization's process to regularly perform self-assessments consistent with enterprise requirements and other Quality Assurance and regulatory requirements. Also, self-assessment is a key element of DOE Order 450.2 *Integrated Safety Management*, DOE Order 442.1A *Employee Concerns Program*, and DOE Order 414.1D *Quality Assurance*, among others. Self-Assessments are integral to most Organizational Assurance functions, as it provides the means by which the effort evaluates and documents its conformance with authoritative direction. Effective self-assessments should be directed at discrete issues as often as possible (e.g., is the organization following document development/control processes?). Far-reaching assessments should be avoided initially, as they require an organizational maturity that will take time to develop.

4.2.2.7 Risk Management

Risk Management develops and implements the organization's general risk evaluation and management processes, consistent with enterprise requirements. It provides a means to identify, record, allocate, implement and track the organization's risks. Effective risk management also requires a moderately advanced level of enterprise maturity. Risk Management is an important aspect of DOE Order 413.3B, *Program and Project Management for the Acquisition of Capital Assets*. Initially the number, magnitude and seeming inability to mitigate identified risks will appear overwhelming. Nonetheless, it is important to identify and track risks to remain cognizant of them and recognized them as part of the enterprise planning basis, even if the means to mitigate risks may not be apparent at a particular time.

4.2.2.8 Knowledge Management

The Knowledge Management function is responsible for development and implementation of the organization's effort directed at compiling, organizing, leveraging, and preserving the organization's knowledge base(s) to support organizational goals and anticipated future needs. It includes a diverse range of efforts to identify, analyze, optimize, and apply information that the organization deems important. In the context of repository systems, it spans matters ranging from the purely technical, well understood (certain) physical/chemical characteristics (waste packages materials, waste forms, corrosion, and waste locations); to less well understood (uncertain) characteristics, (natural fluid flow, volcanism, other low probability events); to very poorly definable characteristics, (cultural influences, societal characteristics).

Knowledge Management functions are often categorized into two broad areas; applied knowledge management and knowledge preservation. The purpose of applied knowledge management is to design processes to ensure the promulgation of current information or impending changes to the workforce. Such processes are useful operational tools, and are largely directed at information necessary to maintain or improve current business practices and models. Knowledge management techniques would be useful for maintaining the continuity of procedural processes (technical culture) over the decades of repository development and operations.

An example of this aspect of knowledge management would be establishing an on-line location for keeping the workforce informed about changes in enterprise operations. These changes are often handled in an ad hoc manner, when the effort to effectively convey changes deserves more formal treatment. Changes to policy, processes, or procedural approaches should be immediately communicated to the workforce, to maintain their cognizance of the current operational basis for the enterprise. Technical innovations or introduction of new standards or requirements can also be efficiently announced in this fashion.

Another example is a formally maintained continuously current history/timeline supported by relevant documentation. This would prove invaluable in, for example, year 25 in understanding the basis for a decision made in year 2. The risk is certain that the effort duration will extend beyond most of the workforce's memory.

The second area, knowledge preservation, consists of efforts to safeguard our understanding of important issues for continuing long-term safety of the repository system by avoiding the loss of institutional and societal knowledge long after repository closure. This includes establishing a long-term historical record of the participant's and enterprise developments. As mentioned above, preservation of the historical record will be important, considering that the effort's objectives will span 2 to 3 workforce generations.

Knowledge preservation envelops both classic subdivisions of knowledge; explicit knowledge, and tacit knowledge. Explicit knowledge is information that is readily codified into a tangible form, i.e., documentary material (reports, analyses, memos, videos, email, databases, etc.) that may be retained in a wide variety of media (paper, film, electronic, etc.). This may be broader than the typical Records Management approach, especially in terms of the retention period. Development of a repository is overwhelmingly driven by regulatory (technical/engineering) considerations. So, recording and preserving the explicit recorded knowledge required to convince a regulator to allow repository operation secures a core set of information requiring preservation. However, regulatory submittals likely constitute less than one percent of the recorded information necessary to produce it. Also, the underlying information may not require long-term retention under Records Management rules.

Tacit knowledge is knowledge that we as individuals possess, but is not readily codified. Skills like playing musical instruments, woodworking and welding are examples, as are inherent personal abilities like writing and mental arithmetic. Tacit knowledge is much more difficult to codify. However, this knowledge class does include information that is not clearly explicit, but can be codified to a certain extent. Examples are technical, societal, or cultural processes that pertain to substantial organized efforts (large engineering projects). This knowledge can be captured by interviewing participants, including the public, and transcribing or recording the conversations (e.g., recording conversations with key leaders and recognized experts).

The current concept of knowledge management was not practiced on projects for previously proposed repository site(s). It is currently recognized internationally as a practice that should be undertaken for nuclear waste repositories, (Zheng, Yang, and Mclean 2010; Romhardt 2014; Umeki, Takase, Hioki, and McKinley 2009).

4.2.3 Information Management

Information Management includes activities that enable a workforce to accomplish its objectives using enterprise-wide information processes and IT systems. Information Management designs and oversees the processes that generate, transmit, and store information. Information Management, with the assistance of IT systems, operates and maintains the information in electronic systems required to process, store and access enterprise information in the principal areas listed below. Information Management has been separated from its customary association within Business Management to avoid dilution of this functional element because of its importance to the successful outcome of a compliance oriented effort.

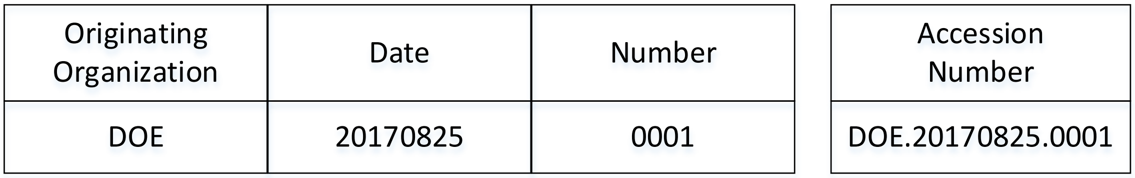
Information managed via this element is the organizational, technical, regulatory, and quality assurance related documentation and information (documentary evidence) necessary to document accomplishment of enterprise objectives and confirm the integrity of the organization's work products. Throughout the effort's timeline (Figure 3), at least until issuance of a construction authorization, and probably significantly thereafter, the most important products will consist of recorded information demonstrating compliance with various enterprise and regulatory requirements. The importance of a robust, integrated, and accessible information management function cannot be understated.

4.2.3.1 Records Management

Records Management is the unique process for capturing information related to the effort, independent of its origin or form. The records management program will need to conform to DOE Order 243.1B *Records Management Program*, including development of records retention and disposition schedules approved by National Archives and Records Administration (NARA) (DOE O 243.1B (4)(a)(2)). As stated in DOE O 243.1B, the effort will need to maintain electronic records in accordance with 36 CFR Subchapter B, *Records Management*, by "building electronic records keeping functionality into the native electronic information systems or by capturing the electronic information systems records in an electronic records management application" (DOE O 243.1B (4)(b)). The use of records management systems that meet the functional requirements of the Department of Defense (DoD) standard 5015.2-STD, *Electronic Records Management Software Application Design Criteria Standard*, satisfies this requirement.

One very essential component of a records management process is an accession number (i.e., unique identifier for a single record). It is applied to records management information and its use should be required in other information systems. For example, a separate identifier should not be affixed in Correspondence Control or Document Control. Rather information processes and systems should exclusively use the unique accession number for identification. The benefit of such an approach should be apparent, in that it provides a single key identifier (field) for reference to any type of record (report, letter, data package, software item, physical specimen, etc.). Conceptually, information systems consist largely of metadata, and refer to the underlying record information by the records management accession number. This mirrors the approach taken by NRC in its Agency Wide Documents Access and Management System (ADAMS). Previous experience has provided a useful example of a suggested format for a records management accession number shown in Figure 9.

To the extent practicable documents should be entered in the records management system in the form specified by NRC for submittals to the agency. This will facilitate eventual transmittal of materials to NRC and should also satisfy NARA requirements. Consultation with NRC is critical as submittal requirements for ADAMS may differ from those applicable to an electronic hearing docket.



Originating Organization	Date	Number	Accession Number
DOE	20170825	0001	DOE.20170825.0001

Figure 9 — Suggested Format for an Accession Number

4.2.3.2 Email Considerations

The importance of proper management and attention to maintenance of email processes/systems cannot be overstressed. The 2012 OMB/NARA *Managing Government Records Directive (M-12-18)* (NARA 2016) includes a requirement that:

> "by December 31, 2016 Federal agencies must manage all email records in an electronic format and can no longer use print and file policies to manage email records. Accordingly, email records must be retained in an appropriate electronic system that supports records management and other agency business needs. In order to successfully meet the Directive's 2016 requirement of managing email electronically, each agency must have in place applicable records schedules, agency policies, and IT systems to ensure that emails that are Federal Records can be accessed, managed, and preserved until the appropriate disposition is applied."

Management of email can be facilitated by using a single email client for work related electronic communications. For example, Licensing Support Network (LSN) (Section 4.2.3.9) considerations can be efficiently met by use of a single email client by enterprise participants.

The indoctrination and training of MOW must stress that use of the email system forfeits any right to privacy and that emails are records even though the retention period will vary according to the content. The workforce should avoid using the email system for personal purposes and should avoid using personal email to conduct enterprise business. This should be much easier than in the past, as most users will be able to access a web-based version of their private email client from work; however, MOW will need to be cautioned that work related information exchange must take place on the enterprise email system. It should also be stressed that workforce document collaboration systems are to be used to avoid transmittal of large volumes of potentially LSN relevant email attachments via the email system.

