Technical Discussion on the Fuel Cyber Security Proposed Rulemaking

Public Meeting

Thursday December 10, 2015

Fuel Cycle Cyber Security Rulemaking Working Group

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Agenda

- Introductory questions
- Risk Management Framework
- Consequence analysis and screening examples
- Discussion on control sets
- Staff approach to drafting rule language
- Questions

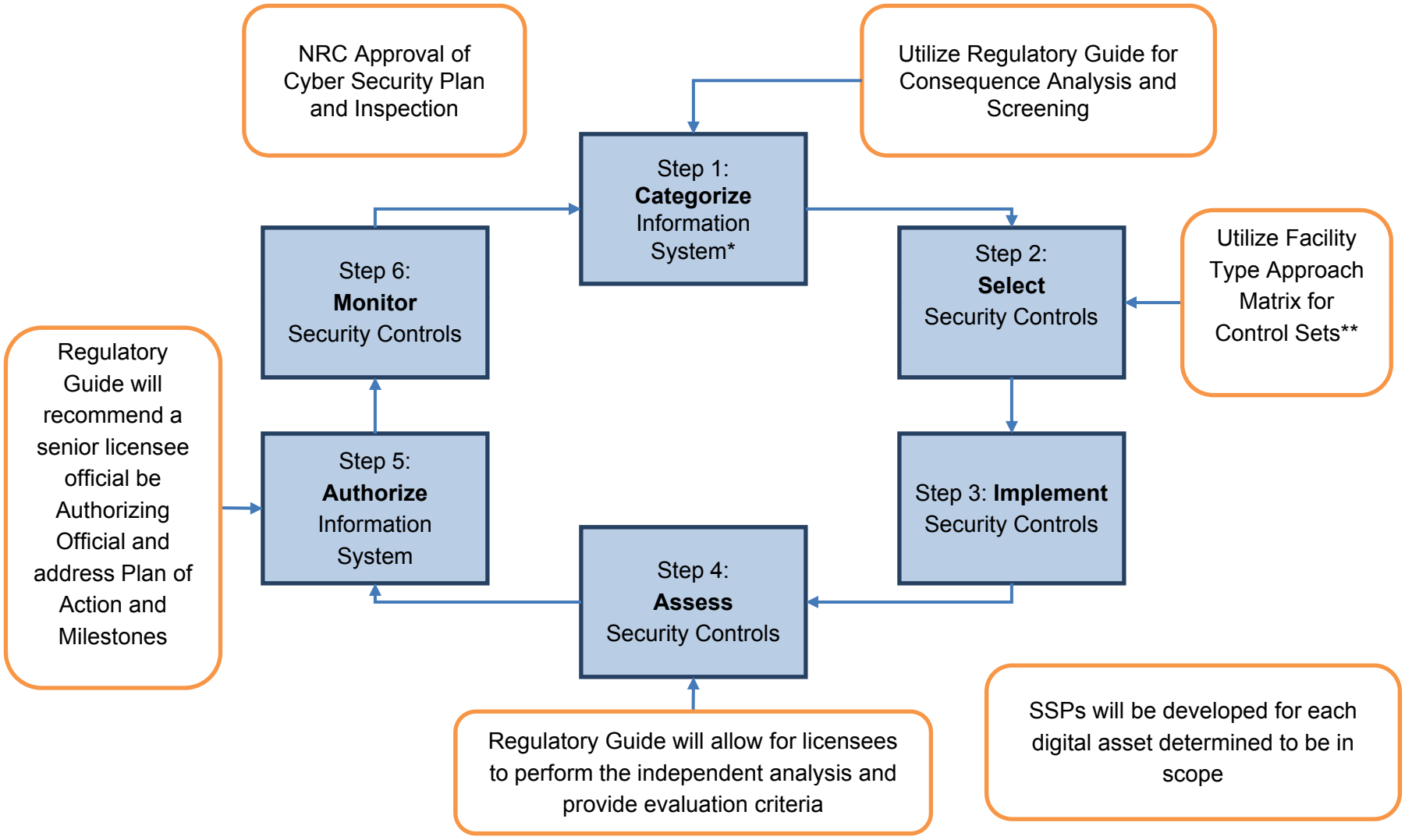
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Introductory Questions

- What concerns, if any, do you have with the staff's approach?
- Are there aspects that appear to be overly complicated or confusing?
- Are there aspects in which we have common ground?

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Figure 5 - Risk Management Framework



*Evaluate each digital asset, group of digital assets, or information system. **Tailor each control consistent with NIST guidance.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Step 1: Categorize Information Systems

INPUT: Security Plans/Orders, FNMC Plan, ISAs/IROFS, Process and Operational Controls

- Perform analyses to determine digital assets associated with active and latent consequences of concern
- Determine digital assets associated with 3S (safety, security, safeguards) functions
- Apply screening methodology to consider equivalent function by alternate means
- Document justification for assets screened out in this fashion

OUTPUT: List of in-scope digital assets

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Discussion on Technical Issues Document Questions

What is the U.S. Nuclear Regulatory Commission (NRC) staff trying to prevent? (Question 1)

What are the consequences of concern under consideration to address safety, security, and safeguards (3S) functions? (Question 2)

What are the thresholds related to the consequence of concern for 3S functions? (Question 3)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Discussion on Technical Issues Document Questions

How is the draft approach risk-informed and consequence based? (Question 5)

How is the draft approach graded and performance-based? (Question 6)

What digital assets are currently anticipated to be evaluated as part of the rule? (Question 7)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Table 1 - Consequences of Concern

Function and (Applicability)	Consequence of Concern	Thresholds	Examples of Digital Assets within Scope for Screening*
Safety (Applies to all FCFs)	Significant exposure events which could endanger the life of workers or could lead to irreversible or other serious, long-lasting health effects to workers or members of the public (e.g., nuclear criticalities and releases of radioactive materials or chemicals).	Radiological exposure: - 25 rem or greater worker; - 25 rem or greater or 30 mg or greater intake of uranium in soluble form outside the controlled area (any individual). Acute chemical exposure: - Could lead to irreversible or other serious, long lasting health effects to a worker or any individual located outside the controlled area	Digital assets associated with significant exposure events which may include: - Operational and process controls (i.e., analysis determines that compromise results in a significant exposure event). [Active] - Digital assets associated with preventing and mitigating significant exposure events (e.g., IROFS). [Latent] - Digital assets with a nexus to a significant exposure event (e.g., Security, MC&A). Security digital assets required in response to Security Orders (e.g., ICM, ASM). [Latent]
Security of SSNM (Applies to Cat I's)	Radiological Sabotage and Theft or Diversion of Formula Quantities of SSNM.	Loss of the capability to protect against the DBTs as defined in: - 10 CFR 73.1(a)(1) Radiological Sabotage - 10 CFR 73.1(a)(2) Theft or Diversion of Formula Quantities of SSNM.	Digital assets associated with protecting against the DBTs. [Latent] - Security Plans - Security Orders
Security and Safeguards of SSNM (Applies to Cat I's)	Loss of control and accounting of Formula Quantities of SSNM	Loss of the capability to: -Timely detect the possible abrupt loss of five or more formula kilograms of SSNM from an individual unit process; - Rapidly determine whether an actual loss of five or more formula kilograms occurred; - Continually confirm the presence of SSNM in assigned locations; and - Timely generate information to aid in the recovery of SSNM in the event of an actual loss.	Digital assets associated with control and accounting of Formula Quantities of SSNM. [Latent] - Security Plans - FNMC Plan - Security Orders

