Unified Security Management

Nuclear Cyber Security

cmplid://

the.compliance.daemon

USM Methodology Education

October 2016

Forward

This paper describes the Unified Security Management (USM) approach to implementing and maintaining a cyber security program for the nuclear power industry.

This document explains the USM approach to the Risk Management Framework (RMF) Security Lifecycle defined within US National Institute of Standards and Technology (NIST) Special Publications (SP). Specifically this document provides guidance of how the USM can be used to support the RMF in a nuclear generation operator's implementation of a Cyber Security Plan (CSP) based on the US Nuclear Regulatory Agency's (NRC) Regulatory Guide (RG) 5.7, Cyber Security Programs For Nuclear Facilities or the Nuclear Energy Institute's (NEI) document 08-09, Cyber Security Plan for Nuclear Reactors.

These two documents are extremely similar in nature, but differences between them do exist and will he highlighted within this text. Additionally, this document will explain how cmplid:// supports utilizing guidance from additional documents in order to increase the maturity of a nuclear cyber security program based on RG 5.71 or NEI 08-09.

This document frames the discussion within the structure of the NIST Security Lifecycle as while nuclear power plant operators may not be subject to the US Federal Information Systems Management Act (FISMA) the RG 5.71 and NEI 08-09 controls were based on the SP 800-53 control library which was designed to integrate with the RMF's Security Lifecycle.

Contact

cmplid:// Inc.
www.cmplid.com
info@cmplid.com

License

Credits

The USM is largely nothing more than an extension of the NIST provided guidance on security management taken to the logical conclusions of that guidance. cmplid:// is extremely grateful to NIST, particularly the Computer Security Resource Center for their work.

The USM has been influenced by and seeks to fulfill Albert Einstein's great advice:

Everything should be made as simple as possible, but not simpler.

USM Automation

The USM is "as simple as possible, but no simpler". It does require appropriate tools in order to manage all of the structured data that the USM requires. cmplid:// the.compliance.daemon, the security management automation solution provided by cmplid:// inc. fully supports all of tasks and processes described within this paper. For more information contact us at www.cmplid.com or info@cmplid.com.

References

The following documents are referred to in this document:

Regulatory Guide 5.71 Cyber Security Programs For Nuclear Facilities

U.S. Nuclear Regulatory Commission, January 2010

> *This regulatory guide provides an approach that the NRC staff deems acceptable for complying with the Commission's regulations regarding the protection of digital computers, communications systems, and networks from a cyber attack as defined by 10 CFR 73.1.*

NEI 08-09 Cyber Security Plan for Nuclear Power Reactors [Rev 6]

Nuclear Energy Institute, April 2010

> *This document was developed to assist licensees in constructing and implementing their Cyber Security Plan license submittal as required by 10 CFR 73.54.*

NEI 13-10 Cyber Security Control Assessments [Rev 4]

Nuclear Energy Institute, November 2015

> *This guidance document was developed to streamline the process for addressing the application of cyber security controls to the large number of CDAs identified by licensees when conducting the analysis required by 10 CFR 73.54(b). The goal is to minimize the burden on licensees of complying with their NRC approved cyber security plan, while continuing to ensure that the adequate protection criteria of 10 CFR 73.54 are met.*

NEI 10-04 Identifying Systems and Assets Subject to the Cyber Security Rule [Revision 2]

Nuclear Energy Institute, July 2012

> *The purpose of NEI 10-04 is to provide guidance on the identification of digital computer and communication systems and networks subject to the requirements of 10 CFR 73.54.*

NEI 10-09 Addressing Cyber Security Controls for Nuclear Power Reactors

Nuclear Energy Institute, 2011

> *This document (NEI 10-09) has been developed to: facilitate consistent understanding of the cyber security controls; ensure consistent understanding of the attack vectors associated with NEI 10-09 (Revision 0) September 2011 ii controls; describe a method to document and justify crediting existing programs, processes, and defensive architectures; and, provide a consistent methodology for addressing cyber security controls.*

> NOTE: This document was not endorsed by the NRC for use and much of the guidance provided within is therefore of limited value.

IAEA NSS No.17 Computer Security at Nuclear Facilities

International Atomic Energy Agency, 2011

> *This publication is in the Technical Guidance category of the IAEA Nuclear Security Series, and deals with computer security at nuclear facilities. It is based on national experience and practices as well as publications in the fields of computer security and nuclear security. The guidance is provided for consideration by States, competent authorities and operators.*

NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems Revision 1

National Institute of Standards and Technology, February 2010

> *This publication, developed by the Joint Task Force Transformation Initiative Working Group, transforms the traditional Certification and Accreditation (C&A) process into the six-step Risk Management Framework (RMF).*

NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations Revision 4

National Institute of Standards and Technology, April 2013

> *Special Publication 800-53, Revision 4, provides a more holistic approach to information security and risk management by providing organizations with the breadth and depth of security controls necessary to fundamentally strengthen their information systems and the environments in which those systems operate—contributing to systems that are more resilient in the face of cyber attacks and other threats. This "Build It Right" strategy is coupled with a variety of security controls for "Continuous Monitoring" to give organizations near real-time information that is essential for senior leaders making ongoing risk-based decisions affecting their critical missions and business functions.*

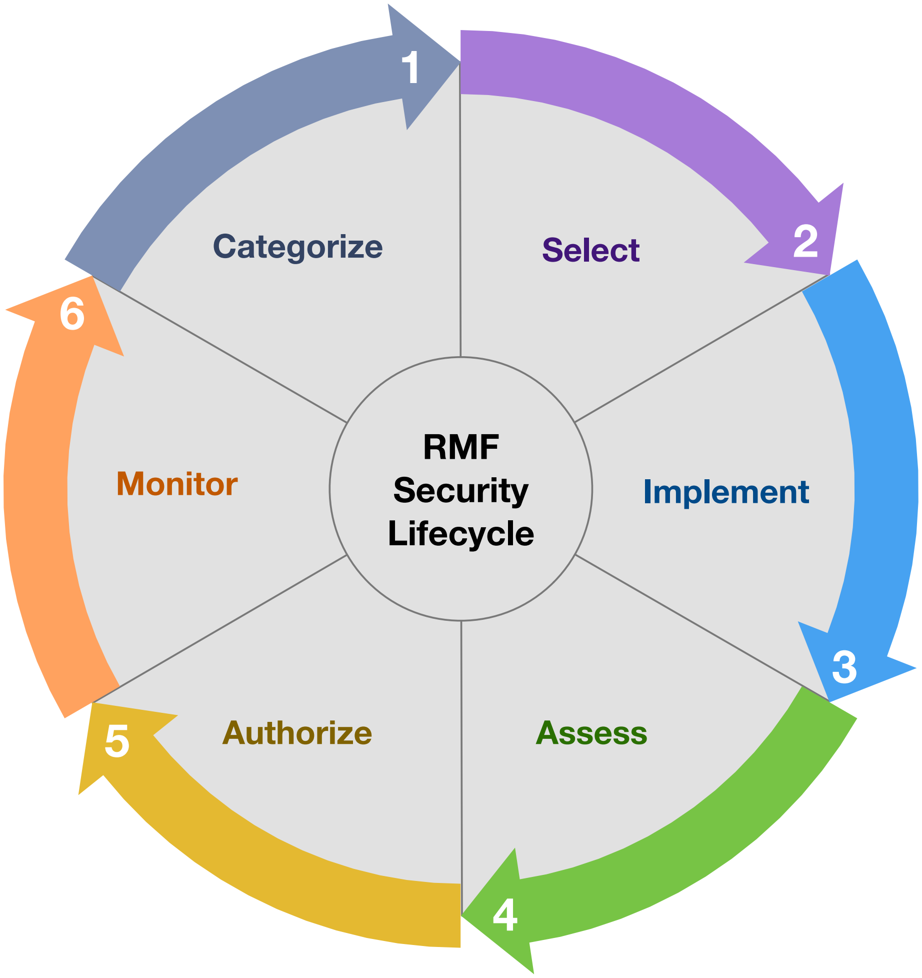
NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.0

National Institute of Standards and Technology, February 2014

> *The resulting Framework, created through collaboration between government and the private sector, uses a common language to address and manage cyber security risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses.*

The RMF Security Lifecycle

The Security Lifecycle, described within NIST SP 800-37 provides 6 distinct steps of security management. The operations within these phases and their place within the RMF are described in this document. The steps are depicted in the following diagram:



Each of these steps is guided by NIST Special Publications (SP) or Federal Information Processing Standards (FIPS). SP 800-37 provides this high-level description of these steps:

> ***Categorize*** *the information system and the information processed, stored, and transmitted by that system based on an impact analysis.*
>
> ***Select*** *an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.*
>
> ***Implement*** *the security controls and describe how the controls are employed within the information system and its environment of operation.*
>
> ***Assess*** *the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.*

> ***Authorize*** *information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.*
>
> ***Monitor*** *the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.*

In the following discussion of these steps, the relevant nuclear cyber security publications are substituted for their SP or FIPS equivalents. As will be seen, each of these steps contains a set of distinct tasks that must be executed with relevant inputs and outputs to achieve a stated objective.

The USM is not a replacement for the RMF, it is simply a methodical approach to implementing the RMF.

Overview of the USM

The USM can be most succinctly explained by its primary characteristics.

Resource-Based

All security requirements apply to various types of Resources. This aspect of the USM relies heavily on the NIST defined concept of control inheritance:

> *Common controls are security controls that are inherited by one or more organizational information systems. Common controls are identified by the chief information officer and/or senior information security officer in collaboration with the information security architect and assigned to specific organizational entities (designated as common control providers) for development, implementation, assessment, and monitoring.* ***Common control providers may also be information system owners when the common controls are resident within an information system. [emphasis added]***

The key difference between NIST control inheritance and USM control inheritance is the emphasis placed on organizational responsibility. Designating a control as common from the NIST perspective is almost exclusively a product of the responsibility for development, implementation, assessment, and monitoring of the control. Within the USM common controls are designated based on the implementation Resource for the control, which will determine responsibility. The emphasized sentence in the quote above speaks to this.

NIST documents are organized around the protection of Information Systems, defined as:

> *A discrete set of information Resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.*

Similarly, RG 5.71/NEI 08-09 are organized around the protection of Critical Digital Assets (CDA), defined as:

> *A subcomponent of a critical system that consists of or contains a digital device, computer or communication system or network.*

The issue with each of these definitions, from the perspective of security management efficiency and effectiveness, is that largely the requirements of the RMF and the CSP do not apply solely to Information Systems or CDAs respectively, introducing ambiguity and confusion.

Training requirements apply to personnel groups, physical security requirements apply to physical locations, policies and procedures are written for organizations, etc… Further many of the security requirements that apply to Information Systems or CDAs, as defined, only apply to certain components thereof, firewalls are installed on networks, authentication is enforced on software, etc…

The USM is designed to reduce or eliminate this type of ambiguity and confusion as much as possible. The alignment of the security program to the types of Resources within scope is the first step in this process.

Resource Types

Each of the security requirements defined within a security program apply to one or more Resource Types. The USM recognizes nine basic Resource Types to which the security requirements apply.

Name	Description
Software	Compiled computer code
Hardware	Automated processing systems and the underlying Operating Systems
Network	Physically and logically connected devices, usually communicating via the TCP/IP protocol suite
Source Code	Human modifiable (uncompiled or interpreted) source code
Media	Information storage
Information	General classes of information that require protection based on the sensitivity to compromise of confidentiality, integrate, or availability
Location	Facilities, rooms, racks, containing Resources requiring protection
Organization	Collections of Resources (people, equipment, facilities, etc...) with a common mission, business objective, or purpose
Personnel	People within scope of the compliance program

Additionally, Resource types specific to security programs, e.g. the RMF and CSP, can be specified when necessary.