4.2.3.3 Correspondence Control

Correspondence Control is an element of records management providing for centralized receipt and transmittal of official enterprise correspondence including its distribution. Effective implementation of this function is important to the successful operation of the enterprise's administrative processes. Correspondence Control is often dismissed as just another part of Records Management. While it is an integral part of Records Management; it is important enough to deserve identification as a separate function. As an example, proper control of correspondence from the government oversight bodies, the licensee (applicant), the regulator, and the public is essential to maintaining a rigorous record of written commentary or direction influential to the enterprise's direction. Many correspondence items will ultimately be traceable to requirements or commitment management items.

4.2.3.4 Document Development

Documents developed for the effort should have the same 'look and feel' and the most efficient way to accomplish this is to have a limited number of organizational elements responsible for final production of enterprise documents. This also ensures that enterprise documents are expeditiously entered into the records management system and document control (if appropriate). Document Development should also have responsibility for the process that defines responsibilities for preparing, reviewing, approving, revising, and changing, technical reports and procedures for enterprise-wide activities, including science and engineering. The function should also be responsible for ensuring enterprise documents are finalized in the electronic form specified by Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794(d)) and by NRC for electronic submittals to the agency (NRC 2011). This may seem a trivial detail, however, unless instituted early, the conversions to ensure compliance at a later stage will consume significant resources.

4.2.3.5 Reference Registry

Thousands of references will be cited in documentation produced during the effort, consisting of both public and copyrighted information in addition to the enterprise's own documentation. Reference registry processes and systems for documenting (and retaining copies) of references is critical to ensuring the integrity and defensibility of enterprise documents. Careful attention should be given to defining the metadata requirements for cited references. The reference registry process needs to be integral to the document development process. To enable this, document reference citations must include a link (internal to enterprise systems) to the reference in the reference registry. Based on previous experience, it should not be acceptable to cite entire documents unless that is really intended, for example, when referring to a broad concept. Specific page citations should represent the norm.

The reference registry is a particular case where exclusive use of the unique accession number for identification provides a distinct advantage. The benefit is that the accession number provides a single reference to any type of record (report, letter, data package, software item, physical specimen, external publication, etc.). Any of these types of records may be referenced in an enterprise report. Document release must be constrained by having secured the appropriate copyright release or agreement, if appropriate. This may also seem a less-than-important detail; however, the RDO should take the necessary precautions to avoid litigation as an unauthorized distributor of copyright material.

4.2.3.6 Document Control

Document Control is an element of records management providing for the necessary control of certain documents essential to conduct of operations. Document Control is the means of ensuring the availability and use of the current authoritative version of information, whether it is a report, policy, plan, procedure, list, drawing, image, etc.

Most activities will be governed by established policies, plans, or procedures. MOW will need to know where to find the authoritative version of these protocols. One role of document control is to maintain the process by which such documents are controlled and to make the list readily available to the workforce (on the enterprise network). The controlled document list will become extensive. As an example, the listing for a previously considered repository project included about 9500 controlled documents (many with multiple versions) consisting of about 30 document types ranging from individual calculations, to extensive reports, procedures, and interface definition documents, to highlight a subset.

Document control also has a crucial important interface with QA (NQA-1 2015, Requirement 6, Document Control), since the conduct of the QA program needs to conform to the current revision of procedures that are usually only identifiable via the controlled document system. Changes to controlled documents can sometimes lead to onerous processes unnecessarily absorbing effort unnecessarily, and Document Control processes must be designed to avoid this. NQA-1 addresses this in Requirement 6, Document Control, part 300 Document Changes, and judicious use of the provisions in paragraph 302 can prove advantageous:

- "301 Major Changes - Changes to documents, other than those defined as minor changes, are considered major changes and shall be reviewed and approved by the same organizations that performed the original review and approval unless other organizations are specifically designated. The reviewing organization shall have access to pertinent background data or information upon which to base their approval.
- 302 Minor Changes - Minor changes to documents, such as inconsequential editorial corrections, shall not require that the revised documents receive the same review and approval as the original documents. To avoid a possible omission of a required review, the type of minor changes that do not require such a review and approval and the persons who can authorize such a decision shall be clearly delineated."

4.2.3.7 Data Management

Data Management is also an element of records management, because data generated by the effort probably meets the definition of a federal record. Data management provides a process specifically designed to handle the special needs of data, which often involves large complicated electronic files, and requires assignment of important, and likely extensive metadata that will enable its identification, later discovery and potential use. Such data files are often crucial references that must also be accounted for in a process/system designed to track references included in enterprise documents. Management of these datasets can be similar to document control in that there will be a need to maintain traceability among various versions of a particular dataset, as well as, other datasets. Traceability is defined in NQA-1 as the ability to trace the history, application, or location of an item and like items or activities by means of recorded identification. Based on experience from a previously considered repository project information storage of data may require terabytes of electronic storage.

Managing data sets also reinforces the advantage of using a single accession number for each record. The investigator originates the set of data (the record) and has the discretion to name it and provide other metadata related to it. The set is assigned an accession number that can thereafter be uniquely and reliably referenced via the reference registry, document control system, or software configuration management. The data set is stored in the enterprise storage area network (SAN) where access and change authority can be restricted as appropriate.

4.2.3.8 Software Configuration Management

Software configuration management is an element of information management providing for the necessary control of software used in the conduct of operations. Software configuration management is the means of ensuring the availability and appropriate use of the current authoritative version of software, whether it is commercial off the shelf (COTS), or developed software.

MOW will need a single location to find the authoritative version of software. One role of software configuration management is to maintain the process by which software versions are controlled and make the list readily available to the authorized workforce, preferably online. The software configuration list will become extensive. As an example, the listing for a previously considered repository project included about 650 controlled QA software items (many with multiple versions).

Similar to document control, software configuration management (or control) has an important interface with QA, since the appropriate use of software is often based on the specific version employed. This is most efficiently accomplished by establishing a single software configuration control process and system. Software configuration management is addressed in NQA-1 Subpart 2.7, *Quality Assurance Requirements for Computer Software for Nuclear Facility Applications*, paragraph 203 of which states "Software configuration management includes, but is not limited to, configuration identification, change control, and configuration status control. Configuration items shall be maintained under configuration management until the software is retired." Each configuration item should have its own unique accession number for identification and reference purposes.

4.2.3.9 License Support Network

License Support Network (LSN) is an element of records management that consisting of processes and protocols designed to satisfy the procedural requirements of 10 CFR Part 2, Subpart J of NRC’s licensing rules (see also NRC 2004a). Nominally, the purpose of this rule is to facilitate the discovery process for an eventual NRC evidentiary proceeding. Substantively, LSN requires any documentary evidence that is ‘relevant’ to an applicant’s submittal, be provided for posting on the LSN within 90 days. The importance of LSN compliance unmistakable, as the applicant must certify it is in compliance with the rule at least six months before submittal of a license application.

Compliance with LSN requirements will by necessity be enterprise-wide. A certification approach will need to be designed, documented, implemented, and then assessed before the RDO official can provide a certification to NRC. MOW (DOE participants, contractors, etc.) will require training in LSN compliance. Documents (including email) will need to be marked with respect to relevancy (i.e., relation to the licensing proceeding).

The processes to ensure compliance with LSN requirements can be complicated, involving record material in many different forms, and — very importantly — it includes email. Additional challenges have arisen in the past decade such as how instant messaging, social media, and other innovations such as machine-translated voicemails will be addressed by LSN rules. Consultation with the DOE Office of General Counsel will be critical to resolving such matters.

In other programs the submittal of documents to the LSN first required submittal to the applicant’s litigation support contractor for review and classification before upload to the LSN. In combination with other procedural steps this effectively shortened the 90-day allowance for posting materials to the LSN to 14 days.

4.2.4 IT Systems

The IT Systems or Services include activities necessary to define, design, implement, and maintain IT systems to support the organization’s processes and functions. Systems that are developed to support the business and technical efforts are essentially important to the overall success of the enterprise and generally fall into two categories: a) information systems; and b) high performance computing systems. The purpose of information systems is to collect and store administrative and technical information and its associated metadata for day-to-day use and compliance with information related requirements. High performance computing systems provide the calculation capability or other data intensive systems to support science and engineering efforts.

IT Systems are the tools supporting the processes that are the responsibility of organizational elements other than IT. Their categorization corresponds closely to the general organizational element functions. However, this correspondence is not exact, because there are IT services necessary to create and maintain IT systems that are not necessarily uniquely related to the functions of other organizational elements. An example is the IT network. While the network is necessary to support most of the organization’s support element functions and processes, it is not uniquely related to one particular function or process. A number of the organization’s support element functions and processes may be supported by a single IT system. An example of this is the IT Configuration Management Systems, which support a number of functions and processes (e.g., records management, correspondence control, document control, data management, and software configuration management). Co-mingling of an organizational element’s processes with IT system is an inevitable outcome of deploying integrated IT systems. Otherwise, one could not avoid deployment of single-use stove-piped IT systems that are antithetical to efficient use of resources, and confounding to users and processes.

This section describes the IT Systems required to support the IT services required for the RDO. Criteria that should be used to evaluate potential solutions are identified and where feasible, examples of existing solutions that might be considered are provided. Because there are a broad range of possible solutions available, when possible, IT Systems solutions are presented for three IT environments: Cloud-based, On-Premises, Hybrid (mix of Cloud and On-Premises).

The RDO requires IT services to support the organization's mission. Many of those IT services are similar to those employed in most other business organizations. However, some of the services have requirements that are unique to an RDO, as indicated below. The following IT services/system categories are discussed:

- Day-to-Day IT Operations
- Assurance Systems (unique requirements)
- Business Systems
- Document Production and Management (unique requirements)
- Configuration Management (unique requirements)
- Data Production and Management (unique requirements)
- NRC License Support Network (unique requirements)
- Disaster Recovery
- Historical Systems (unique requirements)

While these services are necessary for the organization, there are dependencies among them. Some services such as Day-to-Day IT Operations are required before others can be implemented, because they provide infrastructure for other IT services. Another example is Business Systems which must be in place early in the life of an organization because it directly supports establishment of the organization.