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Table 1 - Consequences of Concern (continued)

Function and (Applicability)	Consequence of Concern	Thresholds	Examples of Digital Assets within Scope for Screening*
Security of SNM of Moderate Strategic Significance (Applies to Cat I and II)	Unauthorized removal of special nuclear material of moderate strategic significance	Loss of the capability to: - Detect, assess and respond to unauthorized access or activities within controlled areas containing SNM of moderate strategic significance.	Digital assets associated with unauthorized removal of SNM of moderate strategic significance. [Latent] - Security Plans - FNMC Plan - Security Orders
Security and Safeguards of SNM of Moderate Strategic Significance (Applies to Cat I and II)	Loss of control and accounting of SNM of moderate strategic significance	Loss of the capability to: - Maintain accurate, current, and reliable information on, and confirm, the quantities and locations of SNM; - Permit rapid determination of whether an actual loss of a significant quantity of SNM has occurred, with significant quantity being either: More than one formula kilogram of strategic SNM; or 10,000 grams or more of uranium-235 contained in uranium enriched up to 20.00 percent. - Generate information to aid in the investigation and recovery of missing SNM in the event of an actual loss.	Digital assets associated with control and accounting of SNM of moderate strategic significance. [Latent] - Security Plans - FNMC Plan - Security Orders
Physical Security of Classified Information (Applies to FCF's with a Part 95 FSC or NRC is the CSA)	Loss or unauthorized disclosure of classified information	Loss of the capability to protect classified information.	Digital assets associated with physical security of classified information. [Latent] - Standard Practices and Procedures Plan - Security Plans

*The digital assets within scope may also include: support systems equipment which, if compromised, would adversely impact 3S functions; and cyber security features needed to meet commitments in the cyber security program.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Discussion on Technical Issues Document Questions

How are the design basis threats (DBTs) factored into the determination of digital assets within scope of the rule? (Question 10)

How is the consequence analysis performed? (Question 11)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Latent Consequence Analysis

The purpose of a “latent analysis” is to identify those digital assets that, if compromised, could fail to prevent, mitigate, or respond to a 3S event associated with a consequence of concern.

The licensee is encouraged to use any of the following to identify those digital assets that perform or support a 3S function from the:

- ISA (categorize IROFS as “digital/non-digital” before considering accident sequences);
- Security order commitments and physical security plan;
- Standard Practices and Procedures Plan; and
- Fundamental Nuclear Material Control Plan.

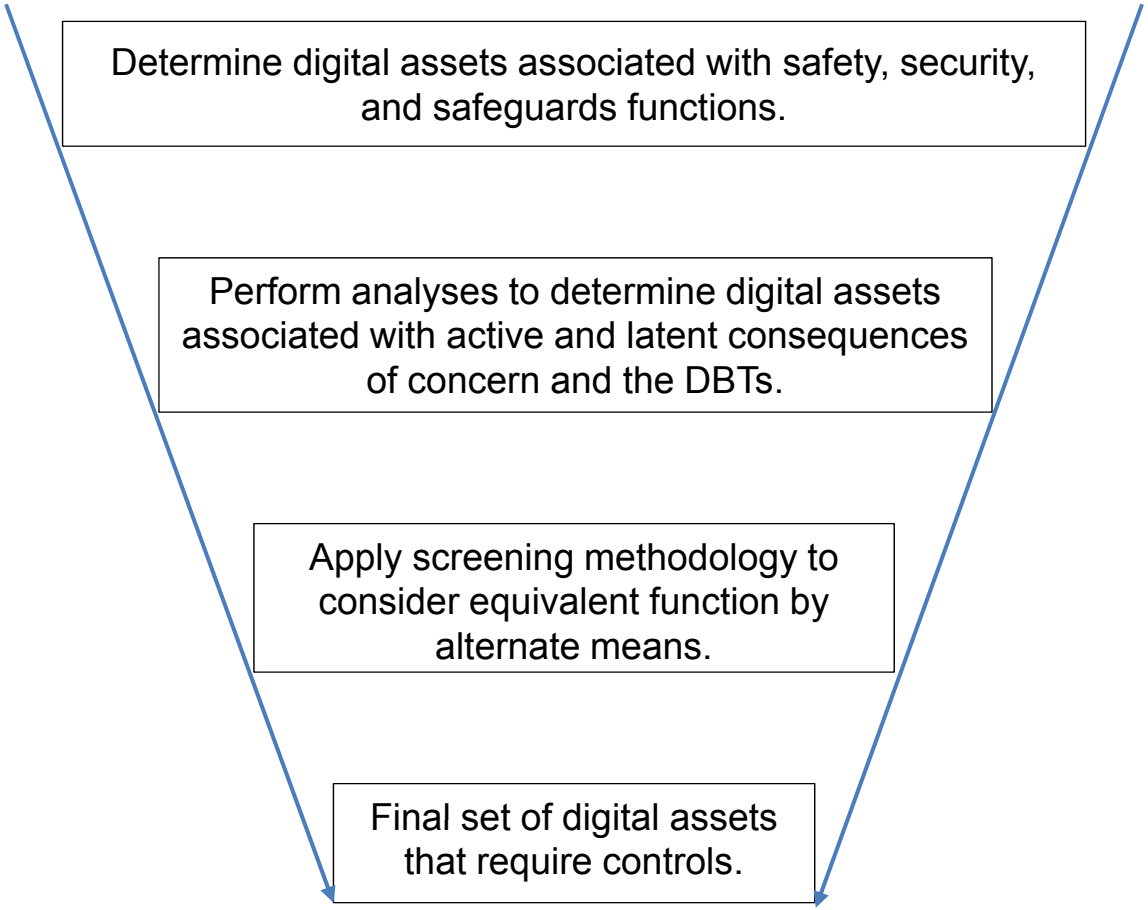
For this analysis, a licensee will group the digital assets based on the function type (e.g., safety, security and safeguards of SSNM (or DBT), security and safeguards of SNM of moderate significance, and security of classified information).

A licensee will then determine the need to address cyber security controls by utilizing Figure 6, “Screening Methodology for Digital Assets with a Latent Consequence of Concern.”