Name	Description
Information Systems	A discrete set of information Resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Critical Systems	An analog or digital technology based system in or outside of the plant that performs or is associated with a safety-related, important-to-safety, security, or emergency preparedness function. These critical systems include, but are not limited to, plant systems, equipment, communication systems, networks, offsite communications, or support systems or equipment, that perform or are associated with a safety-related, important-to-safety, security, or emergency preparedness function.
Hardware Component	A physical asset with its own equipment database asset tag that while may be a component of a CDA, will not have the RG 5.71/NEI 08-09 Controls applied directly to it.

Control inheritance in a Resource-based process is determined not solely on the organization responsible for the controls, but rather on the Resources receiving protection from a control.

Training requirements apply to personnel groups, the information systems or CDAs accessed by the trained personnel inherit the protection provided by the training.

Physical security requirements apply to physical locations, the information systems or CDAs within those locations inherit the physical security protection.

Policies and procedures are written for organizations, all of the Resources owned by the organization inherit the protection provided within the policies and procedures.

Firewalls are installed on networks, all hardware and software attached to or reachable from the networks, inherit the protection of the firewalls.

In this way, inheritance does lead back to the division of responsibility for the security controls, but provides a simple mechanism for doing so: those organizations responsible for the implementation of the Resources where the inherited controls are applied, are responsible for the common control provided.

Attribute-Informed

Characteristics of the Resources will dictate the necessity for and implementation of the applicable requirements. These characteristics (or Attributes) of the Resources are specific to the defined Resource Types and are used throughout the USM for all aspects of security management.

They provide the mechanism for associating risk, vulnerabilities, compliance, governance, and configuration management activities throughout the security program. Attributes can be divided into four categories:

Compliance Scope Attributes

Attributes that indicate inclusion in the scope of a security program. These attributes are based on the business objectives of the security program, as documented within the programs literature.

Security Posture Attributes

Attributes that indicate the required security posture for a Resource within scope. These attributes are based on and developed through analysis of the security requirements mandated by the security program, relative to the population of Resources within scope of the program.

Risk Indicator Attributes

Attributes that identify risks to the business processes or system functions supported by the Resources within scope. These attributes are determined based on the risk analysis process adopted by the organization and minimally must indicate the level of risk to Confidentiality, Integrity, or Availability.

Optionally, risk indicator attributes can identify the level of risk in regard to deficiencies in the protection, detection, response, or recovery of negative events.

Information Attributes

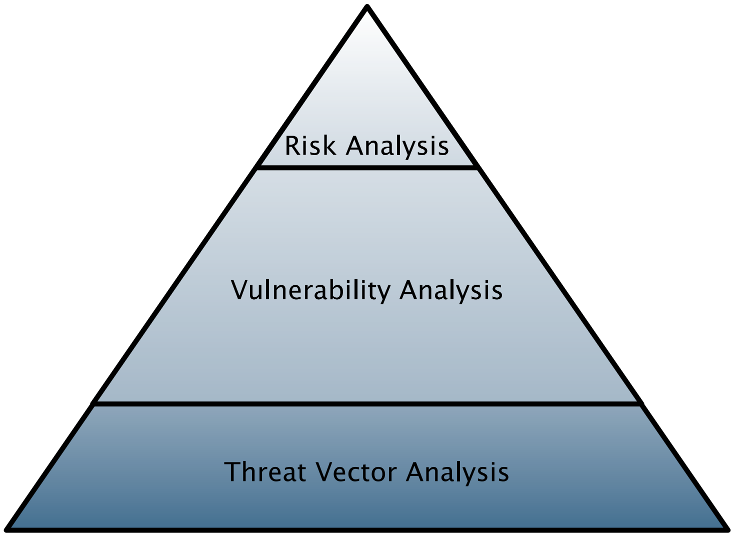
Attributes that identify information about a Resource that is useful for personnel managing the Resources, but that is not required for each of the previous mentioned roles, i.e. Information Attributes are by definition, not necessary to determine scope, indicate security posture, or identify risk.

The USM approach is flexible and mandates that end-users identify and document each of these types of attributes with the granularity necessary and the language required to be effectively communicated throughout their organization.

Objective-Producing

The requirements are applied to address identified risks, vulnerabilities, or threat vectors and each of these must be evaluated in accordance with the business or technical objectives that must be met.

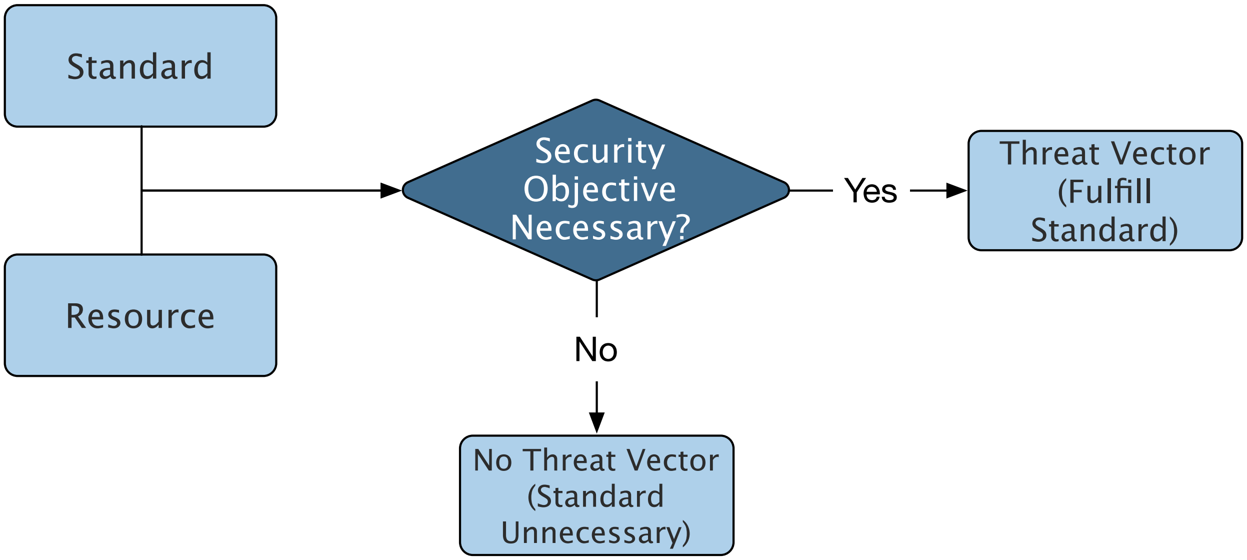
The USM provides for a hierarchical structure of objective-based analysis, depicted in the diagram to the right as a pyramid.



Threat Vector Analysis

The bottom of the pyramid indicates that the base analysis will be that of determining Threat Vectors for the Resources within scope. This analysis provides that IF a threat vector exists (on a Resource) for a given security requirement's objective, THEN the security requirement SHALL be fulfilled. That may be all of the analysis that is completed for some Resources.

A variety of factors influence the type of analysis that will be conducted, chief among them are the type of Resource (business or technical) and the information available about relevant vulnerabilities.


Standard
Resource
Security Objective Necessary?
Yes
Threat Vector (Fulfill Standard)
No
No Threat Vector (Standard Unnecessary)

Threat Vector Analysis Example

Standard

> *RG 5.71 B 1.3 a2 Access Enforcement: [Licensee/Applicant] is responsible for the following: assigning all user rights and privileges on the CDA consistent with the user authorizations*
>
> *NEI 08-09 D 1.3 a2 Access Enforcement: This Technical cyber security control: Assigns user rights and privileges on the CDA consistent with the user authorizations*

Security Objective

Ensures logical access accounts have only the permissions required to fulfill their required business objectives.

Resource(s)

Paperless Chart Recorder (1-PCR-101) This Resource provides logical user interaction, operational parameters may be viewed or set from the HMI, based on the password or PIN entered, therefore the Threat Vector exists: The organization must ensure that only appropriate personnel have access to the password/PIN that allows configuration.

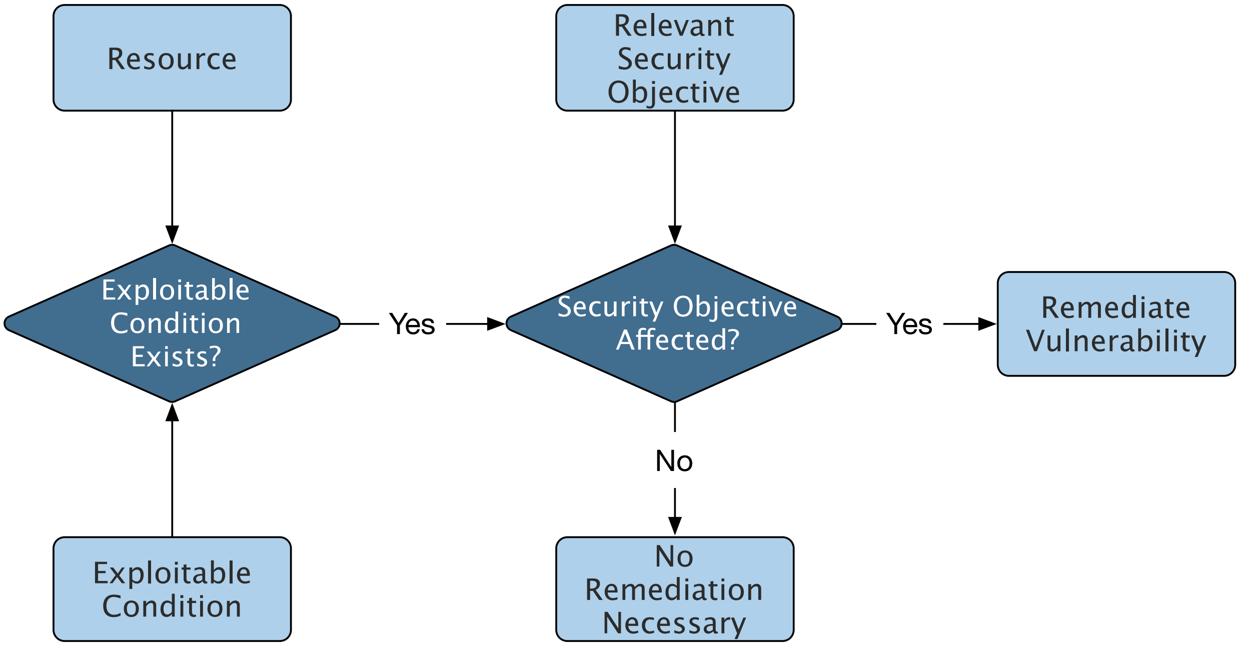
Pressure Transmitter (1-PT-101) This Resource provides no logical user interaction, the configuration may only be modified through connection of a laptop that modifies the configuration and updates the firmware stored in an EPROM, therefore the Threat Vector Does Not Exist, failure of this security requirement cannot be used to exploit the Resource.

NOTE: There is, obviously, a threat to the pressure transmitters configuration, in that unauthorized changes could be made to the configuration through the use of the laptop, however, other controls, concerning portable device access and disabling communication ports will be relied on to protect against those threats.

> Threat Vector analysis is accomplished at a granular level to identify those prescribed security standards that must be addressed for the Resources within scope.

Vulnerability Analysis

The middle section of the pyramid indicates that in addition to Threat Vector Analysis, the USM provides for a mechanism to analyze vulnerabilities (Exploitable Conditions) present within Resources that could impact the fulfillment of a given security requirement's objective. This analysis provides that IF an Exploitable Condition exists for a given Resource AND the Exploitable Condition could negatively affect a required security objective, THEN the vulnerability must be remediated.