The current IT world provides essentially three models for delivering IT services based on the type of environment: On-Premises; Cloud; and Hybrid (combination of On-Premises and Cloud).

The on-premises environment is a delivery model that is installed and operated from a customer's in-house server and computing infrastructure. It utilizes the organization's native (resident) computing resources. It is the most common and traditional model. While more expensive to set up and operate, an on-premises context is considered the most secure.

The cloud computing environment provides commodity services to customers. There are principally three major types of services which are referred to as the computing stack:

- IaaS – Infrastructure as a Service, providing hardware, network, and operating system(s)
- PaaS – Platform as a Service, providing a development platform(s)
- SaaS – Software as a Service, providing application(s)

There are three major vendors providing commercial cloud services: AWS (Amazon Web Services); Google; and Microsoft. Recognizing that government agencies have unique requirements, each vendor provides services specifically tailored for local, state, and federal governments. For example, Microsoft has a service called Azure for government. The major advantages of 'cloud services' are rapid provisioning, elastic scalability (rapidly accommodate expansion or reduction of services needed), and to lesser extent cost (pay for what is used). When an organization combines on-premises and cloud services to deliver an IT service, it is considered a 'Hybrid' solution. While not as common as either cloud or on-premises, hybrid solutions strive to utilize the best of both worlds (on-premises and cloud).

General criteria that should be applied when considering a vendor to provide an IT solution in most environments are:

- Sustainability (endurance over time)
- Maturity (software evolved over time, etc.)
- Due Diligence (financial viability, reputation, technical support, etc.)
- Flexibility
- Cyber Security

- Integration facilities
- Records retention

Criteria that should be considered specifically for cloud services are:

- Environment compliance (e.g., Federal Risk and Authorization Management Program (FedRamp), Health Insurance Portability and Accountability Act (HIPAA (Public Law 104 - 191) compliance)
- Disaster Recovery Options
- Security Plan (identity management, etc.)

On-Premises solutions should also include the following criteria:

- Ability to separate content for the RDO
- Support different personnel security requirements (citizen vs. non-citizen)
- Content accessible from the internet
- Certification as a Federal Computing Site (e.g., FEDRAMP)
- Provide disaster recovery of data and IT systems
- Provide scalability

Hybrid solutions should consider both Cloud-based and On-premises criteria.

There are numerous IT solutions available using On-Premises, Cloud-based, or Hybrid environments to deliver many of the IT services listed herein. Since many of the IT services are common to most organizations, the choices are also similar. There are also some unique IT services for a RDO, such as:

- Document Production and Management – the RDO will have quality assurance requirements above normal standard practices including reference verifications and copyright registrations.
- Data Production and Management – the data files produced from modeling and simulations as well as the input parameters must be tracked and maintained as part of the organization’s records.
- Assurance Systems – unique systems requirements mandated by DOE orders and the NRC policy (e.g., DOE O 413.3B, Corrective Action System, and Nuclear Safety Culture).
- NRC Licensing Support Network (LSN) – This IT service supports the process outlined in Section 4.2.3.9 and includes mechanisms for the organization to collect, mark, and transmit ‘relevant’ documentary material, including emails, to an NRC-identified service that provides the content to a web application that is available to the public.
- Historical Systems – historical content from past or other ongoing programs.

In summary, there are enough solutions available to support a RDO, whether that solution is delivered via On-premises, Cloud-based, or a combination of both. This section is intended to provide a starting point to identify the IT systems required, criteria that might be employed in selecting the systems, and examples of the solutions for each of the delivery models presented. In some cases, there is no available software that can be delivered for either Cloud-based or On-Premises environments, in such cases, solutions can be developed for either on-premises or cloud services.

4.2.4.1 Concepts, Considerations, and Terms

Figure 10 illustrates a very conceptual IT architecture diagram including the major IT systems services required to support the RDO. The architecture generally consists of ten basic IT services that are designed to support the processes of the organization’s functional elements. The architecture needs to facilitate connection(s) between the RDO IT services and other internal and external architectures. For example, enterprise information (usually documents) will need to be submitted electronically to NRC’s ADAMS (external), as well as shared within various systems within RDO itself (internal). The architecture will also need to allow public access to certain parts of the RDO’s system to benefit from transparency and foster consent on the part of the interested public.

General IT systems considerations amount to the criteria that should be applied in selecting IT systems regardless of the environment (Cloud-based, On-Premises, Hybrid) in which the system will reside. In addition to these criteria, there are criteria specific to each environment for some IT services. These are identified where appropriate.

- Sustainable
  - Ability to endure over time – have been available for at least last 5 years
  - IT system recognized as a leading product in the industry
- Vendor Due Diligence
  - Financial Viability – demonstrated ability to continue operations to support the system and enhance it; in business more than 5 years. Evaluate through reviews of annual reports, etc.
  - U.S. Company – not foreign held or subsidiary.
  - Reputation in the industry – established leader in industry/software
  - Technical Support – provide support through blogs, call-in, chat, incident tracking, tiered services (24x7, professional services)
  - Training – provide on-site, online (video, etc.), third party.
  - User Groups – user population should be large enough to host user groups/ conferences

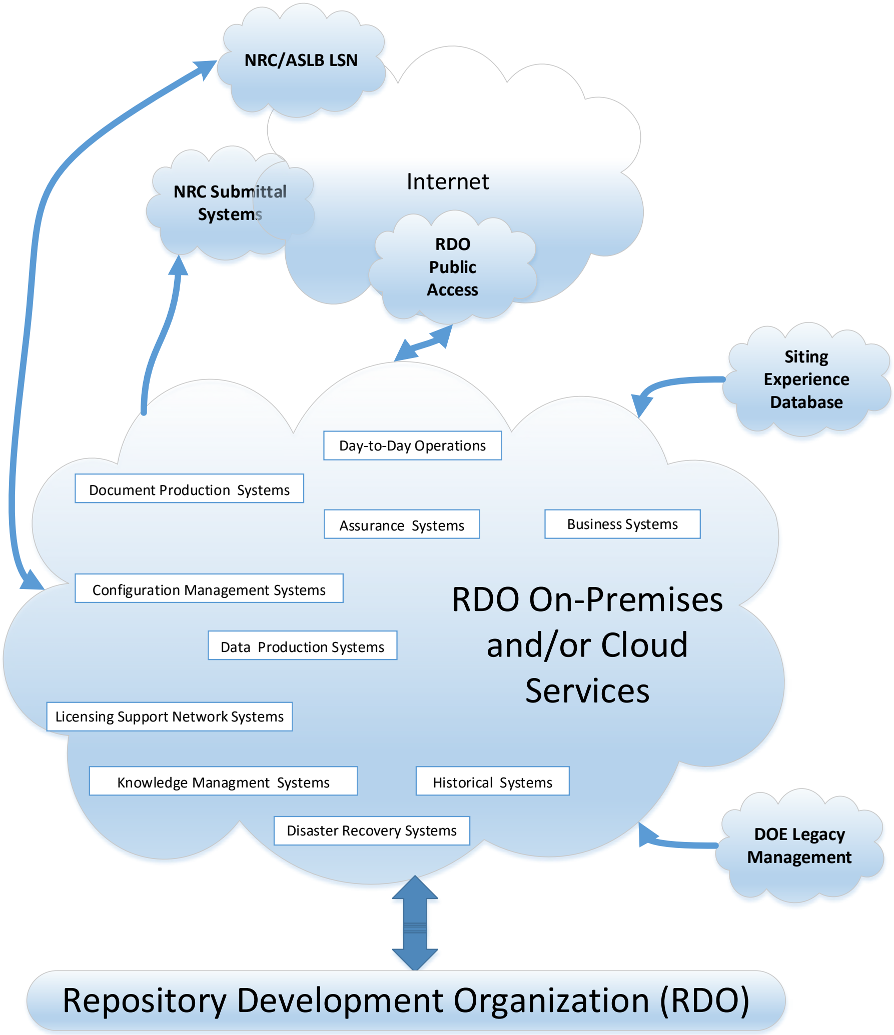

NRC/ASLB LSN
NRC Submittal Systems
Internet
RDO Public Access
Siting Experience Database
Day-to-Day Operations
Document Production Systems
Assurance Systems
Business Systems
Configuration Management Systems
RDO On-Premises and/or Cloud Services
Data Production Systems
Licensing Support Network Systems
Knowledge Managment Systems
Historical Systems
Disaster Recovery Systems
DOE Legacy Management
Repository Development Organization (RDO)

Figure 10 — Conceptual IT Architecture

- Maturity
  - Over time the number of defects should be on the decline
  - The software should have 'evolved' to fill its role (features upgraded)
  - Availability of experienced personnel in the industry
- Standardization
  - Government mandated security requirements (FedRamp for cloud, etc.)
  - DOE mandated requirements for IT Systems
- Cyber Security
  - National Security Systems Requirements (NIST)
  - National Infrastructure Protection Plan Requirement (Department of Homeland Security)
  - Authorized Reseller/Trusted Source
- Flexibility
  - The System should be adaptable, i.e.; ability to extend capabilities
  - Should be easily customized to organization mandates
- System Integration
  - Common Data Format integration – avoid having to convert data to/from application formats. Support a data transformation service to convert content between application specific formats
  - Security Integration - security methods integrate with existing installation, industry standards.
  - IT System should integrate with other systems by providing vertical integration, i.e.; integrate by creating additional functional entities or by horizontal integration, i.e.; through communication with other systems.
- Records Retention
  - IT system must support the records retention requirements of the organization.
  - IT system must provide content separation to facilitate unique records retention requirements (e.g., Controlled Unclassified Information).

4.2.4.2 Timing / Schedule for IT Systems

The timing for providing IT services is part of the 'Build / Maintain Infrastructure' timeline (Figure 3) and in the overall IT timeframe diagram below (Figure 11) for the RDO and would need to be implemented during the 'Startup' phase and completed by the 'Initiation' phase.