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Figure 3 - Screening

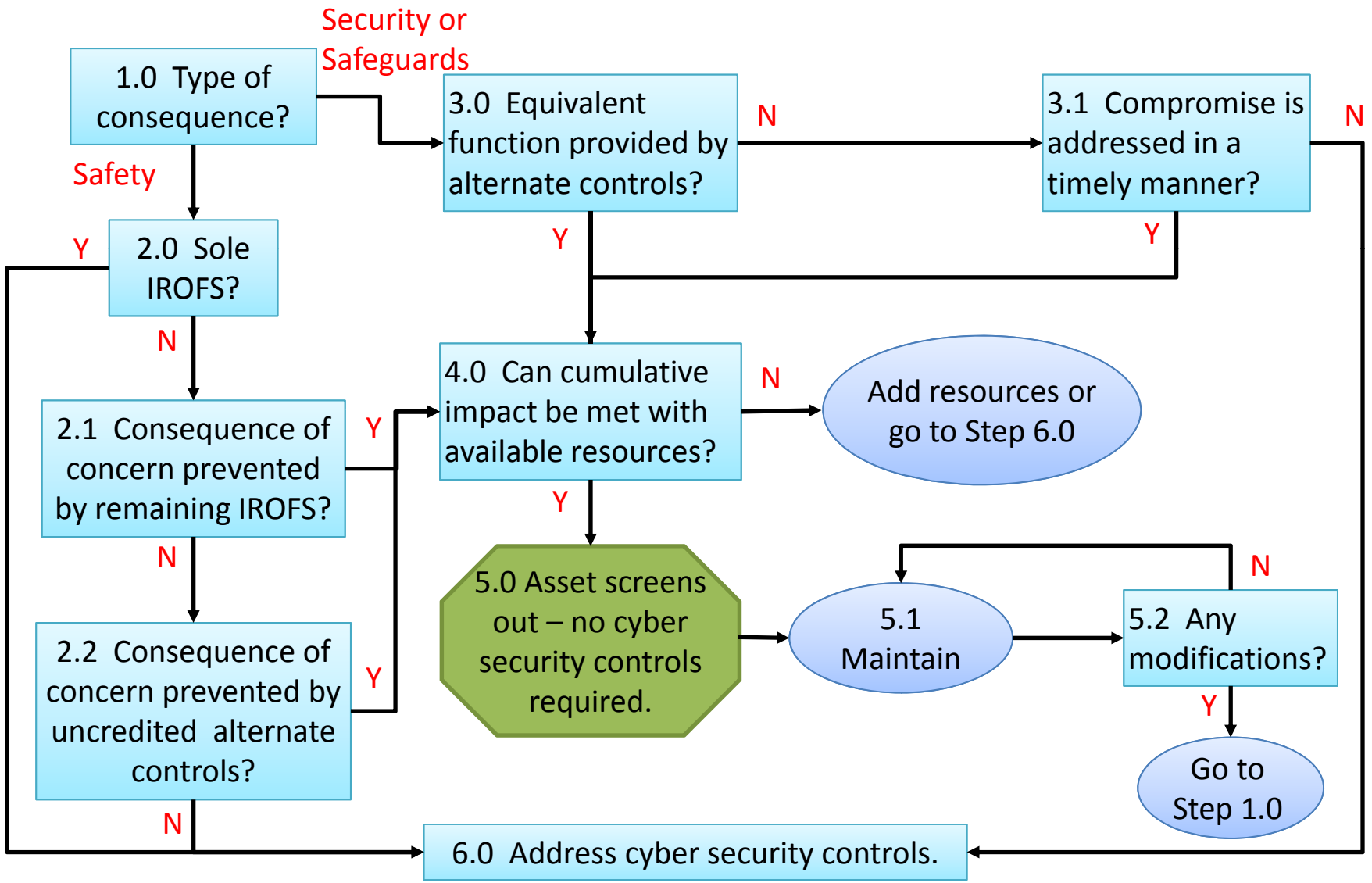
Determine the Applicable Digital Assets



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Figure 6 - Screening Methodology for Digital Assets with a Latent Consequence of Concern

Note: Detailed guidance for this diagram is in the early stages of development.



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Example 1: Non-digital IROFS

Background: ISA accident sequence FIRE-07 has two IROFS

Potential CoC: Release due to fire could result in an exposure of 25 rem to a worker

IROFS 005: Combustible controls – non-digital

IROFS 007: Fire brigade response – non-digital, digital radios could not compromise function

Alternate Control: None

No digital assets therefore, "no consequence" determination. Screening methodology not applicable and requirements met – no cyber security controls needed.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Example 2: Digital combined with non-digital IROFS

Background: ISA accident sequence CRIT-13 has two IROFS

Potential CoC: Criticality

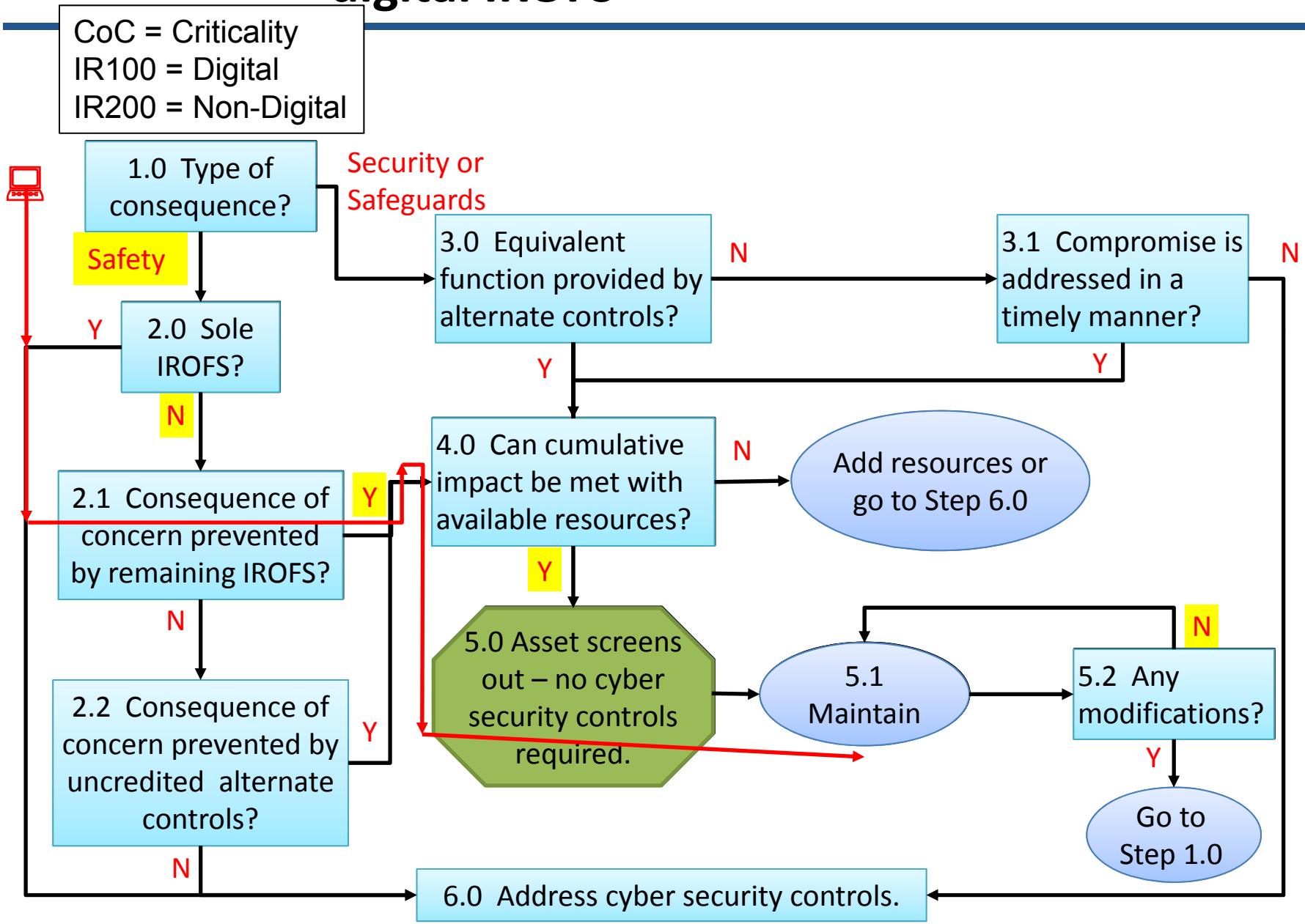
IROFS 100: Mass control – digital asset within IROFS boundary relies on data from the MC&A database