Resource
Relevant Security Objective
Exploitable Condition Exists?
Yes
Security Objective Affected?
Yes
Remediate Vulnerability
No
Exploitable Condition
No Remediation Necessary

Vulnerability Analysis Example

Exploitable Condition

Insecure encryption of attachments sent by PearOS that could potentially reveal the secret key used to encrypt message content.

Resource

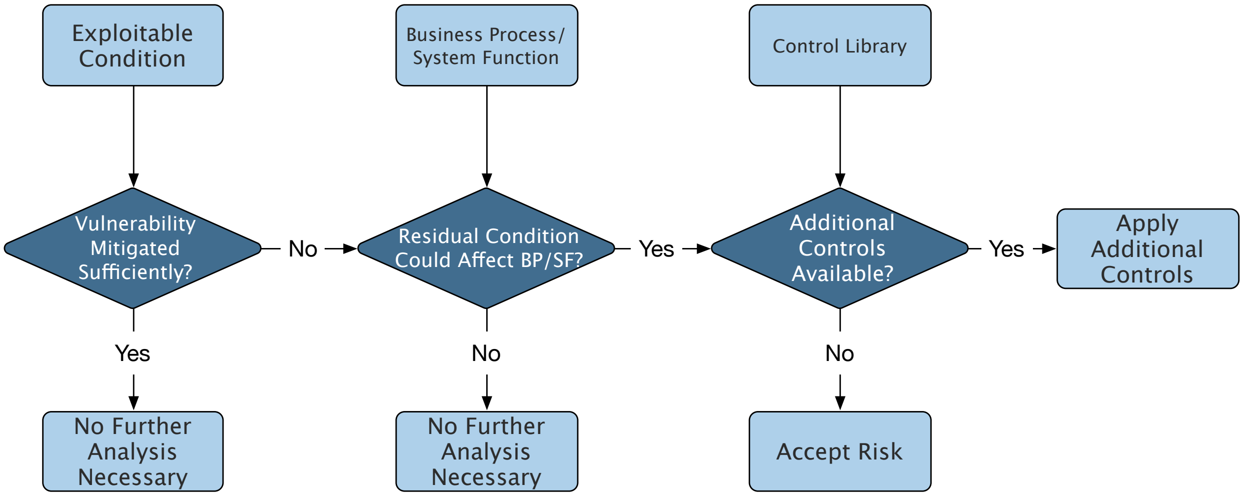
Officer Workstation (1-OW-101) This Resource is running PearOS, therefore the Exploitable Condition exists on the Resource, However, this workstation is on a physically secured air-gapped network and therefore, there is no opportunity for unauthorized personnel to observe the communications. The relevant security objective: Ensures that information with high-confidentiality requirements is protected during transmission, is met through the physical protections and remediation of the vulnerability is not required.

In many cases, this vulnerability analysis is all that is necessary to determine the appropriateness of the remediation.

Risk Analysis

The top section of the pyramid indicates that in addition to Vulnerability Analysis, the USM provides for a mechanism to analyze risks to the Business Processes and System Functions supported by the Resources. This analysis is useful when Exploitable Conditions exist that complete remediation is impossible or extremely difficult or where additional mechanisms should be employed.

Risk Analysis evaluates those Exploitable Conditions and determines that, if left unmitigated or mitigated insufficiently, they could lead to Negative Events on the supported Business Process or System Functions. The purpose of this analysis is to identify any security mechanisms that are appropriate for implementation on the affected Resources in addition to or in place of the basic vulnerability remediation.


Exploitable Condition
Business Process/ System Function
Control Library
Vulnerability Mitigated Sufficiently?
No
Residual Condition Could Affect BP/SF?
Yes
Additional Controls Available?
Yes
Apply Additional Controls
Yes
No
No
No Further Analysis Necessary
No Further Analysis Necessary
Accept Risk

Risk Analysis Example

Exploitable Condition

Race condition in httpd version 1.0, that if exploited could cause all communications from the server to cease.

Resources

All historian servers are running httpd version 1.0, therefore the Exploitable Condition exists on these Resources, However, significant time and costs would be required to upgrade all historian servers to the latest version.

System Function Supported

These servers support the real time understanding of plant status and are used for operational decision making.

Negative Event(s) Possible if Condition Exploited

Operators would lose the Plant Process Computers ability to reliably show the state of many plant systems.

Additional Controls Available

The control room has many redundant sources for most of the information within the PPC, loss of the historian server would be an inconvenience, but do not rely solely on the Plant Process Computer for status. These systems are physically located within Vital Areas within the plant with limited access, and are isolated from external networks via a data diode. The Resources running httpd version 1.0 must eventually be upgraded, but the mitigating conditions reduce the risk to the System Function to an acceptable level in the meantime.

Risk Analysis is useful when vulnerability analysis is insufficient. Generally speaking, systems will be patched or configurations changed, etc… once a known vulnerability is known for them. However, there may be times where patching a system or changing its configuration is not practical; this is where risk analysis comes into play.

Operations Facilitated by the USM

The advantage of the USM is, as it states, the Unified nature of it. Each of the analysis methods described previously (Threat Vector, Vulnerability, Risk) is facilitated through the attributes provided for each of the Resources within scope. The following operations are facilitated through the Resource-based, attribute-informed, objective-producing methodology:

Compliance Management

Compliance management ensures that the security posture required by the security programs is in place for each Resource managed.

Risk Management

Risk management ensures that the security posture is appropriate within the context of the Business Processes or System Functions supported.

Vulnerability Management

Vulnerability Management ensures that the security posture is functioning correctly.

Governance Management

Governance Management ensures that the security posture is managed by appropriate personnel.

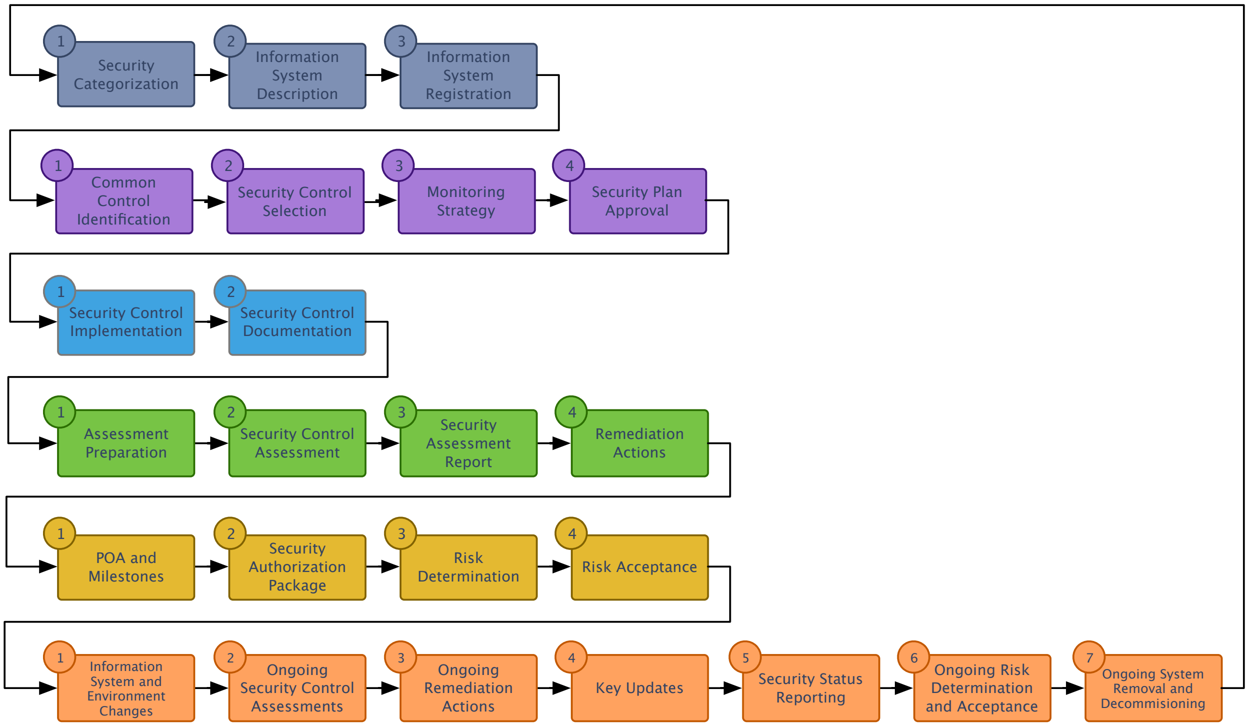
Configuration Management

Configuration Management ensures that the security posture is maintained throughout the Resources life.

This document focuses on Compliance Management for nuclear power plant operators.

Security Lifecycle Tasks

The following diagram depicts the individual tasks within each of the Security Lifecycle phases from SP 800-37:


1 Security Categorization
2 Information System Description
3 Information System Registration
1 Common Control Identification
2 Security Control Selection
3 Monitoring Strategy
4 Security Plan Approval
1 Security Control Implementation
2 Security Control Documentation
1 Assessment Preparation
2 Security Control Assessment
3 Security Assessment Report
4 Remediation Actions
1 POA and Milestones
2 Security Authorization Package
3 Risk Determination
4 Risk Acceptance
1 Information System and Environment Changes
2 Ongoing Security Control Assessments
3 Ongoing Remediation Actions
4 Key Updates
5 Security Status Reporting
6 Ongoing Risk Determination and Acceptance
7 Ongoing System Removal and Decommissioning

The following table provides a narrative of each of these tasks, from SP 800-37:

Phase	Name	Description
Categorize	Security Categorization	Categorize the information system and document the results of the security categorization in the security plan.
	Information System Description	Describe the information system (including system boundary) and document the description in the security plan.
	Information System Registration	Register the information system with appropriate organizational program/management offices.
Select	Common Control Identification	Identify the security controls that are provided by the organization as common controls for organizational information systems and document the controls in a security plan (or equivalent document).
	Security Control Selection	Select the security controls for the information system and document the controls in the security plan.
	Monitoring Strategy	Develop a strategy for the continuous monitoring of security control effectiveness and any proposed/actual changes to the information system and its environment of operation.
	Security Plan Approval	Review and approve the security plan.

Phase	Name	Description
Implement	Security Control Implementation	Implement the security controls specified in the security plan.
	Security Control Documentation	Document the security control implementation, as appropriate, in the security plan, providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs).
Assess	Assessment Preparation	Develop, review, and approve a plan to assess the security controls.
	Security Control Assessment	Assess the security controls in accordance with the assessment procedures defined in the security assessment plan.
	Security Assessment Report	Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment.
	Remediation Actions	Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s), as appropriate.
Authorize	Plan of Action and Milestones	Prepare the plan of action and milestones based on the findings and recommendations of the security assessment report excluding any remediation actions taken.
	Security Authorization Package	Assemble the security authorization package and submit the package to the authorizing official for adjudication.
	Risk Determination	Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.
	Risk Acceptance	Determine if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable.
Monitor	Information System and Environment Changes	Determine the security impact of proposed or actual changes to the information system and its environment of operation.
	Ongoing Security Control Assessments	Assess a selected subset of the technical, management, and operational security controls employed within and inherited by the information system in accordance with the organization defined monitoring strategy.
	Ongoing Remediation Actions	Conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the plan of action and milestones.
	Key Updates	Update the security plan, security assessment report, and plan of action and milestones based on the results of the continuous monitoring process.