Figure 11 identifies the timelines and sequence in which the IT services should be planned to be available to the organization and the relative timing of implementation. Since Day-to-Day operations provide the basic infrastructure for the other IT services, this service needs to occur early and be completed before the others can occur. The Business System Functions are also required early in an organization and so this function must also occur early. Note that many of the services can be implemented concurrently. The length of the timeline for each service provides a relative degree of effort to implement the services (Business System functions require more effort than Document Production). There is no intent on identifying the length of each phase, in that the phases identify order not elapsed time.

4.2.4.3 IT Systems Architecture

To the extent practicable, the system architecture will be based on interconnected internet (cloud) technologies (Figure 9). The intent is to take advantage of interconnectivity, ease of access, scalability and economies of scale by employing IaaS and SaaS technologies that are readily available from commercial sources. Where not possible because of demonstrable security concerns, some reliance on on-premises resources may be unavoidable.

With a cloud solution, the on-premises solution will provide local desktop hardware and internet connectivity to the cloud. A user would then authenticate with the cloud, load their virtual desktop and then perform their daily tasks. Using the document sharing capability, documents produced by the RDO would be stored and versioned on the cloud and interested parties could be able to review and comment.

Additionally, a data pipeline could be configured to manage the workflow of the document from inception to publication. Leveraging the cloud capability as models are developed and run, the capability would execute using the automatic elasticity of the cloud platform allowing the scientist the capability to take advantage of latent compute cycles which will shorten the result delivery. Most (~95%) computing resources for the RDO could be hosted in the cloud and managed accordingly. The local infrastructure would provide internet connectivity and local workstations for accessing the virtual desktops managed by the RDO.

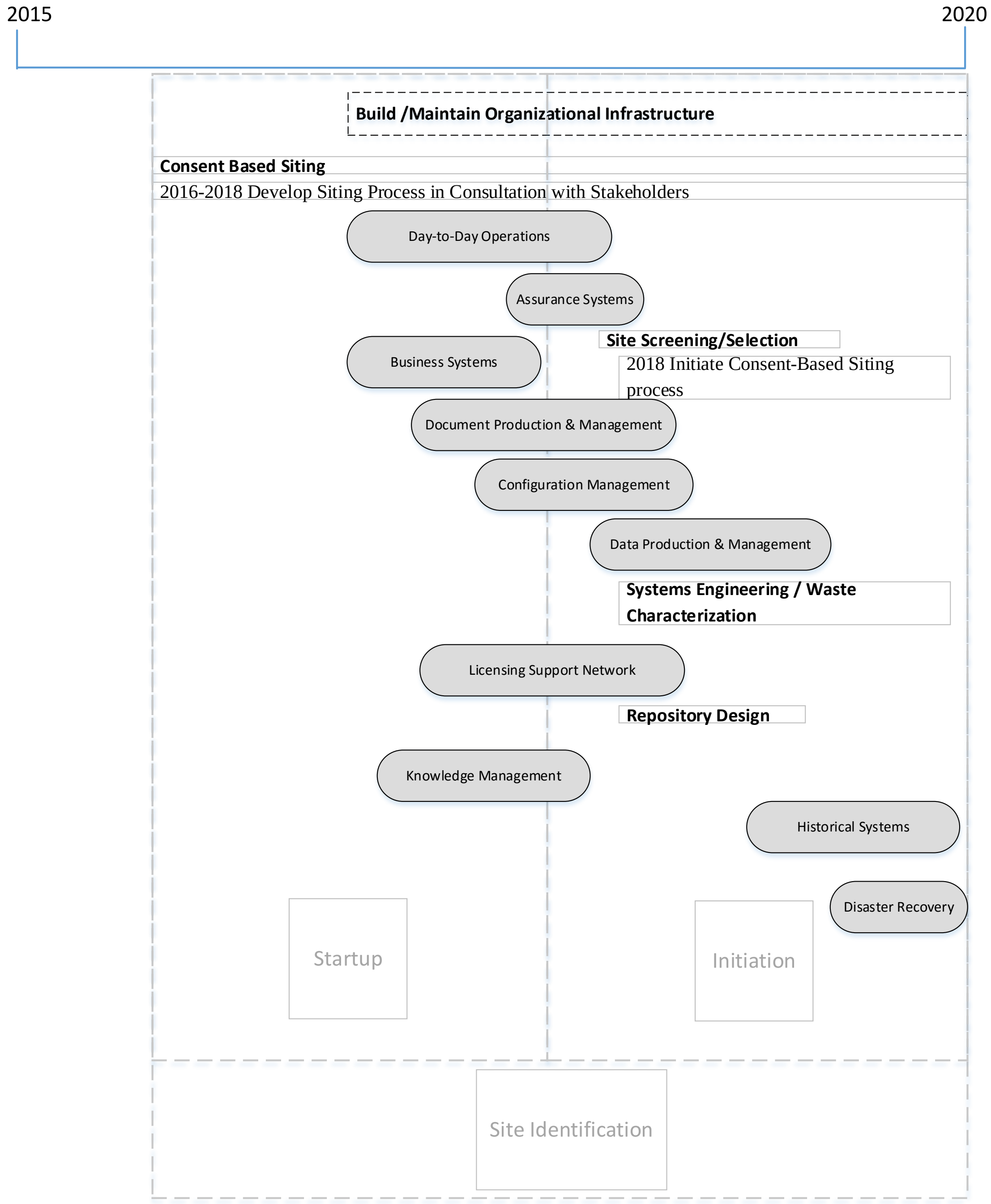

2015
2020
Build /Maintain Organizational Infrastructure
Consent Based Siting
2016-2018 Develop Siting Process in Consultation with Stakeholders
Day-to-Day Operations
Assurance Systems
Site Screening/Selection
Business Systems
2018 Initiate Consent-Based Siting process
Document Production & Management
Configuration Management
Data Production & Management
Systems Engineering / Waste Characterization
Licensing Support Network
Repository Design
Knowledge Management
Historical Systems
Disaster Recovery
Startup
Initiation
Site Identification

Figure 11 — IT Service Implementation Sequence

4.2.4.3.1 Cloud Environment

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (NIST 2011).

NOTE: Cloud computing can be provided by both an on-premises vendor (referred to as a 'Private Cloud') and an external vendor ("Public Cloud"). For the purposes of this discussion, unless named otherwise, whenever cloud computing is mentioned, it is "Public Cloud".

Cloud Computing: The Computing Stack

Cloud computing consists of three major types of services called the computing stack (Kepes 2016).

- IaaS – Infrastructure as a Service — the vendor provides computing infrastructure platforms as a commodity service at the vendor's operations center. The vendor provides the hardware, physical security, network, and utilities for the operation of the infrastructure. Other key features provided are server maintenance and a vendor provided mechanism for disaster recovery. A key advantage is 'speed' and 'scalability'. Vendors provide the service quickly and can scale to meet increased demand. Customers can then add their software (either custom or COTS) to provide IT functionality.
- PaaS – Platform as a Service — the vendor provides not only a computing infrastructure (IaaS) consisting of hardware, but also a development platform for developing and deploying applications quickly and efficiently. The service is available through the internet. Note that the distinction between IaaS and PaaS has blurred since there is not much that can be done with just a hardware platform.
- SaaS — Software as a Service — the vendor provides software applications, hardware, physical security and utilities within the vendor's infrastructure and customer rents the required services via the internet. This model allows the customer to consume the required services offered by the vendor without the need to host the software inside their premises and allows the customer access to the service from the internet. In addition to the advantage of 'speed' and 'scalability', the customer is now relieved of the task of managing software. This service is designed for end-user-applications delivered over the web. Typically, a provider licenses an application to a customer as a service on demand through a subscription in a pay-as-you-go model.

Cloud computing is a rapidly growing trend. It is not uncommon for organizations to employ some on-premises services, some 'private cloud' services, and some SaaS cloud computing from external vendors to deliver an IT system. This is often referred to as a 'Hybrid' cloud.

Major Vendors in Cloud Computing

Amazon Web Services (AWS) — AWS primarily provides IaaS or PaaS solutions, which includes:

- Compute infrastructure – Run and manage applications, automatic elasticity, high scale load balancing for virtual servers
- Storage and Content Delivery infrastructure – Scalable storage with global content delivery.
- Database infrastructure – Managed database services with simple data warehousing.
- Networking infrastructure – Isolated cloud resources and dedicated network connectivity capability.
- Security and Identity services – Hosted and managed active directory and user access.
- Management Tools – Track user activity and monitor resources and applications

Additionally, AWS has begun to branch out and provide some SaaS solutions (Robinson, et al. 2014) like:

- Desktop Virtualization – Desktop computing service with standard templates and includes capability to bring own licenses.
- Email and Calendaring –Secure managed email and calendaring
- Document Sharing – Enterprise document storage and sharing, including collaboration and versioning.
- Business Intelligence – Machine learning and business intelligence tools.
- Search – Scalable search clusters.

Microsoft — Azure Government

Microsoft Azure Government delivers a U.S. based cloud solution designed specifically to support strategic scenarios for U.S. government organizations including the Department of Defense, federal, state, and local governments, and their solution providers. It provides a comprehensive and open IaaS and PaaS for the U.S. government community including infrastructure, network, storage, data management and identity management delivered through secure and compliant hybrid cloud solution (Microsoft 2015).

Azure Government is designed to meet the higher level security and compliance needs for sensitive, dedicated, U.S. public sector workloads found in regulations such as FedRAMP and Department of Defense Enterprise Cloud Service Broker (Microsoft 2015).

Azure Government compute services can be broken into two classes: Azure Virtual Machines and Azure Cloud Services (Microsoft 2015).