IROFS 200: Safe geometry – non-digital

Alternate Control: None

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Example 2: Digital combined with non-digital IROFS



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Example 3: Two digital IROFS with no alternate control

Background: ISA accident sequence CRIT-34 has two IROFS

Potential CoC: Criticality

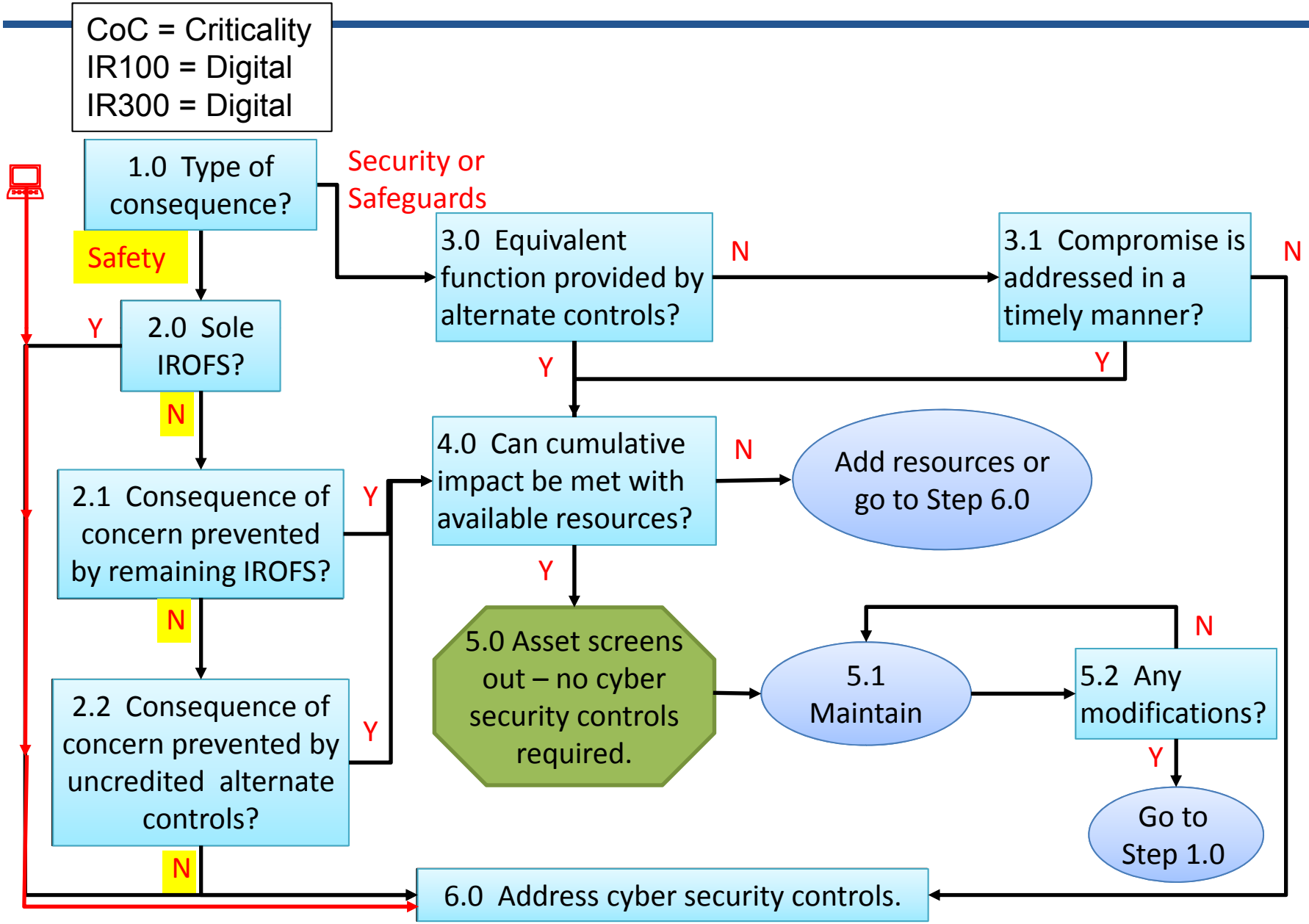
IROFS 100: Mass control – digital asset within IROFS boundary relies on data from the MC&A database

IROFS 300: Moisture control – digital because laptop (support system) calibration could compromise function

Alternate Control: None

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Example 3: Two digital IROFS with no alternate control



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Example 4: Sole digital IROFS