Phase	Name	Description
Monitor	Security Status Reporting	Report the security status of the information system (including the effectiveness of security controls employed within and inherited by the system) to the authorizing official and other appropriate organizational officials on an ongoing basis in accordance with the monitoring strategy.
	Ongoing Risk Determination and Acceptance	Review the reported security status of the information system (including the effectiveness of security controls employed within and inherited by the system) on an ongoing basis in accordance with the monitoring strategy to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation remains acceptable.
	Information System Removal and Decommissioning	Implement an information system decommissioning strategy, when needed, which executes required actions when a system is removed from service.

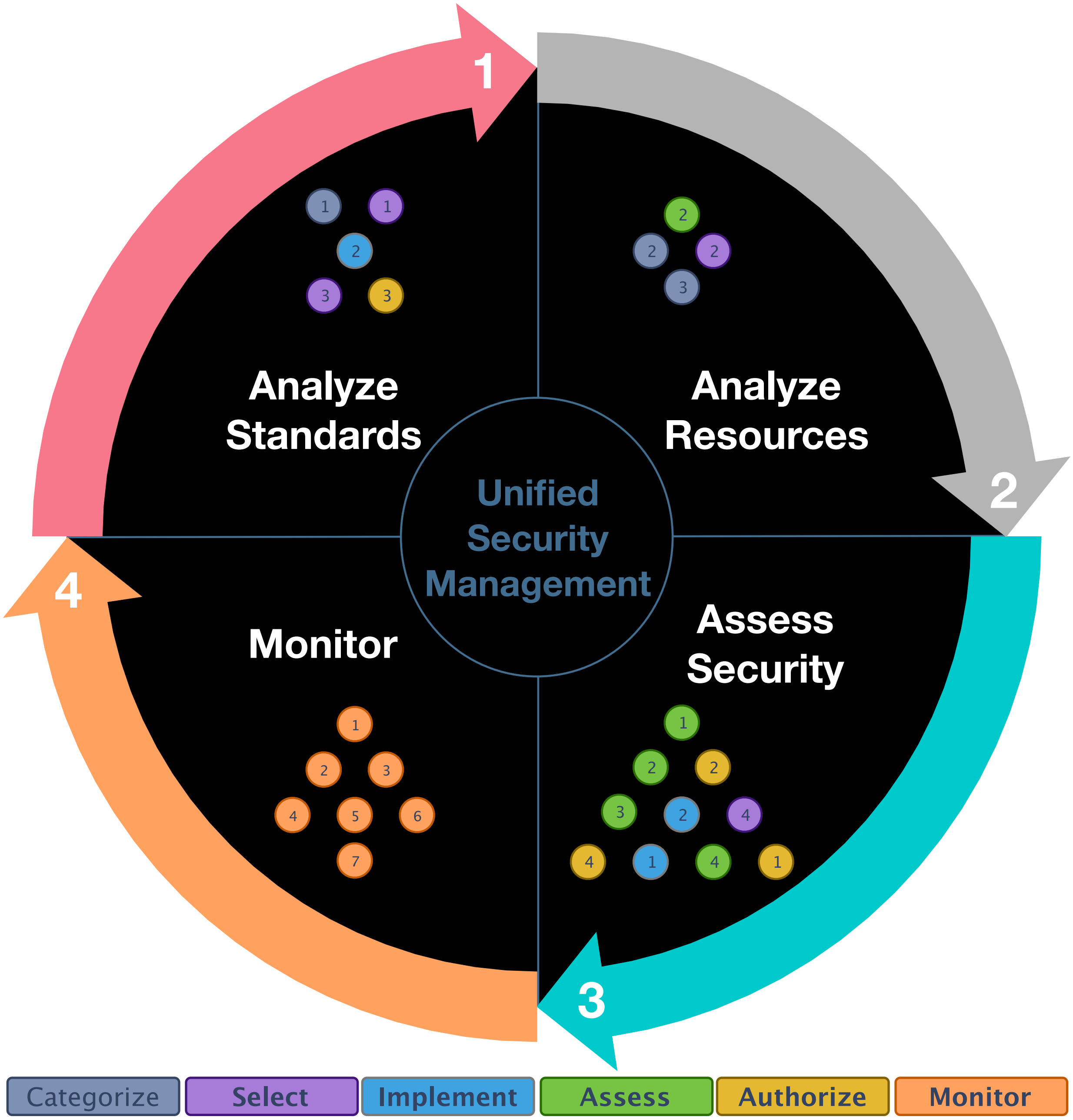
The Security Lifecycle is described with the tasks in sequential order, however, that is not required by the RMF, as described in SP 800-37:

> *Since the tasks in the RMF are described in a sequential manner, **organizations may choose to deviate from that sequential structure** in order to be consistent with their established management and system development life cycle processes or to achieve more cost-effective and efficient solutions with regard to the execution of the tasks.*

This is good, because as will be discussed, there are better sequences for these tasks. The USM provides for each of these tasks to be completed, however, the ordering of the tasks is different. This re-ordering of the tasks is designed to increase both the efficiency of process and increase the effectiveness of the resulting program, primarily through introducing consistency through font-loaded analysis.

The USM Approach

The following diagram illustrates the same Lifecycle but with the USM at its center, as it's processes provide significant efficiencies in and increased effectiveness of managing the disparate steps of the security lifecycle. The numbered circles within the quadrants represent the RMF Security Lifecycle tasks supported by the phases.



Obviously, the striking difference is that there are only four "phases" within the USM. This, like with the RMF Security Lifecycle, is someone imprecise.

While the RMF allows for the re-sequencing of the Security Lifecycle, the USM actively recognizes that describing a consistent serial flow to managing technology security, while extremely helpful within educational and policy papers, is often not reflective of real life.

Security management is generally more of a distinct set of operations or processes that are, from an overall perspective, carried out simultaneously throughout an organization. Some resources will be being assessed as others are analyzed, monitoring continuously happens, and standards are analyzed at every change as the regulatory or internal security programs mature.

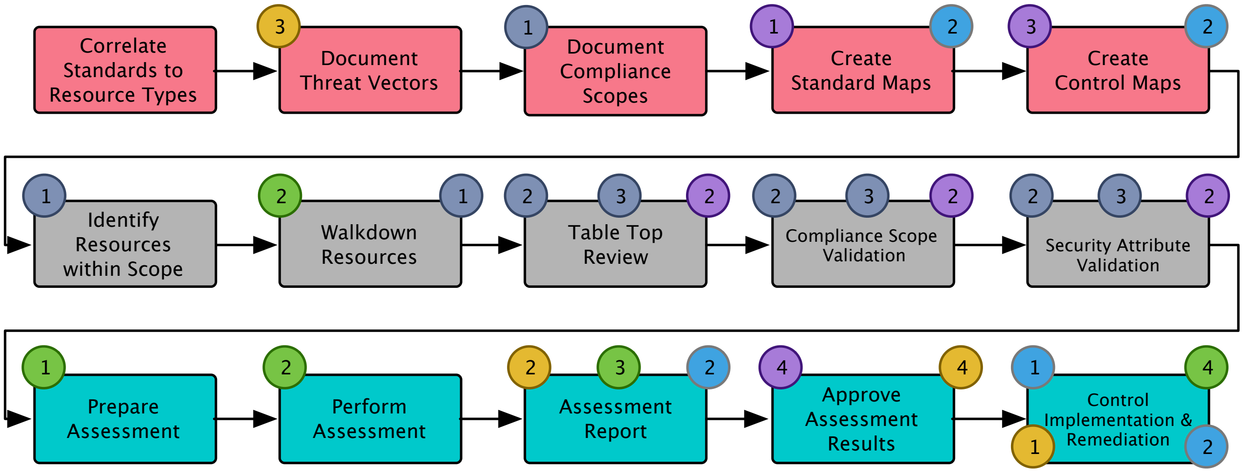
Notably absent is the tasks within the Monitor phase. This is intentional. The monitoring phase of technology security management is the most organization-dependent. Each organizations culture, personnel staffing levels, attitude toward out-sourcing or managed services, etc… will have a significant impact on how the monitoring phase is completed.

This document, with its focus on nuclear power plants, does not attempt to explain the intricacies of the Engineering Change, Corrective Action, Technical Specifications, Preventive Maintenance, Maintenance Rule and other nuclear power specific processes that will support ongoing security management.

The USM is designed to provide extremely efficient and effective processes for its first three phases, which correlate to the first five processes within the RMF Security Lifecycle, but leaves it to the implementing organizations to determine the best approach for the Monitor phase.

USM Lifecycle Tasks

The following diagram depicts the USM tasks and shows their corresponding RMF Security Lifecycle Tasks.


Correlate Standards to Resource Types
3
Document Threat Vectors
1
Document Compliance Scopes
1
2
Create Standard Maps
3
2
Create Control Maps
1
Identify Resources within Scope
2
1
Walkdown Resources
2
3
2
Table Top Review
2
3
2
Compliance Scope Validation
2
3
2
Security Attribute Validation
1
Prepare Assessment
2
Perform Assessment
2
3
2
Assessment Report
4
4
Approve Assessment Results
1
4
Control Implementation & Remediation
1
2

As can be seen, RMF Security Lifecycle tasks are addressed at different phases of the USM process.

The following table summarizes the USM tasks:

Phase	Name	Description
Analyze Standards	Correlate Standards to Resource Types	Review the security Standards provided in the source documents, e.g. RG 5.71/NEI 08-09, NEI 13-10, and/or NSS No 17, and determine which Resource Types they will be applied to.
	Document Threat Vectors	Review the source documents, e.g. RG 5.71/NEI 08-09, NEI 13-10, and/or NSS No 17 and document the specific Security Objectives, Attack Pathway, Exploitable Conditions, and determining Security Posture Attributes for each security Standard.
	Document Compliance Scopes	Review the source documents, e.g. RG 5.71/NEI 08-09, NEI 13-10, and/or NSS No 17, and document the classes of Resource, e.g. Critical Digital Asset, Level 4 Network, CSAT Members, that require protection. Document the specific Standards are applicable and the determining Compliance Scope Attributes.
	Create Standard Maps	Review the security Standards associated with each Compliance Scope and group them according to determining Security Posture Attribute, expected implementation mechanism (Control), and Security Objective.
	Create Control Maps	Review the Standard Maps and document the specific Control(s) that will be used to fulfill the Standards. Document the determining Security Posture Attributes for the Control Maps and the implementation status: Direct, Alternate, or Inherited. Additionally, Control Verification and Validation (Artifacts and Control Tests) can be identified for each Control.
Analyze Resources	Identify Resources within Scope	Review the equipment database to identify the Critical Systems and Critical Digital Assets supporting those systems. NEI 10-04 may be used to identify the criteria for inclusion in the program.
	Walkdown Resources	Physically inspect all CDAs and identify all supporting resources, i.e. connected networks, media, locations, software installed, managing organizations, etc… that require application of the relevant security Standards.
	TableTop Review	Review the results of the walk downs to ensure all Resources in scope have been identified and that an adequate understanding of the Resources Compliance Scope and Security Posture Attributes is known.
	Compliance Scope Validation	Review and approve all Compliance Scope Attributes for all identified Resources.
	Security Attribute Validation	Review and approve all Security Posture Attributes for all Resources within scope of the program.
Assess Security	Prepare Assessment	Identify the appropriate Compliance Scope Standard Maps who's Threat Vector(s) exist, determined by the Security Posture Attributes for the Resource. From the applicable Standard Maps, identify the Control Maps that will be used to fulfill the RG 5.71/NEI 08-09 requirements, based on Security Posture Attribute.