- Azure Virtual Machines — The Azure Virtual Machines service provides on-demand, scalable computing resources
- Cloud Services — performs the infrastructure services such as Operating system patching, monitoring and scaling

Google

The Google Cloud Platform provides the following products:

- Compute Engine – Scalable high performance virtual machines available with either Windows or Linux operating systems
- Pre-emptible Virtual Machines – virtual machines that only last a short period of time
- Custom Machine Types – customizable machine types. Allows custom configurations of CPU and memory
- App Engine – a platform for building scalable web apps and mobile backends. Development tools such as Eclipse, IntelliJ, Git, Jenkins, and PyCharm.
- Container Engine – powerful cluster manager and orchestration system for running Docker Containers. It is built on the open source Kubernetes system

Google also provides networking and id management, with the ability to integrate on-premises and hybrid cloud environments.

Vendor Considerations (Criteria) for Cloud Environment

The cloud criteria for IT systems should include the General IT Systems Considerations and in addition include the following:

- Vendor Experience (minimum of five years' experience)
- Environment Compliance (Approved for Government Work)
  - Is it FedRAMP compliant? (GSA 2016)
  - Is it HIPAA compliant? (Microsoft 2015)
- Vendor Stability (stable business model)
- Vendor Disaster Recovery Options
  - Geographic separation of Network Operations Center (NOC)/Data Center

    - Near Real-time System Replication
- Vendor Security Plan
    - Identity Management
    - Data Security
    - Data Integrity
        - Virtual Machine Protection
        - Database Protection
    - Physical Security – is data housed with the U.S.
- Vendor Integration
    - Co-Location of Customer Equipment
    - Site-to-site VPN

4.2.4.3.2 On-Premises Environment

An on-premises environment consists of hardware, software, network, and support services provided for an organization by that organization. The organization typically provides the IT services at one or more data centers that it manages, hence the name —- 'on-premises'.

"On-premises software is a type of software delivery model that is installed and operated from a customer's in-house server and computing infrastructure. It utilizes an organization's native computing resources and requires only a licensed or purchased copy of software from an independent software vendor" (Google 2016).

It is one of the most common, traditional methods of using enterprise and consumer applications. On-premises software typically requires a software license for each server and/or end user. The customer is responsible for the security, availability and overall management of on-premises software. However, the vendor also provides after sales integration and support services. It is more expensive than cloud software because it requires in-house server hardware, capital investment in software licenses, in-house IT support staff and longer integration periods. However, on-premises software is considered more secure, as the entire instance of software and related data remain on the organization's premises (Google 2016).

On-Premises solutions can also provide 'Private Clouds', which are cloud type services (IaaS, SaaS). These have become more prevalent as an alternative to 'Public Cloud' services as they offer some of cost benefits of a cloud but retain the control and security benefits of on-premises environments.

Criteria for On-Premises Environment

The on-premises criteria for IT systems should include the General IT Systems Considerations (Section 4.2.4.1) and the following:

- The ability to separate the Repository Development Organization's content from the on-premises content (may be considered as 'Private Cloud')
- Ability to provide security for the organization's members
    - Support for Contract Personnel (citizen and non-citizen)
    - Support for MOW personnel
- Ability to provide access to content/systems via the Internet
    - Access to content must available to the RDO and public via the Internet
    - Access to selective IT systems must be available to the RDO and the public.
    - Access to selective IT systems and content must NOT be available to the public
- Flexible Application facilities
    - Ability to support the organization's unique requirements
- Be certified as a Federal Computing site
- Ability to scale the infrastructure to meet the organization's computing requirements
    - Scale data storage

  - Scale CPU and Memory
  - Scale Network capacity
- Ability to meet the organization’s service levels
  - o Support hours
  - o Support response time
- Provide disaster recovery of IT systems and Data
  - Provide off-site backup of data and software
  - Provide disaster recovery site to continue critical operations

Example of On-Premises Environment

An organization with a 24 hour/day — 7 day/week data center with dedicated climate and electrical power systems.

Hardware infrastructure for general computing:

- Windows or Linux Servers — Dell Power Edge, HP Blades
- SAN (Storage Area Network) — EMC Symmetrix, Network Appliance
- Ethernet Network – Cisco Routers, switches

Operating System Software infrastructure for general computing:

- Microsoft Windows Server software
- Microsoft Windows Desktop software
- RedHat, SuSe Linux software

Application development software for general computing:

- Internet Server Software — Microsoft’s IIS, Apache, TomCat
- Web Development Software

Database and ‘big data’ management system software:

- Microsoft SQL Server
- Oracle
- MYSQL
- Hadoop
- Mongo

COTS for day-to-day IT operations:

- Microsoft Exchange — provides email services for Outlook clients
- Oracle ERP — Accounts Payable, Account Receivable
- PeopleSoft — Payroll and HR services software
- Microsoft SharePoint – Web collaboration environment
- FileNet – document management support

Data Center Services

- Data backup and Archiving
- Records Management
- Disaster Recovery backup site
- Network Monitoring — SolarWinds
- Application Monitoring
- Help Desk for general computing and applications
- Desktop Support

High Performance Computing Cluster for Modeling and Simulations configuration for example:

- 1,800 nodes of 2.6 gHz Intel Sandy Bridge processors
- 64 GB ram per node
- Cray C S300-LC Green Blade hardware platform running RHEL6 O/S

4.2.4.3.3 Hybrid (mixture of On-Premises and Cloud-based)

A hybrid deployment is a way to connect infrastructure and applications between cloud-based resources and existing resources that are not located in the cloud (on premises). The most common method of hybrid deployment is between the cloud and on-premises infrastructure to extend and grow an organization’s infrastructure into the cloud while connecting cloud resources to the internal system. In short, hybrid cloud solutions are constructs that couple private resources and cloud services (Weinman 2016).

The cloud may act as the front end of an application to deliver content while connected to an on-premises database that is updated with data using internal systems. The reverse may also true. The cloud may act as the back end process to collect data and then share it with an on-premises internal system.

Criteria for Hybrid environment

The criteria for deploying IT systems in a hybrid environment are the combination of both cloud and on-Premises criteria.

Example of Hybrid environment

An organization with an on-premises email can utilize a Cloud-based filtering service to reduce the volume of spam, virus, and email threats before it reaches the on-premises network. In addition, an organization can utilize email archiving cloud services to reduce storage requirements and provide compliance to unique records retention requirements.

4.2.4.4 IT Systems / Services

This section describes the IT Systems/Services that directly relate to various organization element’s functions.

4.2.4.4.1 Day-to-Day IT Operations

These are IT Systems that provide the IT infrastructure necessary for most businesses. They would likely be provided by the enterprise’s designated IT organization. In addition, these systems will be able to support the software applications required for day-to-day operations.

- Desktop Support — maintain enterprise Common Operating Environment for desktops and provide customer support ticketing and resolution documentation (help desk)
- Email – COTS messaging system that will support instant messaging, calendars, etc. As discussed in Section 4.2.3.9 email functionality will need to be designed to satisfy LSN requirements. The impact on an IT solution is:
  - An email client plug-in is needed to query the user about the ‘relevancy’ of the content.
  - A process must be available that captures the emails marked as ‘relevant’ and send them to a service that will format and prepare them for delivery to the LSN.
  - Email from the organization and to the organization must be scanned periodically to determine if emails have been properly ‘marked’.
- Collaboration (External and Internal) — systems that will support workflow, approvals, and communication capability with both internal and external entities, for example Microsoft SharePoint, SharePoint On-Line, AWS Collaboration Tools.
- Content backup — automated back-up for designated software applications and data per enterprise requirements, for example NovaStor Data Center backup software

- Communications Capabilities (phone, audio/visual): Contract communication and video capability
- HPC capability (Modeling Support) — hardware and software system support for the clusters
- Hardware (server and desktop) support — maintains and manages hardware and refurbishment efforts
- Access control — security authorization for access to each system (userIDs, metagroups, etc.), (e.g., Kerberos userID/password control, Microsoft Active Directory)
- Software License Management — tracks licenses and ensures legal obligations are met for server and desktop software
- Network Storage — Large SAN capacity
- Networking and Infrastructure Support — network presence with internal and external access capability; system administration assistance with network and hardware components; contract for an Internet Service Provider presence, (e.g., EMC'S Clarion and Symmetrix solutions, Dell's 3PAR solution)

Table 4 — IT Environment Considerations — Day-to-Day Operations

ON-PREMISES	CLOUD	HYBRID
The Day-to-Day IT Operations are the foundation for an on-premises data center. Once implemented for an on-premises organization, they could be made available to the members of a RDO. Otherwise the RDO would take on the responsibility of providing its own on-premises data center and data center staff. By utilizing 'virtual infrastructure' technology (Private Cloud), an on-premises data center could provide IT systems similar to Public Cloud services.	The cloud solution for Day-to-Day IT operations will mirror the hybrid solution in some respects. There must be a local network and local workstations to access the cloud services. These local resources must be maintained and administered by IT professionals. However, for the cloud solution a virtual desktop can be provided to the organization users and corporate computing applications and resources will reside on in a cloud service.	While most of the Day-to-Day IT systems would likely be provided by the on-premises data center, some of the IT systems could be supplemented using cloud services, notably email and Collaboration.

4.2.4.4.2 Organizational Assurance Systems

IT System capabilities to support Organizational Assurance requirements include the following:

- Safety Conscious Work Environment (SCWE) — enable the workforce in identifying and correcting safety risks.
- Corrective Action Program (CAP) — systems that track areas of concern and document the measures taken to resolve them
- QA — support for administrative and procedural activities implemented in systems that ensure requirements and goals for a product, service or activity will be fulfilled
- NRC Information Submittal Systems — Systems that provide IT capability to transmit data and documents to NRC
  - ▪ Manage content specifically to meet Atomic Safety and Licensing Board requirements for posting on the LSN publically accessible website Manage content specifically to meet NRC requirements for submittal to NRC's ADAMS

Table 5 — IT Environment Considerations — Organizational Assurance Systems

ON-PREMISES	CLOUD	HYBRID
An on-premises solution would host corrective action tracking software as a dedicated service for the RDO or include the organization as a participant in existing software provided by the on-premises data center. Example: AssurX's Corrective and Preventive Actions (CAPA) software.	There are cloud environments which provide IaaS for hosting the systems required to meet assurance systems requirements (e.g., Qualitech Solutions BPI System provides Corrective Action Software in the Cloud).	There is no real benefit for a Hybrid solution. A hybrid solution has not been demonstrated as a feasible solution for this IT system service.