Background: ISA accident sequence FIRE-15 has a sole IROFS

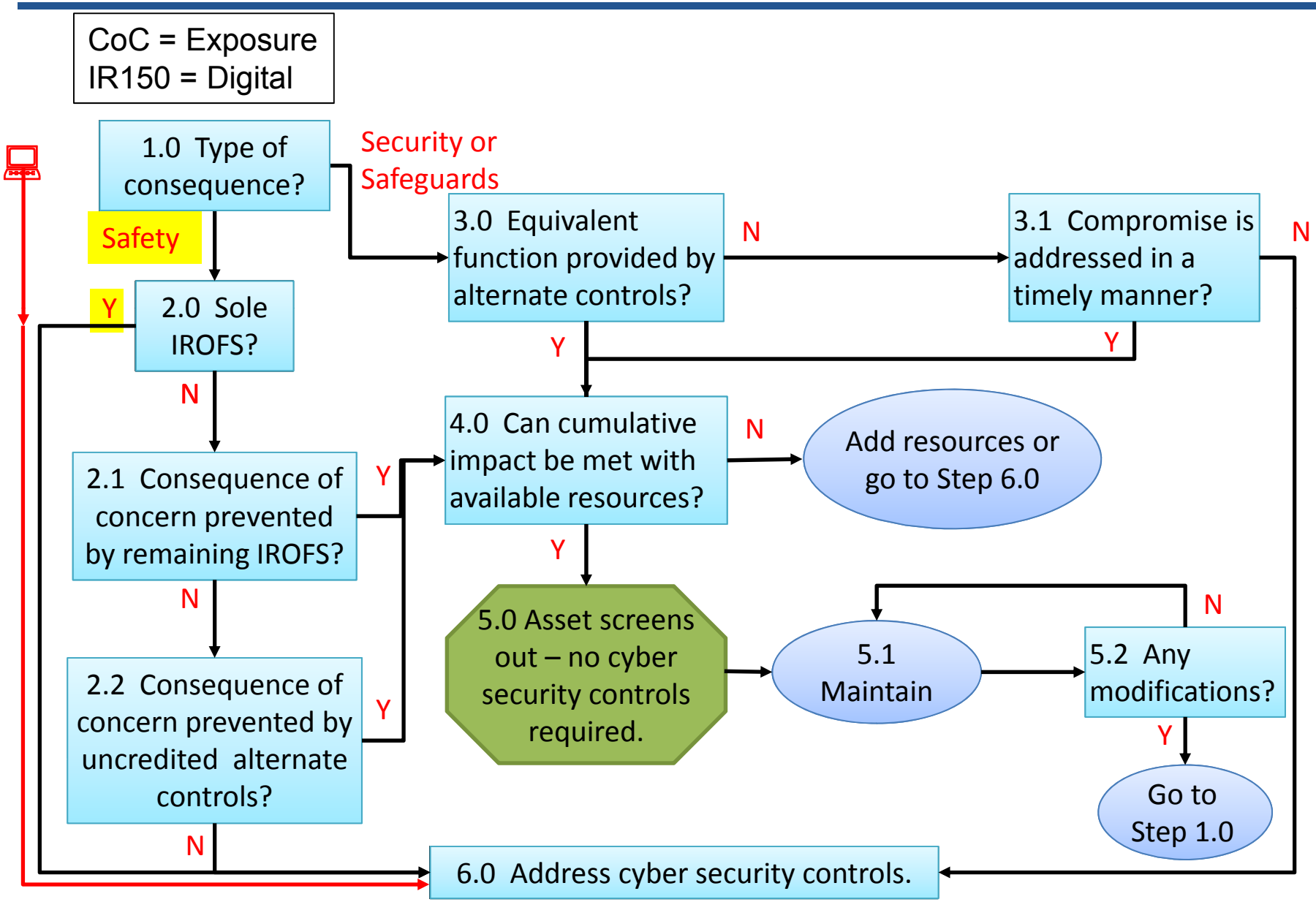
Potential CoC: Onsite radiation release could result in a 25 rem exposure to a worker

IROFS 400: Digital hydrogen monitor alarm

Alternate Control: None

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Example 4: Sole digital IROFS



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Example 5: Two digital IROFS with alternate control

Background: ISA accident sequence FIRE-20 has two IROFS with an alternate control

Potential CoC: Onsite radiation release could result in a 25 rem exposure to a worker

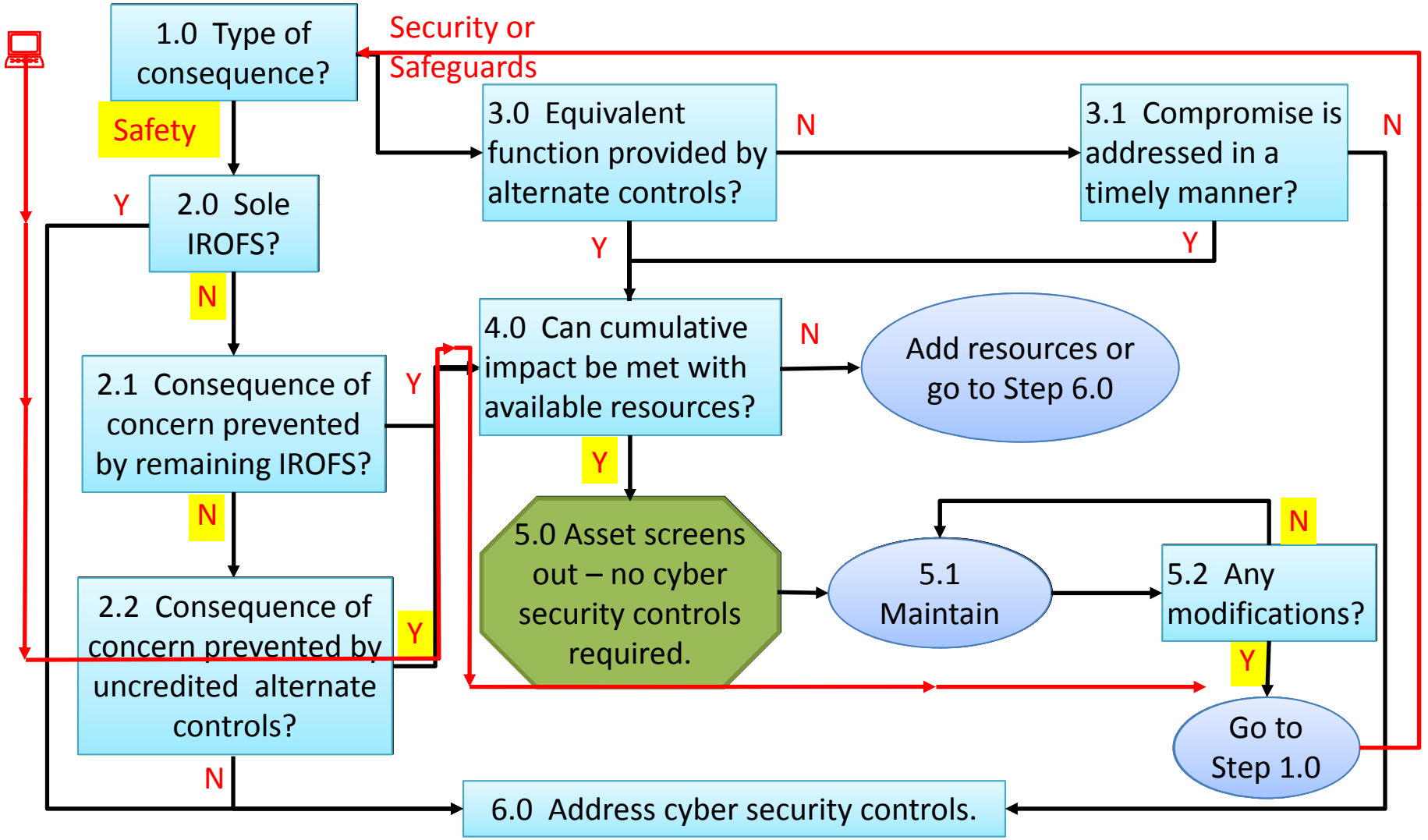
IROFS 400: Digital hydrogen monitor alarm