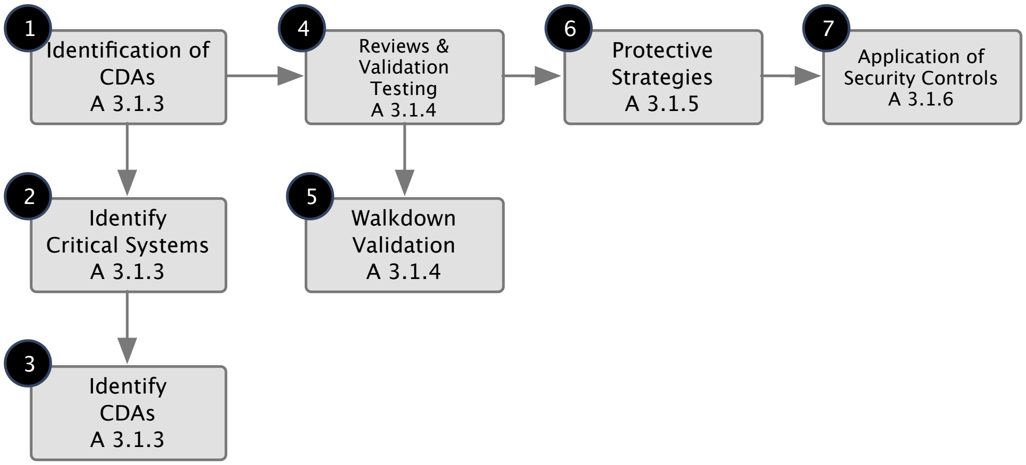
Phase	Name	Description
Assess Security	Perform Assessment	Review each distinct Control from all relevant Control Maps and determine the implementation status and optionally the disposition of the corresponding Artifact and Control Test.
	Assessment Report	Document all findings from the assessment, including both implemented and not-implemented Controls, the disposition of each Artifact and/or Control Test, and the recommended remediations, if required.
	Approve Assessment Results	Submit Assessment Report for CSAT approval and submission to Records Management.
	Control Implementation & Remediation	Identify all remediation activities required within the Corrective Action Program and plan for plant or procedure modifications as required.

Nuclear Cyber Security Processes

With this overview of the USM approach to the RMF Security Lifecycle, it is now time to turn our attention to the specifics within RG 5.71/NEI 08-09. The tasks within the RMF and the USM are much more complete than the security management tasks described in RG 5.71/NEI 08-09, NEI 13-10, and IAEA NSS No. 17. Each of those documents takes a much simpler approach, relying on overall process that transcend their specific purposes, provide the regulatory framework or technical guidance for technology security at nuclear power plants.

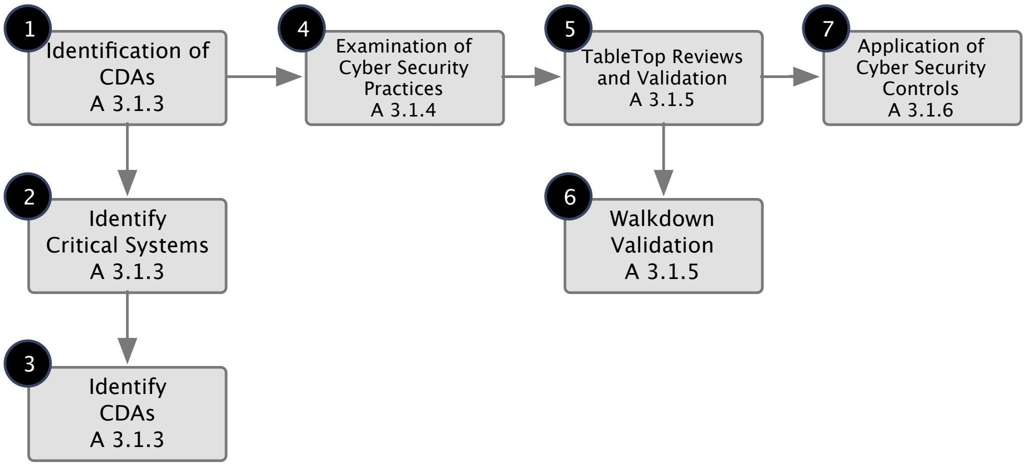
RG 5.71/NEI 08-09 Overall Process

The following diagram illustrates the process defined in Appendix A of RG 5.71.


1
Identification of CDAs A 3.1.3
2
Identify Critical Systems A 3.1.3
3
Identify CDAs A 3.1.3
4
Reviews & Validation Testing A 3.1.4
5
Walkdown Validation A 3.1.4
6
Protective Strategies A 3.1.5
7
Application of Security Controls A 3.1.6

This diagram illustrates the almost identical process defined within Appendix A of NEI 08-09:

As can be seen there are few differences, mostly semantic, visible from these diagrams in the overall process. Detailed information on the processes themselves can be found in the respective document.


1
Identification of CDAs A 3.1.3
2
Identify Critical Systems A 3.1.3
3
Identify CDAs A 3.1.3
4
Examination of Cyber Security Practices A 3.1.4
5
TableTop Reviews and Validation A 3.1.5
6
Walkdown Validation A 3.1.5
7
Application of Cyber Security Controls A 3.1.6

Implementation Differences

There is one key difference between the guidance provided by each of the documents 3.1.6 section.

RG 5.71 states:

> *With respect to technical security controls, [Licensee/Applicant] used the information collected in Section 3.1.4 of this plan to conduct one or more of the following for each CDA:*
>
> - *implementation of all of the security controls specified in Appendix B to RG 5.71*
> - ***for a security control that could not be applied**, implementation of alternative controls that eliminate threat/attack vectors associated with one or more of the security controls enumerated in Appendix B to RG 5.71 by:*
>   - *documenting the basis for employing alternative countermeasures*
>   - *performing and documenting an attack vector and attack tree analysis of the CDA and alternative controls to confirm that the countermeasures provide the same or greater protection as the corresponding security control identified in Appendix B to RG 5.71*
>   - *ensuring that the alternative controls provide at least the same degree of protection as the corresponding security control identified in Appendix B to RG 5.71*
> - *not implementing one or more of the security controls enumerated in Appendix B to RG 5.71 by:*
>   - *performing an attack vector and attack tree analyses of the specific security controls for the CDA that will not be implemented*
>   - *documenting that the attack vector does not exist (i.e., is not applicable), thereby demonstrating that those specific security controls are not necessary **[Emphasis Added]***

While NEI 08-09 provides:

> *1. Implementing the cyber security controls in Appendices D and E of NEI 08-09, Revision 6.*
>
> *2. **Implementing alternative controls/countermeasures that eliminate threat/attack vector(s)** associated with one or more of the cyber security controls enumerated in (1) above by:*
>
> > *a. Documenting the basis for employing alternative countermeasures;*
> >
> > *b. Performing and documenting the analyses of the CDA and alternative countermeasures to confirm that the countermeasures provide the same or greater cyber security protection as the corresponding cyber security control; and*
> >
> > *c. Implementing alternative countermeasures that provide at least the same degree of cyber security protection as the corresponding cyber security control;*
> >
> > *d. Implementing an alternative frequency or periodicity for the security control employed by documenting the basis for the alternate frequency or periodicity. The basis incorporates one or more of the following:*
> >
> > > *i. NRC Regulations, Orders*
> > >
> > > *ii. Operating License Requirements (e.g., Technical Specifications)*
> > >
> > > *iii. Site operating history*
> > >
> > > *iv. Industry operating experience*
> > >
> > > *v. Experience with security control*
> > >
> > > *vi. Guidance in generally accepted standards (e.g., NIST, IEEE, ISO)*
> > >
> > > *vii. Audits and Assessments*

viii. Benchmarking

ix. Availability of new technologies.

3. Not implementing one or more of the cyber security controls by:

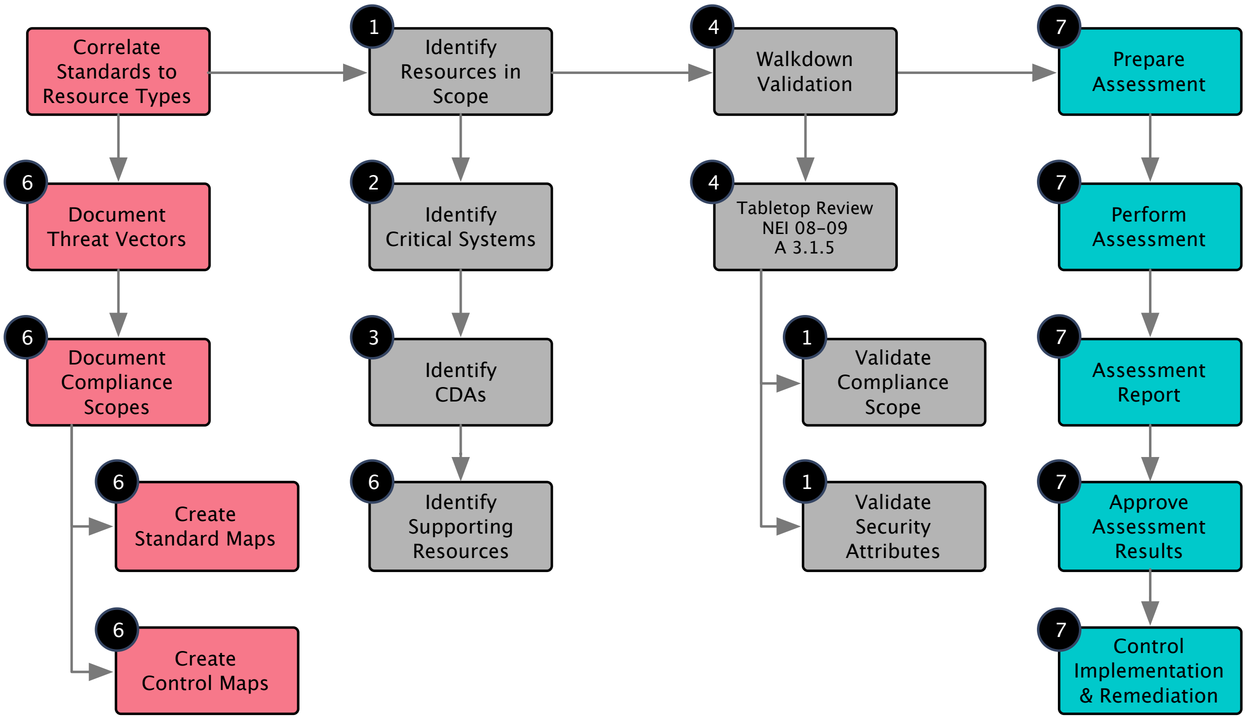
a. Performing an analysis of the specific cyber security controls for the CDA that will not be implemented

b. Documenting justification demonstrating the attack vector does not exist (i.e., not applicable) thereby demonstrating that those specific cyber security controls are not necessary.

NEI 08-09 lacks the language that prescribes that alternate controls may only been used when the actual control cannot be applied, though both documents provide for a blanket exception to applying controls if the control could negatively impact the SSEP functionality of the CDA.

USM Process for Implementing a Nuclear CSP

This diagram illustrates the USM approach to these processes, complete with the corresponding number of the RG 5.71 process above:


Correlate Standards to Resource Types
6 Document Threat Vectors
6 Document Compliance Scopes
6 Create Standard Maps
6 Create Control Maps
1 Identify Resources in Scope
2 Identify Critical Systems
3 Identify CDAs
6 Identify Supporting Resources
4 Walkdown Validation
4 Tabletop Review NEI 08-09 A 3.1.5
1 Validate Compliance Scope
1 Validate Security Attributes
7 Prepare Assessment
7 Perform Assessment
7 Assessment Report
7 Approve Assessment Results
7 Control Implementation & Remediation

The USM approach is characterized by the front-loaded analysis performed. While this analysis cannot be 100% complete prior to performing the assessments themselves, much of the Standard and Control analysis is possible early on, as there are only so many possible ways, regardless of the Resource population specifics to implement the vast majority of the security Standards.