4.2.4.4.3 Business Systems

Systems that will provide the business infrastructure to manage training, logistics, financials, procurement and contracts management, asset management, and human resource services. They are the generally applicable systems for most businesses and would likely be provided by the enterprise's IT organization.

- Staffing Management — monitors the hiring, separations and benefits for enterprise employees and contractors
- Employee Concerns Program — monitors the reporting and resolution of reported employee concerns
- Training — assigns, tracks and documents training requirements
- Facilities — manages and monitors the physical locations for the enterprise
- Financials / Funding / Payroll — manages enterprise funding
- Project Controls — manages the schedule, resources, costs of the effort
- Procurement — provides the ability to purchase necessary assets and resources
- Contracts Management — tracks and provides legal oversight to ensure the contractual obligations are met
- Asset Management — tracks enterprise-owned physical assets
- Foreign National Request Access Control — provides security authorizations for foreign national employees and contractors
- Travel Records/Expenses: tracks travel and expenses related to the effort

Table 6 — IT Environment Considerations — Business Systems

ON-PREMISES	CLOUD	HYBRID
Business Systems for a RDO would be similar to most organizations. The RDO parent organization could already have IT systems in place to provide the IT systems discussed here and could provide them to the RDO as an on-premises solution. The challenge for sharing business systems with an RDO is the requirement to maintain separate information for the parent organization.	To meet the needs of the business systems the cloud solution will use a mixture of PaaS (to host the required business systems and SaaS. The PaaS solutions will be similar to the on-premises solutions but the servers will be hosted at the cloud solution providers NOC. If SaaS solutions meet requirements those services can be leveraged; for example, Trinet is a SaaS provider for Payroll and other HR services.	While some business system IT solutions could be provided in a cloud environment and some in an on-premises environment, a hybrid environment that utilizes both environments to support a single IT system does not seem viable.

4.2.4.4.4 Document Production Systems

These are systems that support the enterprise's document products. These systems are used for collaboration, technical editing, bibliographic documentation and graphic support. The system will meet mandated requirements on document creation standards and metadata.

- Reference Registry — system that will manage and provide access to copyright documents, as well as bibliographic materials
- Reference Verification — Track and manage verification of references in documents. This function should be part of the document preparation or review and approval process that could be delivered through a custom on-premises solution or through cloud services. There are a number of software solutions that could be implemented in On-Premises or Cloud-based environments (part of IaaS or SaaS). Example: EndNote, BibTex to manage references, KeyPreps for matching citations to references, and Reference Checker, a macro added to Microsoft Word.
- Copyrighted Reference Registry — track and manage the permissions related to copyright materials
- Graphics — software systems that will provide graphics for documents per the enterprise's requirements
- Document Development — workflow that will enable electronic approvals and version control

Table 7 — IT Environment Considerations — Document Production Systems

ON-PREMISES	CLOUD	HYBRID
An on-premises solution would utilize desktop software for developing document products and document management software as a centralized repository, providing version control (check-in, check-out), approvals, security, and document information. The RDO could utilize the on-premises solutions or utilize a 'Private Cloud' to provide the services as a separate SaaS solution. Example: Microsoft Word for document preparation, and SharePoint Server for document management (Gartner 2015) or FileNet.	The cloud solution would leverage a SaaS document production services like Google Docs. This application and relevant documents would reside in the cloud. Inherent in many of these service offerings is online collaboration and versioning where multiple users can work on a document together. These documents can be run through a business process engine (also residing in the cloud) to enforce document standards while managing the required review and approval processes. Additionally, the business process engine will meet reference registry requirements by tracking and managing references (e.g., Google Docs or Office 365 with custom developed business process engine).	An on-premises desktop may provide the software to create and edit documents locally while a cloud service would deliver collaboration, review and approval as well as document management facilities (version control, check-in/check-out, document metadata, reference tracking, etc.). An example is using Microsoft Office on desktops running Windows as the on-premises component. Google Docs or SharePoint Online (with document management add-on) could provide collaboration and document management.

4.2.4.4.5 Configuration Management Systems

These are systems that support managing and versioning of enterprise artifacts (software, data, documentation, etc.)

- Regulatory Document Configuration Management — provides a controlled environment for storing and accessing documentation provided to NRC and other regulatory entities
- Correspondence Control — provides a controlled environment for storing and accessing formal correspondence related to the effort.
- Records Management — certified records management system that meets DoD 5015 requirements for electronic records and NARA requirements for paper documentation
- Document Management/Control — electronic document system that provides controlled submission, version control, and access to formal enterprise products
- Data Management — systems that will provide access, metadata and version control (this will include multiple repositories) for both structured and unstructured data
- Requirements Management — will track requirements via processes and procedures as well as IT system configuration requirements
- Commitment Management — tracks milestones and deliverables
- Facilities and Safeguards & Security — tracks facilities, safeguards and security items
- Software Configuration Management System — track software and licenses used by the enterprise
- Data Management System – systems designed to store technical data
- Licensing Support Network (LSN) Content Transmittal — electronic workflow that enables the timely transmission of licensing support relevant documentation

Table 8 — IT Environment Considerations — Configuration Management Systems

ON-PREMISES	CLOUD	HYBRID
Configuration management can be provided by utilizing dedicated software products such as Microsoft’s Systems Management Server capability to create an inventory of hardware and software in an SMS database.	As mentioned previously configuration management could be provided by a system in the cloud environment. There are several vendors providing configuration management software and many of these solutions can be used in the cloud environment. One possible system would be Puppet. There are additional requirements for RDO related to regulatory document configuration management. These requirements could be met by the collaboration solution and the document production solution (e.g., Puppet, collaboration and document production.)	A hybrid solution does not appear to be feasible solution for this IT system service

4.2.4.4.6 High Performance Computing and Data Systems

These are systems that are necessary to deliver one of the principal products of the effort (i.e., data and analysis results). The type of data generated includes content from performing compliance demonstration assessments and modeling simulations within geographic areas. High Performance Computing (HPC) capability is needed to support this service. HPC Capability is provided by clusters of server nodes (CPU and Memory) attached to a SAN. Data management includes tracking the input parameters and data output files. It is a necessary requirement of modeling software product used in data production.

- Modeling support — systems required to support modeling software applications and required records requirements
- Simulation support — systems required to support simulation software applications and required records requirements
- Compliance Demonstration Analyses — systems that may support COTS applications that support the HPC capabilities
- Geographic Information System (GIS) capabilities — systems to support COTS applications that support geographic information systems for the effort

Table 9 — IT Environment Considerations — High Performance Computing and Data Systems

ON-PREMISES	CLOUD	HYBRID
An on-premises solution would provide HPC environments to support the data modeling/simulations software required. An alternative to a ‘dedicated cluster’, a private cloud solution could be used as an on-premises solution and provide some of the same benefits as a public cloud solution.	The cloud solutions for HPC and document production will also play a role in data production. A similar business process engine will be used to support the data production for the modelling and simulation tools. The cloud solution can provide HPC systems that will be provisioned dynamically for modelling, simulation and GIS solutions. These systems can be allocated ad hoc and be available for the scientists just in time use. Once the systems are no longer needed the virtual machines can be powered down, decreasing cost and load. The data products from these systems will be available after the virtual machines are no longer active.	A Hybrid solution would not be feasible. Either Cloud-based or On-Premises solutions would be more effective.

4.2.4.4.7 License Support Network

The organization must provide to the LSN the documentary material relevant to a repository license application. This includes not only document files but relevant emails. As such, the IT solution must provide the following:

- Relevant emails
- Relevant documents
- Transmission of emails and documents on a regular basis to a service that prepares and delivers the content to the LSN

Table 10 — IT Environment Considerations — Licensing Suppor Network

ON-PREMISES	CLOUD	HYBRID
The NRC License Support Network requirements would be challenging for an On-premises environment coexistent with a parent organization's system. In this scenario the parent's on-premises system would already have an email service in place for the members of its workforce and would then extend that service to the additional members of the RDO. The requirement would be to provide a 'markup' plug-in on the email client workstations for only the RDO members. This could provide unnecessary complications for the parent organization's processes. In addition, the IT solution would have to separate the emails, scan them periodically and deliver them to the service that prepares them for submittal to the LSN. An alternative is to provision the RDO its own email service with its own email server, email address and separate storage. The RDO IT lead would supply the infrastructure and support for the additional service. This would be an example of a private cloud service. The RDO would provide an environment to collect documents where they can be reviewed and marked as final documents and then transmitted to the service that provides the content to the LSN, (e.g., Microsoft SharePoint (with a document management add-on) or a Document management system like FileNet.)	The cloud solution could leverage a SaaS email service offering like AWS email or Google's Gmail for Business. This application and relevant documents would reside in the cloud. Additionally, many of these vendors also include archival and eDiscovery service offerings that are not only compatible with email but can be leveraged for other documents as well. These eDiscovery tools can analyze relevant emails, chats, and documents produced for the organization within the SaaS products and then collect those artifacts for submittal to the LSN. For example: Gmail for Business with Google Vault.	The on-premises systems could employ email markup plugins on client workstations for the RDO MOW, but use a cloud based email server to process the emails provide SPAM and Virus detection, prevent outside threats, and then deliver them to the service that formats the files for submittal to the LSN.

4.2.4.4.8 Knowledge Management Systems

The purpose of a knowledge management system is to support compiling, organizing, leveraging, and preserving the organization's knowledge base(s) to support organizational goals and anticipated future needs, including information systems supporting the understanding of important issues for continuing long-term safety of the repository system by avoiding the loss of institutional and societal knowledge long after its closure. These systems will need to accommodate very large quantities of traditional information (documents), as well as audio and video recordings.