IROFS 500: Digital hydrogen shutoff

Alternate Control: Ventilation (non-digital)

Example 5: Two digital IROFS with alternate controls

CoC = Over 25 rem Exposure
IR400 = Digital
IR500 = Digital
Alt. Cnt. = Ventilation control, non digital



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Example 6: Security impact with alternate control

Background: Asset relied upon in the security plan for intrusion detection

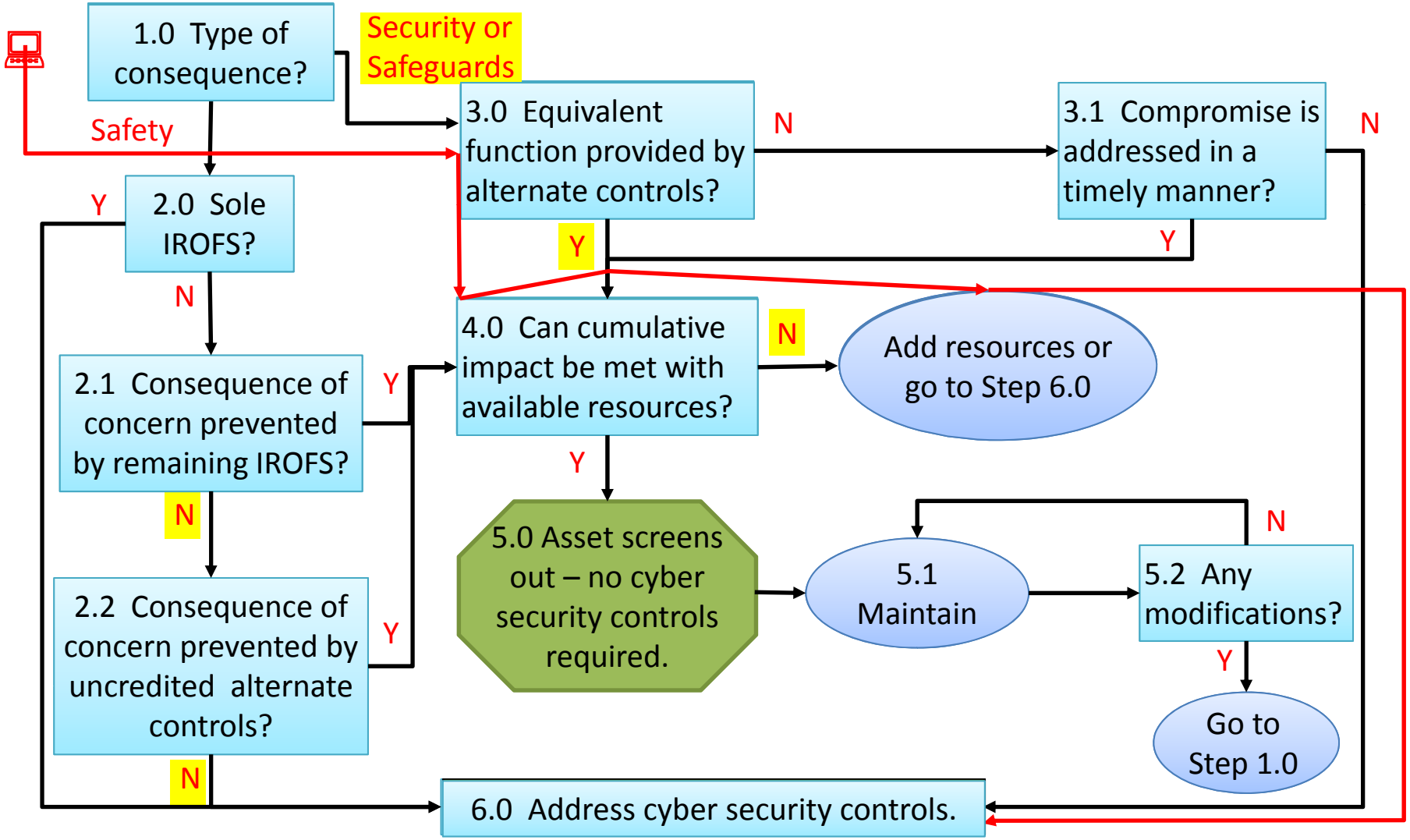
Potential CoC: Loss, theft, or diversion of significant quantities of SNM

Alternate Control: Guards

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Example 6: Security impact with alternative controls

CoC = Loss, theft, or diversion
Digital Asset = Intrusion detection
Alt. Cnt. = Guards



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Example 7: Information security impact with potential alternate control

Background: Asset relied upon in the security plan for locked door (card reader)