Implementation Guidance

The overall approach within the USM is to format the **information** in the source documents into **structured data** that can be consistently communicated and consumed throughout the organization. Structuring the data can take many different forms, a commercial security management automation solution such as cmplid:// is the best approach, but other mechanisms such as commercial GRC metrics aggregators or simple assessment tools, internally developed databases, and spreadsheets can suffice. The efficiencies and effectiveness of the USM can be realized over traditional analysis methods regardless of the implementing technology.

The most important principle to remember is this:

> If your process is flawed, automated tools will only help you do flawed work quicker.

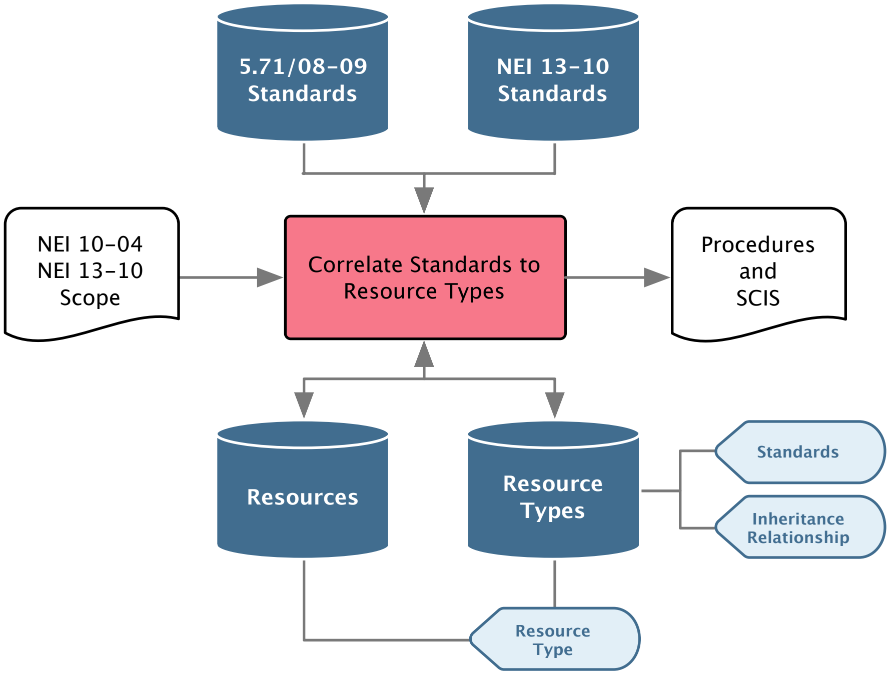
Many organizations have learned this over the last few years, there has been much re-work in the nuclear cyber security space in the US, as organizations have used and abandoned tools that did not support a competent process.

The following sections provide a more detailed breakdown of the USM tasks for implementing a nuclear CSP. Some of the sections provide high-level diagrams of the recommended data structure, through they are not detailed DB design information.

Analyze Standards

Correlate Standards to Resource Types

Review the security Standards provided in the source documents, e.g. RG 5.71/NEI 08-09, NEI 13-10, and/or NSS No 17, and determine which Resource Types they will be applied to.



This process starts with the Standards in structured data and results structured data definitions for the Resource Types and Resources.

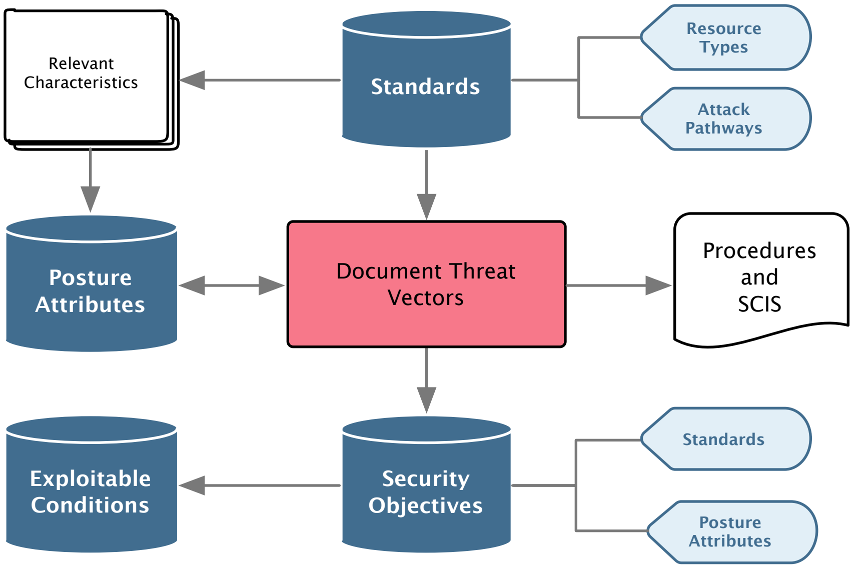
The output of this process will provide the the high level structure of the organizations procedures and the foundation of the Security Control Implementation Strategy (SCIS).

The following examples are of RG 5.71 Standards associated to resource types:

Standard	Applicable Resource Types
B.4.1 Identification and Authentication Policies and Procedures	Organization
B.4.3 Password Requirements [Licensee/Applicant] ensures that, where used, passwords meet the following requirements:	Hardware, Software
C.3.3 Malicious Code Protection [Licensee/Applicant] established, deployed, and documents real-time malicious code protection mechanisms at security boundary device entry and exit points, CDAs (if applicable), workstations, servers, and mobile computing devices (i.e., calibrators) on the network to detect and eradicate malicious code resulting from the following:	Network, Hardware
C.3.9 Error Handling: Inclusion of sensitive information, such as passwords, in error logs or associated administrative messages is prohibited.	Source Code
C.1.5 Media Transport [Licensee/Applicant] physically protects and stores CDA media in transport in a manner commensurate with the sensitivity of the data.	Media
C.5.3 Physical and Environmental Protection	Location
C.10.4 Specialized Cyber Security Training	Personnel

Document Threat Vectors

Review the Standards from the source documents, e.g. RG 5.71/NEI 08-09, NEI 13-10, and/or NSS No 17 and document the specific Security Objectives, Attack Pathway, Exploitable Conditions, and determining Security Posture Attributes for each security Standard.



This process is unique to the USM. There is no definition of Threat Vector in any of the NRC developed or endorsed documents. There is a definition for the Attack Pathways, but they alone are insufficient to determine the necessity of the CSP Standards.

Essentially, the USM provides this as the definition of a Threat Vector:

The combination of a required Security Objective, a negative impact of Exploitation of a Condition present, and the presence of an Attack Pathway, for a Resource in scope of the program. There are five NRC defined Attack Pathways, but the USM prescribes 2 additional ones for completeness:

1) Direct Network Connectivity

2) Wireless Network Capability

3) Portable Media and Equipment

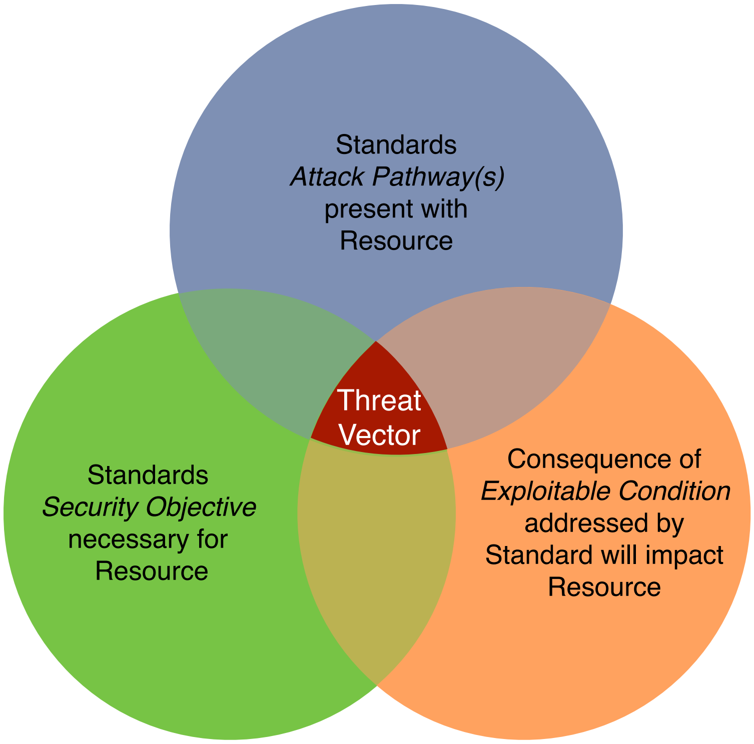
4) Supply Chain

5) Direct Physical Access

6) (USM) Human Performance

7) (USM) Entropy

The following is a diagram of the required elements of a Threat Vector.



If any of these elements is not present for a Resource, the corresponding security Standards are determined to be unnecessary, as the Threat Vector does not exist.

Each of these three components of a Threat Vector can be determined by defining Security Posture Attributes. These Security Posture Attributes are derived from the Standards themselves.

Consider the examples from the Resource Type analysis above:

B.4.1 Identification and Authentication Policies and Procedures

Security Objectives	Exploitable Condition	Determining Security Posture Attributes
Ensures organizational personnel understand their roles and responsibilities for securing resources within scope of the security program.	Resources within scope of the security program will be inconsistently managed according to personnel specific proclivities or ‘tribal knowledge.’	Human Performance:True
Ensures resources within scope of the security program are developed, implemented, and maintained according to appropriate organizationally defined standards.	Resources within scope of the security program will be inconsistently managed according to personnel specific proclivities or ‘tribal knowledge.’	Human Performance:True

B.4.3 Password Requirements: [Licensee/Applicant] ensures that, where used, passwords meet the following requirements:

Security Objectives	Exploitable Condition	Determining Security Posture Attributes
Ensures Logical User Interaction is limited to appropriate users.	Logical user account authentication mechanisms can be derived through brute-force or dictionary-based attacks.	Weak Authentication Mechanism: True

C.3.3 Malicious Code Protection: [Licensee/Applicant] established, deployed, and documents real-time malicious code protection mechanisms at security boundary device entry and exit points, CDAs (if applicable), workstations, servers, and mobile computing devices (i.e., calibrators) on the network to detect and eradicate malicious code resulting from the following:

Security Objectives	Exploitable Condition	Determining Security Posture Attributes
Ensures malicious code cannot propagate or execute within the technology infrastructure.	Malicious code will be used to compromise organizational resources.	Firewall Boundary: True Hardware Contains Communications Ports:True Defensive Strategy Network: True

C.3.9 Error Handling: Inclusion of sensitive information, such as passwords, in error logs or associated administrative messages is prohibited.

Security Objectives	Exploitable Condition	Determining Security Posture Attributes
Ensures that security relevant information that must be protected from unauthorized disclosure is protected.	Compromise of sensitive information.	Stores Sensitive Information: True Transmits Sensitive Information: True

C.1.5 Media Transport: [Licensee/Applicant] physically protects and stores CDA media in transport in a manner commensurate with the sensitivity of the data.