4.2.4.4.9 Historical Systems

Historical Systems provide Information from past programs. These systems could include, but are not limited to:

- Siting Experience Database — The Centralized Used Fuel Resource for Information Exchange (CURIE) website maintained by the Oak Ridge National Laboratory for the DOE provides an archive of documentation regarding efforts to site nuclear waste facilities, both in the U.S. and abroad
- DOE Legacy Management – repository of YM information systems
- YM License Support Warehouse – search capability that extends to information in the YM Lead Laboratory information archive
- YM Report Center – a search tool that provides quick and easy access to YM data such as the Technical Data Management System, the Direct Input Reference System, the Controlled Document Information System, the CAP system and the Records Information System
- YM RAIDS — Request for Additional Information Development System (RAIDS) – information system dedicated to the development of responses to RAIs from NRC
- YM Hearing Process Support System — system dedicated to the development of information to support the applicant's participation in NRC adjudicatory hearings for YM

Table 11 — IT Environment Considerations — Historical Systems

ON-PREMISES	CLOUD	HYBRID
There is currently an on-premises environment for this IT system service. An on-premises solution to host these IT Systems should include the following software: • Microsoft's SharePoint Server (SharePoint 2013 or later) • Microsoft SQL Server DBMS (SQL Server 2008 or later) • Microsoft SQL Server Reporting Services (SQL Server 2008 or later) • Microsoft Windows Server (2008 or later) • Microsoft FAST Search	There are cloud environments which could provide either IaaS platforms for hosting the Historical systems software or SaaS providing the software environment for the items listed under the on-premises solution. For example: Microsoft Azure Government could provide: • SharePoint Online • SQL Server Azure (provides SQL Server database and reporting services) • Windows Server • FAST Search Services	A hybrid solution has not been demonstrated as a feasible solution for this IT service

4.2.4.4.10 Disaster Recovery Systems

These capabilities provide data and application backups both locally and at a remote site. They are essential and mitigate the risk of data and service loss in the event of a local disasters or application failures. They would provide basic services at a remote site in the event of a site disaster.

- Off Site Backup: per enterprise requirements, automated movement of back-ups to a designated off-site location
- Disaster Recovery Plan: documented plan that identifies the process for recovery; includes hardware and software that will enable recovery per the enterprise's requirements

Table 12 — IT Environment Considerations — Disaster Recovery Systems

ON-PREMISES	CLOUD	HYBRID
If there is already an on-premises disaster recovery of business continuity solution in place, then the RDO could take advantage of the service if the RDO uses existing on-premises services. Otherwise, providing business continuity in the form of disaster recovery is an expensive and complex IT system to implement for a new organization. Engaging an off-site service to host critical functions is a popular solution as well as using an organization's satellite location has also been an alternative. Employing 'Private Clouds' to deliver RDO IT systems using IaaS and SaaS would simplify disaster recovery in an on-premises environment as replacement systems could be regenerated more quickly. For example, Iron Mountain provides off-site data backup services. Sun provides off-site disaster recovery host services.	Most of disaster recovery will be provided as a service for a cloud solution. The cloud service provider will have a disaster recovery plan that can fail over to a geographically separated NOC from the primary NOC used by the organization. This will include automated backup of the virtual machines and a detailed disaster recovery plan for the organization to implement.	A hybrid solution would include on-premises backup to local SAN with supplemental backup using a cloud service.

4.3 Science/Engineering

Science and Engineering is the organizational element responsible for the direction, coordination, performance, and oversight of science and engineering activities. These will include interactions with DOE to formulate direction, mitigate complex issues involving internal and external organizations, present work-related material to upper management, approve technical and non-technical products and documents, and allocate resources to the performance of regularly scheduled work and rapid response tasks associated with repository sciences and engineering.

As described in Section 3, "The specific configuration and details of the scientific and engineering organizational elements is beyond the scope of this report." The context in which the science and engineering organizational elements will operate has yet to be established. Hence, only general descriptions of the following functions are provided.

4.3.1 Chief Technical Advisor

The Chief Technical Advisor is responsible for advising the RDO Manager and other members of the organization's management team on the adequacy and completeness of produced scientific and engineering information and working to ensure technical work performed by and for the organization is sound, credible and meets the highest standards of scientific integrity.

The Chief Technical Advisor is also responsible for providing technical and operational integration between the organization's regulatory office and other technical groups in the development of regulatory responses, condition report planning and execution of design integration, software configuration management and oversight of ongoing science activities. Another principal responsibility of the Chief Technical Advisor is ongoing maintenance and fostering of relationships with internal and external national science interests, DOE and its legal counsel, and oversight groups (Nuclear Waste Technical Review Board, National Science Foundation, etc.).

4.3.2 Systems Engineering

This element manages the systems engineering activities conducted by the organization and is responsible for evaluating the potential for waste management system optimization based on various characteristics including, waste location, waste inventory, waste characteristics (e.g., thermal properties), canister and container characteristics, etc. The reports, analyses and other documentation of the results of this element's efforts will begin to populate the various configuration management systems discussed above.

This function is responsible for conducting the system analysis activities supporting phased deployment of a comprehensive nuclear waste management system. These activities are approached in an adaptive manner. Integrated system analysis and system engineering principles are applied to evaluate an integrated approach to transportation, storage, and disposal in the waste management system, with an emphasis on adapting to evolving national policy/direction. These analyses will support the establishment of functional and operational requirements for the waste management system, provide the framework for future planning activities (i.e., transportation hardware procurements), support environmental impact analyses, and support future strategic decisions for accepting SNF from shutdown and operating reactors.

4.3.3 Waste Inventory and Acceptance

The waste inventory and acceptance organizational element's responsibilities are directed evaluating and implementing strategies consistent with a phased (staged) development approach for a repository. These focus on achieving initial operation of a repository for the DOE-managed HLW and SNF using that portion of the inventory that is currently ready for disposal and that presents the fewest technical and regulatory challenges, which is the existing defense HLW glass and cooler DOE-managed SNF (SNL 2014). The principal task of this element will be to maintain an inventory of DOE-managed HLW and

SNF and continuously evaluate treatment options to supply a repository waste disposal inventory as the effort develops.

Much of the inventory has not yet been placed into a final form for disposal (SNL 2014, DOE 2014), and might be suitable for different waste forms and disposal approaches than assumed to date. Based on today's understanding, selection of disposal options with suitable characteristics might allow DOE to simplify waste treatments, potentially accelerating cleanup activities and avoiding or reducing costs associated with projected treatments for some parts of the waste inventory. Depending on the characteristics of the selected repository site and future developments with respect to waste treatment options, additional HLW waste forms other than those currently anticipated could be considered in a later phase of repository development.

There could be significant benefits in terms of reduced waste package cost and simplification of operations if larger, higher-thermal-load packages can be shown to be disposable at the repository after initial operation has begun. Such packages could be used in a subsequent phase of operations, with appropriate regulatory approval.

4.3.4 Repository Science and Engineering (Science and Technology)

Repository sciences and engineering manages and performs the technical repository development activities conducted by the organization, consistent with various approaches that may be defined by DOE. In addition to general repository science efforts, this element is responsible for siting, site characterization, performance assessment, and performance confirmation.

4.3.4.1 Siting Studies

The Siting Studies function is responsible for and conducts the technical siting related activities for the RDO. The function will need to provide environmental, geoscience, and engineering expertise to develop the information needed by the NEPA compliance element to develop the EA(s), EIS, or PEIS, as necessary. The reports, analyses, data collected and other results of this element's efforts will begin to populate the various configuration management systems discussed above.

Neither the NWPA nor the AEA establish a specific process for locating, evaluating, and selecting sites for repositories for DOE-managed SNF and HLW. However, we can anticipate the fundamental activities that will support siting of a proposed repository:

- Evaluation of sites considered for selection
- Information supporting EAs for one or more sites
- Initial information collection to support an EIS

4.3.4.2 Site Characterization Studies

The Site Characterization Studies function is responsible for and conducts site characterization activities for the RDO. Such activities typically involve a broad range of techniques, including environmental, geologic and geophysical surveys as well as exploratory drilling. The reports, analyses, data collected and other results of this element's efforts will populate the various configuration management systems discussed above. Information from site characterization will provide the bulk of information used in the license application and the accompanying EIS. Site characterization may involve several thousand participants, and the support organization processes and systems need to be well developed and exercised to accommodate the inflow of information. Site Characterization activities address regulatory and technical matters as the effort begins to develop the substance needed to support the license application.

NRC's rule, 10 CFR Part 60, Subpart B, Preapplication Review, provides the agency's current expectations relative to site characterization. Also, 10 CFR 60.16 requires a site characterization plan with its contents specified in 10 CFR 60.17. Even though it is anticipated that the regulation may be revised (Rubenstone 2012) it provides some insight into NRC's expectations.

4.3.4.3 Compliance Demonstration (Performance Assessment)

The Compliance demonstration / performance assessment function is responsible for the activities conducted by the RDO to demonstrate compliance with applicable regulations partially based on information gathered during site characterization. The magnitude of this effort is very substantial, and may involve more than a hundred participants. The computer codes used to perform these calculations are complicated and require high performance computer capability for their execution (Section 4.2.4.4).

4.3.4.4 Performance Confirmation

Performance Confirmation is responsible for the development and design of the performance confirmation program derived from site characterization information. Site characterization defines the technical aspects of the site to be licensed, which will require demonstrated compliance with 10 CFR Part 60 Subpart F, Performance Confirmation Program. “Performance Conformation means the program of tests, experiments, and analysis which is conducted to evaluate the accuracy and adequacy of the information used to determine with reasonable assurance that the performance objectives for the period after permanent closure will be met” (10 CFR 60.2). By regulation the “program shall have been started during site characterization and it will continue until permanent closure” (10 CFR 140(b)).

4.3.5 Storage

This element is responsible for the waste storage that may be undertaken by the RDO, consistent with the various approaches that may be defined by DOE. The objective is to lay the groundwork to implement consolidated interim storage as a planned part of the waste management system.