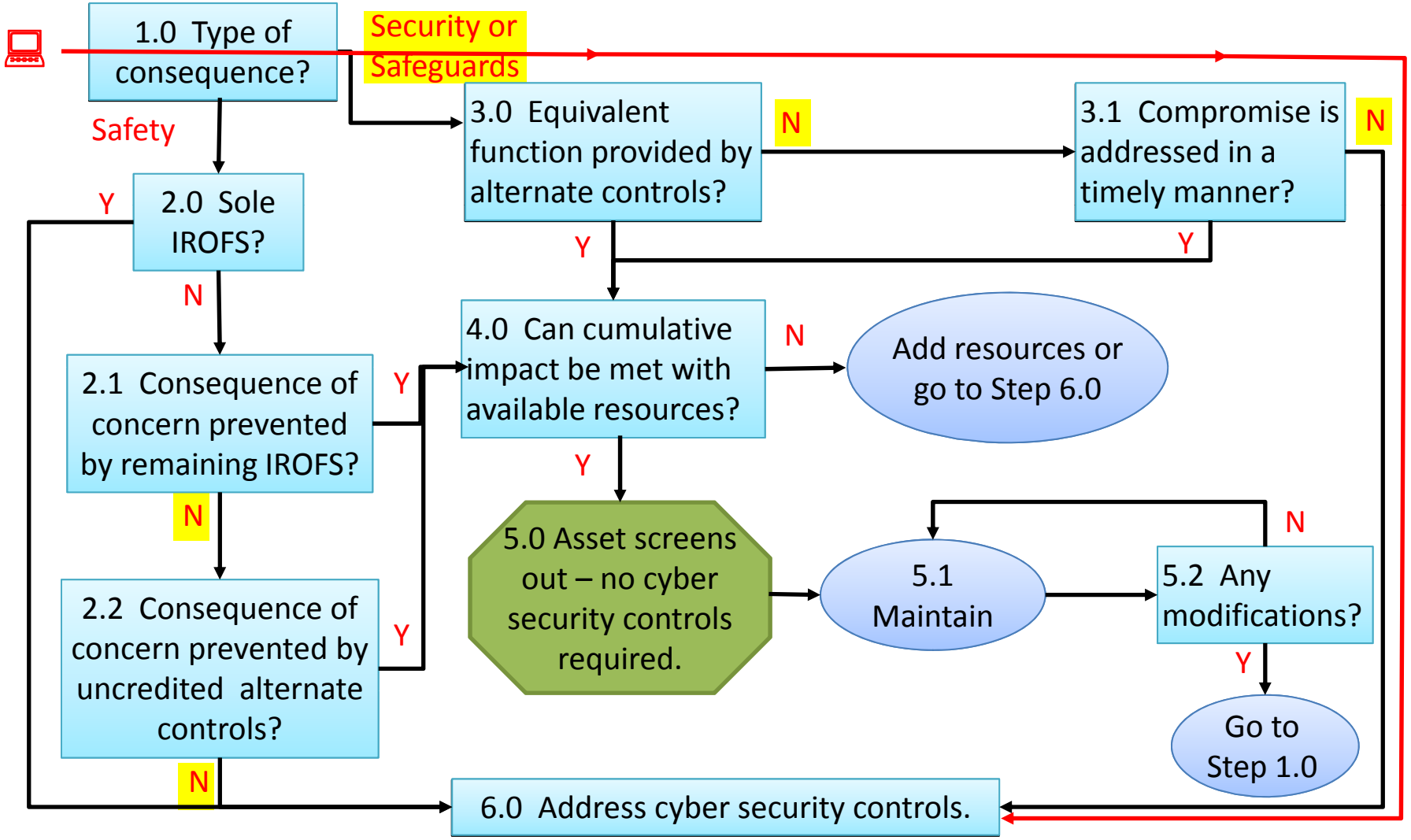
Potential CoC: Loss or unauthorized disclosure of classified information

Potential Alternate Control: Daily guard check

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Example 7: Information security impact with alternative controls

CoC = Loss of classified information
Digital Asset = Door card reader
Alt. Cnt. = Daily guard check



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Active Consequence Analysis

The purpose of an "active analysis" is to identify those digital assets that, if compromised, could directly lead to an event with a safety consequence of concern. An efficient approach for conducting the active analysis may begin by identifying the potential on-site sources that could result in a safety consequence of concern. To identify these potential sources, a licensee is encouraged to use existing analyses such as:

- ISA;
- Process hazards analysis;
- Previously considered malicious digital impacts;
- Vulnerability analysis; or
- Other safety or security information.

Once these on-site sources are identified, further analysis should be performed to determine if a barrier is present to prevent a cyber attack from resulting in a safety consequence of concern. Acceptable barriers to consider include:

- non-digital features, of an acceptable quality, that can withstand the actions resulting from a cyber attack;
- digital assets with cyber security controls applied via the "latent analysis" (note - when credited in an "active analysis," a higher cyber security control set may now be applicable to these assets, see Table 2, "Draft Facility Type Approach Matrix for Cyber Controls"); or
- digital assets with cyber security controls applied via other "active analyses."

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Active Consequence Analysis (continued)

If no existing barrier can be identified, cyber security controls are needed for the digital asset under consideration. The applicable cyber security control set can be determined through Table 2, "Draft Facility Type Approach Matrix for Cyber Controls."

Providing the applicable cyber security control set establishes an acceptable barrier to prevent the cyber attack from actively causing a consequence of concern.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Step 2: Select Security Controls

INPUT: List of in-scope digital assets

- Use Facility Type Matrix to determine control sets to be applied
  - Some digital assets will need the more inclusive control set (high-water mark)
- Determine best approach to address digital assets
  - Individually (simple system)
  - Grouped by function, network or sub-network (complex system)
  - Group of similar digital assets
  - Guidance contained in NIST SP 800-37, Sect. 2.3
- Identify and document **common security controls:** controls that provide security capability for multiple systems
  - For simplicity, a control may be implemented facility-wide and credited in individual System Security Plans (SSP)
  - Example: Common firewall may satisfy SC-7 Boundary Protection for multiple systems
  - Example: Security Event Information Management (SEIM) solution may satisfy SI-4 Information System Monitoring for multiple systems

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Step 2: Select Security Controls (continued)

- Develop draft **System Security Plan** (SSP) for each system or asset type
  - For simple/low functionality systems/devices with common configuration, a single SSP can be developed (**type authorization**)
    - Example: 20 digital video cameras of identical make/model
    - Example: 50 wireless digital pressure transmitters
- **Compensating security controls:** Credit may be taken for other programs that provide equivalent protection
  - Example: System cannot be password protected, is located in room with identity-based physical access control
  - Example: Transmissions may not be encrypted, wiring is housed in hardened conduit
- **Inherited security controls:** Controls inherited from facility-level (common) or other systems
  - Example: SI-4 Information System Monitoring – facility has comprehensive NIDS solution
  - Example: PL-4 Rules of Behavior – developed at facility level

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Step 2: Select Security Controls (continued)

- SSP documentation
  - System description
  - Component Inventory
  - System type/applicable control set
  - For each security control in applicable control set:
    - Description of control implementation, OR
    - Description of/reference to inherited common control, OR
    - Description of/documentation supporting compensating security control, OR
    - Justification/analysis/residual risk for non-application of controls, OR
    - Marked as “Not Applicable”
    - NOTE: Controls cannot be marked as “Not Applicable” without performing the appropriate threat/attack analysis and justification
  - System interconnections
- Monitoring strategy **Authorizing Official** (AO)
  - Senior program official
  - Assumes responsibility for organizational risk decisions
  - Performs system risk review, risk acceptance and system authorization
- AO approves draft SSP for each new system prior to implementation

OUTPUT: Draft SSPs

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Table 2 - Draft Facility Type Approach Matrix for Cyber Controls

Facility Type	Asset Function	Cyber Security Controls	
		Set I[1]	Set II[1]
Category I Facilities	Safety	applicable only for active consequence[2]	applicable only for latent consequence[3]
	Security & Safeguards	applicable for all – add DBT overlay[4]	-
Category II Facilities	Safety	applicable only for active consequence[2]	applicable only for latent consequence[3]
	Security & Safeguards	-	applicable for all
Category III Facilities	Safety	applicable only for active consequence[2]	applicable only for latent consequence[3]
	Security & Safeguards	-	applicable only for response to security orders (where nexus to safety) and physical protection of classified[5]
Part 40 Conversion / Deconversion Facilities	Safety	applicable only for active consequence[2]	applicable only for latent consequence[3]
	Security & Safeguards	-	applicable only for response to security orders (where nexus to safety)