Security Objectives	Exploitable Condition	Determining Security Posture Attributes
Ensures that security relevant information that must be protected from unauthorized disclosure is protected.	Compromise of sensitive information.	Stores Sensitive Information: True

C.5.3 Physical and Environmental Protection

Security Objectives	Exploitable Condition	Determining Security Posture Attributes
Ensures all personnel granted access to resources are authorized and appropriately screened.	Unauthorized personnel will gain access to protected resources.	Contains CDAs: True

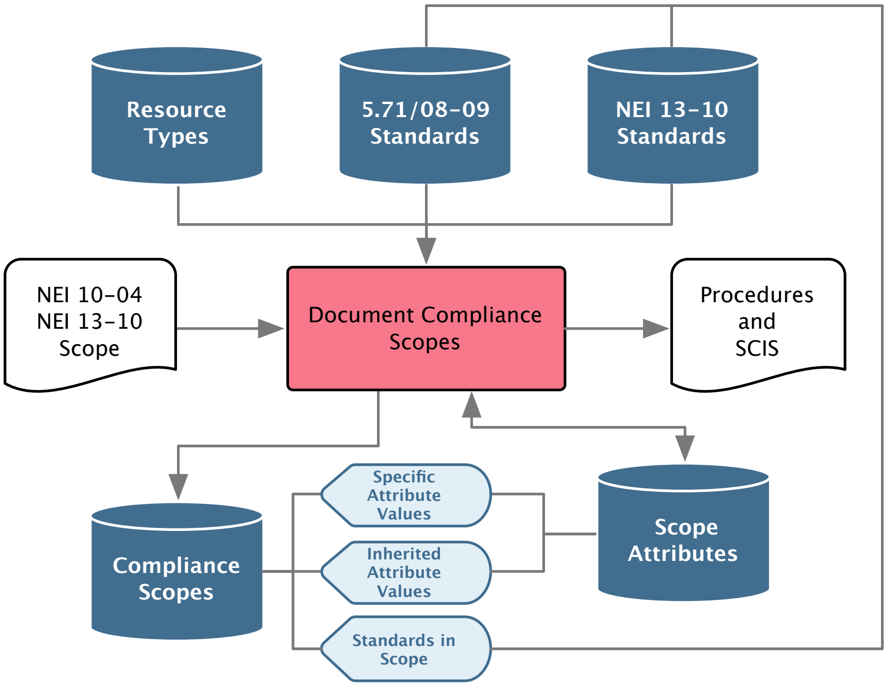
C.10.4 Specialized Cyber Security Training

Security Objectives	Exploitable Condition	Determining Security Posture Attributes
Ensures organizational personnel understand their roles and responsibilities for securing resources within scope of the security program.	Resources within scope of the security program will be inconsistently managed according to personnel specific proclivities or 'tribal knowledge.'	Human Performance:True

Each of these statements are simple and to the point. There is no need to overcomplicate this analysis.

Document Compliance Scopes

Review the source documents, e.g. RG 5.71/NEI 08-09, NEI 13-10, and/or NSS No 17, and document the classes of Resource, e.g. Critical Digital Asset, Level 4 Network, CSAT Members, that require protection. Document the specific Standards are applicable and the determining Compliance Scope Attributes.



This task builds on the previous two tasks. Reviewing the individual Standards and correlating them to defined Compliance Scopes, or classes of Resources, defined within the source documents that require protection.

The following table provides a partial list of the Compliance Scopes that may be defined for a cyber security program based on RG 5.71/NEI 08-09:

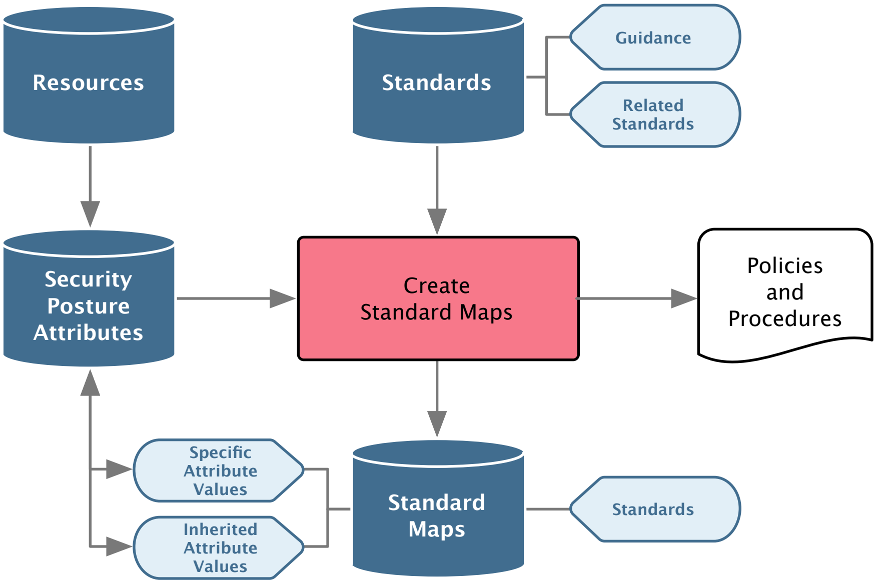
Name	Description	Resource Type	Determining Scope Attributes
Critical Digital Asset	CDAs that could have a direct impact on Critical Systems.	Hardware Software	10-04 CDA Attributes
Direct Impact Critical Digital Asset	CDAs that could have a direct impact on Critical Systems.	Hardware Software	Relevant 13-10 Consequence Analysis Attributes
Indirect BOP Critical Digital Asset	CDAs that solely support a BOP Functional Resource Group and whose compromise or failure could cause a SCRAM or Trip.	Hardware Software	Relevant 13-10 Consequence Analysis Attributes
Level 3 Network	Level 3 networks containing CDAs.	Network	Network Level: Level 3

Name	Description	Resource Type	Determining Scope Attributes
CSAT Personnel	Personnel on the Cyber Security Assessment Team	Personnel Groups	Group Role: CSAT
Protected Area	Protected Area Location with Critical Digital Assets	Location	Location Type: PA
Firewall Boundary	CDAs that are components of a firewall network boundary.	Hardware Software	Provides Defensive Strategy Bi-directional Boundary: True

The Determining Scope Attributes listed above for the Compliance Scopes CDA, Direct Impact CDA, and Indirect BOP CDA are summaries of the actual Scope Attributes defined for these Compliance Scopes for brevity.

Create Standard Maps

Review the security Standards associated with each Compliance Scope and group them according to determining Security Posture Attribute, expected implementation mechanism (Control), and/or Security Objective.



This is the task that produces the most efficiency within the USM. In all security programs there is a measure of redundancy and ambiguity within the prescribed Standards. This is pronounced in RG 5.71/NEI 08-09 as they are based on the NIST SP 800-53 Security Control Library, which is extremely granular and complete in nature.

This granularity however useful, has a price when it comes to the implementation of the program. Standard Maps are simply groups of these security requirements prescribed that consolidate the requirements into a smaller set of requirements that must be evaluated, communicated, and managed.

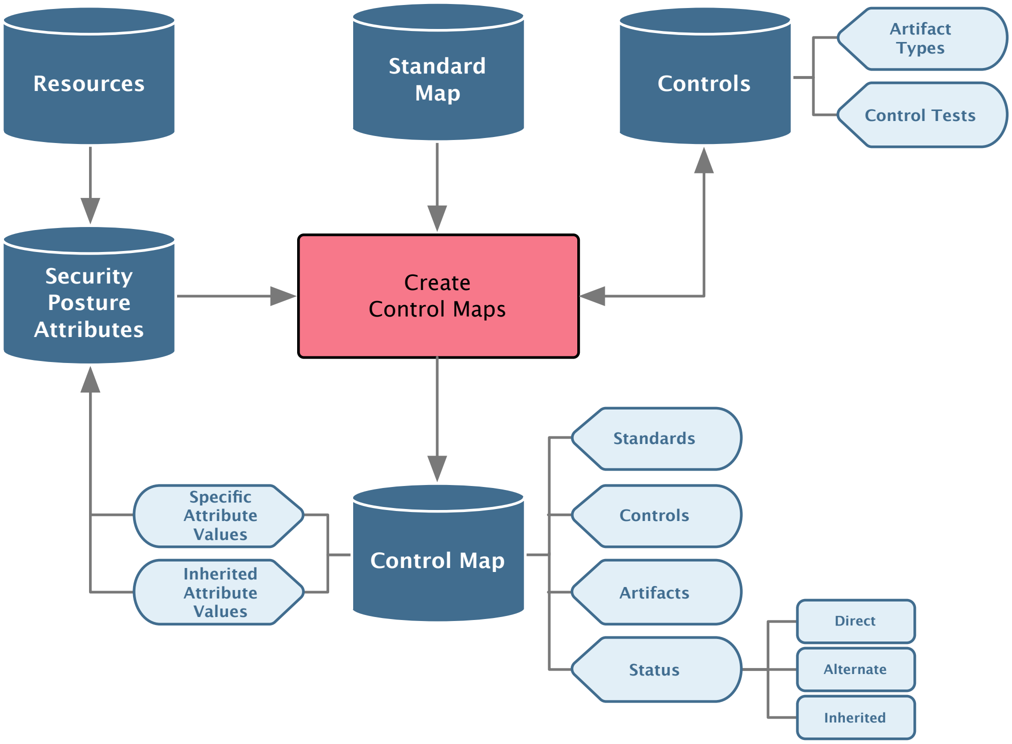
The following table provides examples of Standard Maps from the Direct Impact Critical Digital Asset Compliance Scope (Note: Standards referenced are the NEI 08-09 equivalents of the RG 5.71 Standards):

Text	Determining Posture Attributes
D 1.2 a1 This technical cyber security control: Manages and documents CDA accounts, including authorizing, establishing, activating, modifying, reviewing, disabling, and removing accounts. D 1.2 a2 This technical cyber security control: Reviews CDA accounts consistent with the access control list provided in the design control package, access control program, cyber security procedures and initiates required actions on CDA accounts at least every 31 days. D 1.2 a4 This technical cyber security control: Conducting reviews when as individuals job function changes to ensure that rights remain limited to the individuals job function D 1.2 a5 (iii) This technical cyber security control: Employs computerized mechanisms that support CDA account management functions. The CDA will automatically: Create and protect audit records for account creation, deletion and modification, D 1.2 a5 (iv) This technical cyber security control: Employs computerized mechanisms that support CDA account management functions. The CDA will automatically: Document and notify system administrators of account creation, deletion and modification activities. This is to make system administrators aware of any account modifications and can investigate potential cyber attacks. D 4.1 b7 The identification and authentication policy and procedures provide guidance on managing both user identifiers and CDA authenticators. These items include: Defining initial authenticator content,	End-User Defined Accounts Include Specific (Hardware, Software) Logical User Configuration: End-user defined accounts and permissions OR Logical User Configuration: Static permissions associated with end-user defined accounts
D 1.6 a2 This technical cyber security control: Configures CDAs to enforce the most restrictive set of rights/privileges or access needed by users. D 4.1 b1 The identification and authentication policy and procedures provide guidance on managing both user identifiers and CDA authenticators. These items include: Uniquely identifying users, and processes acting on behalf of a user, D 4.1 b2 The identification and authentication policy and procedures provide guidance on managing both user identifiers and CDA authenticators. These items include: Verifying the identity of users, and processes acting on behalf of a user, D 4.2 a1 This technical cyber security control: Implements identification and authentication technology to uniquely identify and authenticate individuals and processes acting on behalf of users interacting with CDAs. Ensure that CDAs, security boundary devices, physical controls of the operating environment, and individuals interacting with CDAs, are uniquely identified and authenticated and that processes acting on behalf of users are equally authenticated and identified. D 4.6 a1 This technical cyber security control manages and documents user identifiers by performing the following: Uniquely identifying users;	Logical User Interaction Include Specific (Hardware, Software) Logical User Interaction: Users may access operational parameter menus through a proprietary HMI OR Logical User Interaction: Users may access operational parameters through normal IT peripherals via a distinct application installed on the device OR Logical User Interaction: Users may access the OS or firmware through normal IT peripherals via a command shell, Graphical User Interface, or similar