4.3.6 Transportation

This element is responsible for the transportation activities conducted by the RDO, consistent with the various approaches that may be defined by DOE. The objective is to prepare for the transportation to the repository of DOE managed SNF and HLW from sites at which it is currently stored. The primary focus in the near term is on making progress on long lead-time, destination-independent aspects of the transportation infrastructure.

4.3.7 Facility Design

This element is responsible for the RDO facility design activities.

4.3.8 Facility Operations

This element is responsible for the RDO facility operations activities.

5. References

10 CFR 2 Subpart J—*Procedures Applicable to Proceedings for the Issuance of Licenses for the Receipt of High-Level Radioactive Waste at a Geologic Repository*.

10 CFR Part 21. *Reporting of Defects and Noncompliance*, Nuclear Regulatory Commission, 42 FR 28893, June 6, 1977.

10 CFR Part 60. *Disposal of High-Level Radioactive Wastes in Geologic Repositories*. Nuclear Regulatory Commission.

10 CFR Part 1021. *National Environmental Policy Act Implementing Procedures*. U.S. Department of Energy, November 14, 2011.

10 CFR Part 851. *Worker Safety and Health Program*. U.S. Department of Energy, February 9, 2006.

29 U.S.C. 794(d), *Rehabilitation Act of 1973*, as amended by Workforce Investment Act of 1998 (P.L. 105-220).

36 CFR, Subchapter B, *Records Management*.

40 CFR Part 191. *Environmental Radiation Protection Standards for Management and Disposal of Spent Nuclear Fuel, High-Level and Transuranic Radioactive Wastes*. U.S. Environmental Protection Agency, January 1, 2012.

66 FR 55732. *Statements of Consideration for 10 CFR Part 63, Disposal of High-Level Radioactive Waste in a Proposed Geologic Repository at Yucca Mountain, Nevada*. U.S. Nuclear Regulatory Commission. November 2, 2001.

76 FR 34773. *Final Safety Culture Policy Statement*. Federal Register Notice: Nuclear Regulatory Commission, June 14, 2011.

80 FR 79872. *Invitation for Public Comment to Inform the Design of a Consent-Based Siting Process for Nuclear Waste Storage and Disposal Facilities*, December 23, 2015.

ASME NQA-1 2015. Quality Assurance Requirements for Nuclear Facility Applications. New York City, New York: American Society of Mechanical Engineers.

CEQ (Council on Environmental Quality) 2014. *Memorandum for Heads of Federal Departments and Agencies; Effective Use of Programmatic NEPA Reviews*, December 18, 2014.

DoD 5015.2-STD, *Electronic Records Management Software Application Design Criteria Standard*, February 24, 2015. U.S. Department of Defense.

DOE G 413.3-10A, *Earned Value Management System (EVMS)*. Washington, DC: U.S. Department of Energy. 2015.

DOE G 414.1-5. *Corrective Action Program Guide*. Washington, DC: U.S. Department of Energy. 2010.

DOE G 450.4-1C, *Integrated Safety Management System Guide*. Washington, DC: U.S. Department of Energy.

DOE O 243.1B, *Records Management Program*. Washington, DC: U.S. Department of Energy, March 11, 2013.

DOE O 413.3B, *Program and Project Management for the Acquisition of Capital Assets*. Washington, DC: U.S. Department of Energy. 2010.

DOE O 414.1d, *Quality Assurance*. Washington, DC: U.S. Department of Energy.

DOE O 435.1. *Radioactive Waste Management*. Washington, DC: U.S. Department of Energy. 1999.

DOE O 442.1A. *Department of Energy Employee Concerns Program*. Washington, DC: U.S. Department of Energy. 2001.

DOE O 442.2. *Differing Professional Opinions for Technical Issues Involving Environmental, Safety, and Health Technical Concerns*. Washington, DC: U.S. Department of Energy.

DOE O 450.2. *Integrated Safety Management.* Washington, DC: U.S. Department of Energy.

DOE O 470.4B. *Safeguards and Security Program*. Washington, DC: U.S. Department of Energy. 2013.

DOE O 473.3A. *Protection Program Operations*. Washington DC: U.S. Department of Energy. 2016.

DOE P 450.4A. *Integrated Safety Management Policy.* Washington, DC: U.S. Department of Energy.

DOE (U.S. Department of Energy) 2013. *Strategy for the Management and Disposal of Used Nuclear Fuel and High-Level Radioactive Waste*. Washington, DC: U.S. Department of Energy, January 2013.

DOE 2014. *Assessment of Disposal Options for DOE-Managed High-Level Radioactive Waste and Spent Fuel*. Washington, DC: U.S. Department of Energy, October 2014.

DOE 2015. *Report on Separate Disposal of Defense High-Level Radioactive Waste*. Washington, DC: U.S. Department of Energy.

Gartner, 2015. *In-Depth Assessment of SharePoint 2013 for Document and Records Management.* Gartner Research, November 2015

Google 2016. "Google Vault: *Add archiving and eDiscovery to Google Apps*." https://apps.google.com/products/vault/

GSA (General Services Administration) 2016. *FedRAMP; Cloud Service Providers*. U.S. General Services Administration, https://www.fedramp.gov/participate/csps/

IAEA (International Atomic Energy Agency) 2006. *Application of the Management System for Facilities and Activities.* Safety Guide Gs-G-3.1, Vienna, Austria: International Atomic Energy Agency.

Kepes, B. 2016. *Understanding the Cloud Computing Stack SaaS, PaaS, IaaS.* Diversity Limited. http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf

Microsoft 2015. *Microsoft Azure Government Overview.* Microsoft. https://azure.microsoft.com/en-us/documentation/articles/azure-government-overview/

NARA (National Archives and Records Administration) 2016. *Criterial for Managing Email Records in Compliance with the Managing Government Records. Directive.* M-12-18. Washington DC: National Archives and Records Administration Office of the Chief Records Officer. April 6, 2016.

NEI (Nuclear Energy Institute) 2015. *Corrective Action Processes for New Nuclear Power Plants During Construction*. NEI 08-02, DRAFT Revision 4, October 2015. ML15306A511

NIST (National Institute of Standards and Technology) 2011. *The NIST Definition of Cloud Computing*. NIST Special Publication 800-145. Gaithersburg, MD: National Institute of Standards and Technology.

NRC (U.S. Nuclear Regulatory Commission) 2002. *Differing Professional Views or Opinions: 2002 Special Review Panel*, NUREG-1763. Washington, DC: U.S. Nuclear Regulatory Commission.

NRC 2004a. *Licensing Support Network for Documents Relating to the Yucca Mountain Licensing Proceeding Conducted by the U.S. Nuclear Regulatory Commission.* NUREG/BR-0301 Rev 1. Washington, DC: U.S. Nuclear Regulatory Commission. ML041760035.

NRC 2004b. SECY-04-0111, *Recommended Staff Actions Regarding Agency Guidance in the Areas of Safety Conscious Work Environment and Safety Culture*. July 1, 2004. Washington, DC: U.S. Nuclear Regulatory Commission. ML041750238.

NRC 2005. *NRC Regulatory Issue Summary 2005-18: Guidance for Establishing and Maintaining a Safety Conscious Work Environment.* Washington, DC: U.S. Nuclear Regulatory Commission Office of Nuclear Reactor Regulation and Office of Nuclear Material Safety and Safeguards

NRC 2011. *Guidance for Electronic Submissions to the NRC*. Revision 6.1. Washington, DC: U.S. Nuclear Regulatory Commission.

NRC 2014. *Differing Professional Opinions Program Assessment*. Washington, DC: U.S. Nuclear Regulatory Commission, Office of Enforcement, ML14272A541.

Obama, B.H. 2015. Presidential Memorandum—*Disposal of Defense High-Level Radioactive Waste in a Separate Repository*. Memorandum for the Secretary of Energy. March 24, 2015.

Robinson, G., Narin, A., Elleman, C. 2014, "Using Amazon Web Services for Disaster Recovery, Amazon Web Services," October 2014. https://aws.amazon.com/disaster-recovery/

Romhardt, K. 2014. *Processes of Knowledge Preservation: Away from a Technology Dominated Approach*. Zürich, Switzerland: University of Geneva/Geneva Knowledge Group.

Rubenstone, J. 2012. "Emerging Regulatory Challenges in the Management of Spent Nuclear Fuel and High-Level Radioactive Waste," *The Bridge: Linking Engineering and Society*, *42* (2), 32-39. National Academy of Engineering.

SNL (Sandia National Laboratories) 2014. *Evaluation of Options for Permanent Geologic Disposal of Used Nuclear Fuel and High-Level Radioactive Waste Inventory in Support of a Comprehensive National Nuclear Fuel Cycle Strategy*. FCRD-UFD-2013-000371; SAND2014-0187P; SAND2014-0189P, Revision 1. Albuquerque, NM: Sandia National Laboratories.

SNL 2016. *Draft Operating Procedures for a Generic Repository Development Organization*. SAND2016-9090 R; FCRD-UFD-2016-000638. Albuquerque, NM: Sandia National Laboratories.

Umeki, H.; Takase, H.; Hioki, K. and McKinley, I. 2009. "Overview of the JAEA Knowledge Management System Supporting Implementation and Regulation of Geological Disposal in Japan." *Proceedings of the 2009 12th International Conference on Environmental Remediation and Radioactive Waste Management*. ICEM2009 October 11-15, 2009. Liverpool, UK.

Weinman, J. 2016. "Hybrid Clouds: The Best of Both Worlds," Microsoft Publishing. https://azureinfo.microsoft.com/Hybrid-Cloud-the-Best-of-Both-Worlds.html

Zheng, W.; Yang, B.; and McLean, G. 2010. "*Linking Organizational Culture, Structure, Strategy and Organizational Effectiveness: Mediating Role of Knowledge Management*." *Journal of Business Research* 63 (2010): 763–771. Elsevier Publishing.