Text	Determining Posture Attributes
D 4.3 a1 This technical cyber security control ensures that when used, passwords meet the following requirements: Length, strength, and complexity of passwords balance security and operational ease of access within the capabilities of the CDA. D 4.3 a2 This technical cyber security control ensures that when used, passwords meet the following requirements: Passwords have length and complexity for the required security. D 4.3 a4 This technical cyber security control ensures that when used, passwords meet the following requirements: Passwords cannot be found in a dictionary and do not contain predictable sequences of numbers or letters.	Password Authentication Include Specific (Hardware, Software) Authentication Mechanism: Passwords
D 1.12 a1 This technical cyber security control: Identifies and documents specific user actions that can be performed on CDAs during normal and emergency conditions without identification or authentication. D 1.12 a2 This technical cyber security control: Permits actions to be performed without identification and authentication to the extent necessary to accomplish mission objectives, without adversely affecting safety, security, and emergency preparedness functions.	Access Prior to Authentication Include Specific (Hardware, Software) Logical User Interaction: Users may access operational parameter menus through a proprietary HMI OR Logical User Interaction: Users may access operational parameters through normal IT peripherals via a distinct application installed on the device OR Logical User Interaction: Users may access the OS or firmware through normal IT peripherals via a command shell, Graphical User Interface, or similar OR Access Prior to Authentication: Yes
D 3.12 a: This technical cyber security control ensures public key certificates are issued under a certificate policy or obtains public key certificates under a certificate policy from an approved provider.	PKI Used Include Specific (Hardware, Software) Utilizes PKI Infrastructure: Yes

Create Control Maps

Review the Standard Maps and document the specific Control(s) that will be used to fulfill the Standards. Document the determining Security Posture Attributes for the Control Maps and the implementation status: Direct, Alternate, or Inherited. Additionally, Control Verification and Validation (Artifacts and Control Tests) can be identified for each Control.



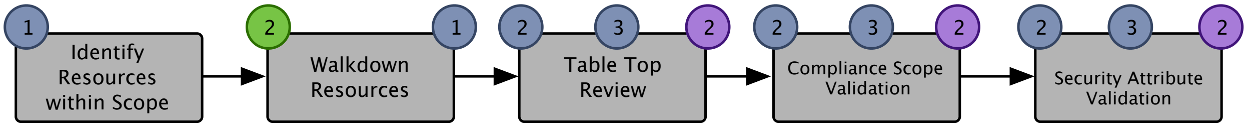
This is the most complex, and yet most important task of all. This task ensures that the implementation of the program and management of the Resources within scope I can be accomplished with consistency and clarity, and can be communicated effectively to responsible personnel. The following table contains examples of Control Maps for Nuclear Cyber Security:

Standard Map	Controls	Status	Determining Posture Attributes
Account Management	Audit process automatically creates and protects audit records for account creation, deletion and modification. Notifications are sent to system administrators and records are maintained of account creation, deletion and modification activities.	Direct	Automated Account Management Include Specific (Hardware, Software) Automated Account Management: Yes
Account Management	All user accounts are reviewed and inactive accounts are disabled according to fleet or site guidelines.	Alternate	Manual Account Management Include Specific (Hardware, Software) Automated Account Management: No

Standard Map	Controls	Status	Determining Posture Attributes
Authentication	All users are required to authenticate prior to gaining access to the Resource	Direct	Authentication Supported Include Specific (Hardware, Software) Authenticates Users: Yes
Authentication	The Resource is located within a Vital Area or a locked and monitored (tamper-switched, continuous video monitoring, Security Officer/Operations rounds patrolled area) within a PA, OCA, or other location minimally secured to the level required by the CSP Appendix E 5 Controls. All personnel granted logical or physical access to this Resource have completed both User Awareness Training and all Technical Training relevant to their responsibilities for the Resource. Hardware must be located on a Level 3 or air-gapped network and may not be directly connected to any network with a security level other than the Hardware's. All personnel granted unescorted physical access to this Resource have been approved through the UAA program, and are subject to both the Fitness For Duty Program and the Behavioral Observation Program. A Surveillance or Preventive Maintenance check exists for this Resource and is executed according to a documented schedule appropriate for the criticality of the Resource and the physical and logical exposure to cyber attack.	Inherited	No Authentication Include Specific (Hardware, Software) Authentication Mechanism: No logical access control (due to adverse impact to SSEP, or lack of support)
Invalid Authentication Attempt Locking	Hardware is configured to lock account access whenever an incorrect password is entered according to the configuration capabilities.	Direct	Invalid Login Attempt Locking Include Specific (Hardware, Software) Authentication Mechanism Protections: Invalid Login Attempt Locking
Integrity Verification	At an approved periodicity, the integrity and functionality of the hardware and software configuration is verified by performing a defined PM or surveillance.	Alternate	No Integrity Verification Exclude Specific (Hardware, Software) Automated Integrity Verification Tools: None

Analyze Resources

The first phase, Analyze Standards, is by far the most complex, time consuming, and ***requires significant technology security expertise.*** This front-loaded analysis however, ensures that the next two phases are well-defined, understood, and extremely efficient.


1
Identify Resources within Scope
2
Walkdown Resources
1
2
Table Top Review
3
2
2
Compliance Scope Validation
3
2
2
Security Attribute Validation
3
2

Identify Resources within Scope

Review the equipment database to identify the Critical Systems and Critical Digital Assets supporting those systems. NEI 10-04 may be used to identify the criteria for inclusion in the program.

Walk down Resources

Physically inspect all CDAs and identify all supporting resources, i.e. connected networks, media, locations, software installed, managing organizations, etc… that require application of the relevant security Standards.

The USM provided documentation of the Compliance Scope Attributes and Security Posture Attributes is a key input to this task. That information effectively provides boundaries for the RG 5.71/NEI 08-09 guidance in Sections 3.1.4 and 3.1.5 and ensures both that a) all information required is gathered during the walk downs and that b) irrelevant information that could cause confusion or consume resources can be identified and discarded. Generally, licensees will create a Walk down Report documenting the information gathered.

Tabletop Review

Review the results of the walk downs to ensure all Resources in scope have been identified and that an adequate understanding of the Resources Compliance Scope and Security Posture Attributes is known.

The tabletop review is designed to provide the small group of designated assessors for a given Resource or the full Cyber Security Assessment Team to review the information gathered in the walk down within the context of the Standards analysis phase. Generally, licensees will create a Tabletop Review Record that is entered into their records management system.

Compliance Scope Validation

Review and approve all Compliance Scope Attributes for all identified Resources.

The Compliance Scope Attributes relevant to the Resources are reviewed to ensure that the answers are correct and that appropriate justification is documented to determine the scope of the Resources. Generally, licensees will create a CDA Determination or similar Compliance Scope Validation Record that is entered into their records management system.

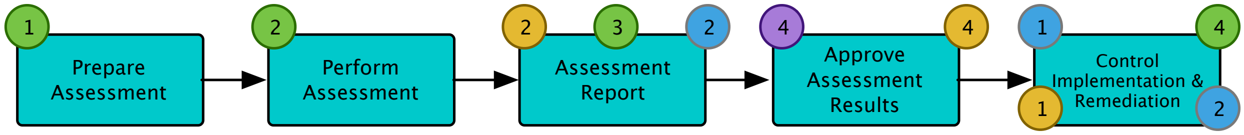
Security Attribute Validation

Review and approve all Security Posture Attributes for all Resources within scope of the program.

The Security Posture Attributes relevant to the Resources are review to ensure that the answers are correct and that appropriate justification is documented. Generally, licensees will incorporate this information into the finalized Tabletop Review Record.

Assess Security

The first phase, Analyze Standards, is by far the most complex, time consuming, and ***requires significant technology security expertise.*** This front-loaded analysis however, ensures that the next two phases are well-defined, understood, and extremely efficient.



Prepare Assessment

Identify the appropriate Compliance Scope Standard Maps who's Threat Vector(s) exist, determined by the Security Posture Attributes for the Resource. From the applicable Standard Maps, identify the Control Maps that will be used to fulfill the RG 5.71/NEI 08-09 requirements, based on Security Posture Attribute.

Perform Assessment

Review each distinct Control from all relevant Control Maps and determine the implementation status and optionally the disposition of the corresponding Artifact and Control Test.

Assessment Report

Submit Assessment Report for CSAT approval and submission to Records Management.

Control Implementation & Remediation

Identify all remediation activities required within the Corrective Action Program and plan for plant or procedure modifications as required.

Incorporating Risk Management

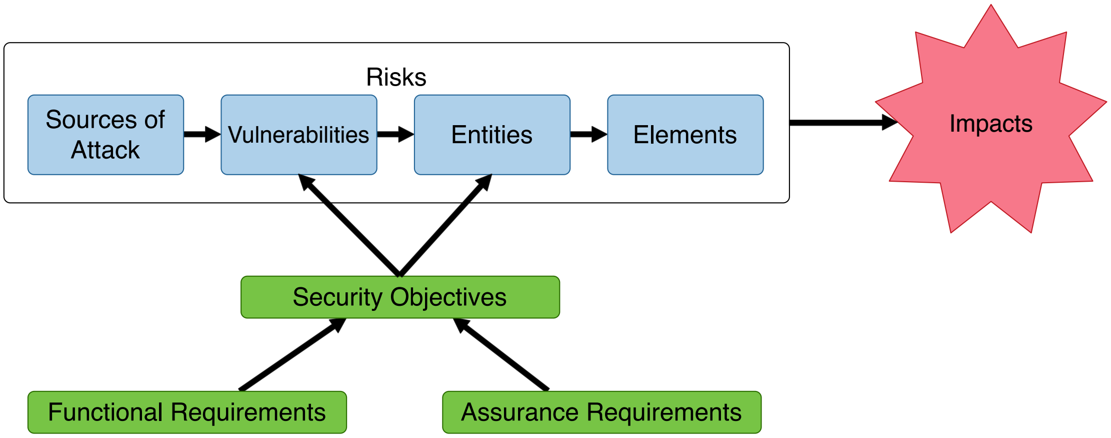
CSPs governed by RG 5.71/NEI 08-09 do not incorporate or require risk analysis, the Threat Vector analysis is all that is required in order to comply with the plans. Nuclear licensee's who want to include risk analysis into their programs as part of maturing those programs over time, could look at the guidance within IAEA NSS No 17.

This paper is not intended to give detailed risk analysis guidance, however a brief discussion of risk analysis is warranted within the context of IAEA NSS No 17. The key difference between the RG 5.71/NEI 08-09 processes and the IAEA NSS No 17 prescribed process is the real absence of risk analysis in the former.

Both the RG 5.71 and NEI 08-09 processes are Threat Vector based and exclusive in nature, the security Standards provided in their respective Appendices (A, B, & C and A, D, & E) are required unless analysis determines that the Threat Vectors do not exist, thereby excluding the Standards from applicability. Neither RG 5.71 nor NEI 08-09 prescribe any process that reasonably resembles any of the popular risk analysis processes, the sections on Risk Management in appendix C of RG 5.71 and E of NEI 08-09 are really nothing more than vulnerability management. Furthermore, neither document defines the term Threat Vector, the definition used throughout this document is cmplid://'s definition.

The IAEA NSS No 17 process however is risk-based and inclusive in nature, requiring implementing organizations to document analysis that requires the inclusion of security controls.

The following diagram illustrates the process, based on the French EBIOS risk analysis method, for determining that security controls are required:


Risks
Sources of Attack
Vulnerabilities
Entities
Elements
Impacts
Security Objectives
Functional Requirements
Assurance Requirements