[1] Set I, II, III, or IV refer to a baseline cyber security controls (see NRC Regulatory Guide for Fuel Cycle Cyber Security and NIST 800.53, Rev. 4)
Set I ≈ "high control baseline" and Set II ≈ "moderate control baseline"; both Set I and Set II include common programmatic controls
[2] Active consequence – asset function needed to prevent a cyber attack from directly causing a safety consequence of concern
[3] Latent consequence – asset function needed to prevent, mitigate, or respond to a safety/security/safeguards event associated with a consequence of concern
[4] DBT overlay – additional cyber security controls specific to the design basis threat (from the NRC Regulatory Guide for Fuel Cycle Cyber Security)
[5] Physical protection of classified – asset function needed for the physical protection of classified information or matter

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Control Set Discussion - Technical Issues Document Questions

What should be done after the final set of digital assets are identified to determine appropriate cyber security controls? (Question 16)

How is the control applicability determination evaluation performed? (Question 17)

Since the proposed control sets only list the names of the controls, how is a licensee to determine the necessary robustness of the control? (Question 18)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

SSP Documentation - Technical Issues Document Question

What information is needed in an System Security Plan (SSP)? (Question 19)

The intent of the SSP(s) is to list and describe the digital assets (systems) that fall within the scope of the rule (i.e., require the application of security controls) and identify their risk categories (dictated by rule/guidance language using the facility-type approach) and document the application of controls to the digital assets (systems). An individual should be able to review the SSP(s) and understand what digital assets (systems) have been identified through the screening process as requiring cyber security controls; what control sets are applied based on the facility-type approach; and the end state of each security control (e.g., description of control implementation, justification and analysis for non-application, use of compensating control, residual risk, etc.). In addition, the SSP(s) may include a description of the following for each digital asset (system):

- Function (e.g., safety, security, safeguards)
- Purpose
- Environment and location
- Responsible individuals
- Support systems
- Interconnections
- Inventory (hardware, software)
- Monitoring strategy
- POAM's as a companion to the SSP
- Control status table (example)
- Controls template (example)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

SSP Documentation Example

Control status table (partial) example:

Control Number and Name	Satisfied	Not Satisfied	Not Applicable	Inherited / Common
AC-1 Access Control Policy	X			
AC-2 Account Management		E3 (M, E1)	E2	
AC-3 Access Enforcement	X			
AC-4 Information Flow	X			
Percent of controls / category	75%	25%		

Controls template (partial) example (AC-1 Access Control Policy and Procedures):

System:	ACME Access Control Enhanced Security System (AACESS)
Function:	Security
Risk category:	High
Control set:	1
Location:	See attached diagram
Responsible individual:	Wile E. Coyote
Support systems and interconnections:	See attached diagram
Inventory:	See attached list
Description:	AACESS is a major application owned by the ACME Security department. AACESS consists of 2 systems: Badge issuance which controls creating and issuing badges with credentials; and the physical access control system which controls utilization of the badge credentials for physical access to the plant and other controlled areas.
Control:	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.
Supplemental Guidance:	The access control policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.
Control Enhancements:	None
Common Control Identification, Scoping Guidance, and Responsibility for Implementation	
ACME provides a plant-wide access control policy for all systems. System owners may develop a system specific access control policy to address system-specific requirements. System owners are responsible for developing formal, documented system-specific procedures to facilitate policy-compliant implementation of the access control policy and associated controls.	
System Specific Implementation Detail	Status: Satisfied
The ACME plant-wide access control policy fully meets the needs for AACCESS. The system depends on the ACME Information Technology Policy Standards & Training Team to develop, coordinate training for, and maintain the ACME IT security policies. In addition, the ACME Security Organization has documented the access control procedures within the AACCESS Security Policy and Procedures document and the Systems Security Plan. Access control is based on a role-based protocol. The role-based user profile ensures that individuals have system access privileges that do not exceed the scope of their duties.	

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Step 3: Implement Security Controls

INPUT: Draft SSPs

- For each system described in SSPs:
  - Implement each cyber security control in control set
  - Where control cannot be implemented, use compensating security controls that meet control intent and demonstrate equivalent protection
  - Where controls or compensating controls cannot be implemented
    - document justification
    - perform threat/attack analysis
    - document residual cyber security risk
- Update SSPs as necessary to reflect changes to/deviations from plan

OUTPUTS: Updated SSPs and digital systems with cyber security controls applied

Step 4: Assess Security Controls

INPUTS: Updated SSPs and digital systems with cyber security controls applied

- Third-party assessment
  - Assessors must possess the required skills and technical expertise
  - Assessors must have independence
    - Separation of roles: assessor cannot be stakeholder, operator, implementer, maintainer
    - Free from undue influence or conflict of interest
  - Assessors formally evaluated and approved by cyber program management
- Controls assessment
  - Implemented correctly?
  - Operating as intended?
  - Producing the required outcome with regards to the intent of the control?

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Step 4: Assess Security Controls (continued)

- Assessment methods (NIST SP 800-53A)
  - **Examine:** Observation of documents, activities, system settings, etc.
  - **Interview:** Discussions with stakeholders/operators to obtain evidence
  - **Test:** Technical testing of processes, procedures or system mechanisms
  - Most controls are assessed qualitatively, technical controls may have quantitative evaluation elements
- **Security Assessment Report** (SAR)
  - Contains assessed status of each required security control
  - Controls are assessed as “Implemented” or “Not Implemented”
  - Documents deltas between SSP and observed controls
- Remediation, SSP update, and re-testing as determined by licensee program processes

OUTPUTS: Final SSPs, Final SARs

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Discussion on Technical Issues Document Question

What is meant in “Step 4 – Assess Security Controls” by an independent assessment? (Question 20)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Step 5: Authorize Information System

INPUTS: Final SSPs, Final SARs

- Controls not in place documented in **Plan of Action & Milestones** (POAM)
  - Developed for each system
  - Companion/Appendix to SSP
  - Contains description of cyber security controls that are not in place
    - Planned upgrades to meet security requirements
    - Pending fixes to known issues
  - For each control not in place, describes:
    - Control Description
    - Description of Security Impact/Consequences
    - Risk Rating (High, Moderate, Low)
    - Impact Rating (High, Moderate, Low)
    - ETA/resources/cost for acceptable remediation
  - Describes/enumerates total residual risk to system based on controls not in place

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Step 5: Authorize Information System (continued)

- Final system documentation package submitted to AO for review
  - SSP
  - SAR
  - POAM with residual risk determination
- System Authorization
  - AO reviews residual risks
  - **Authority to Operate** (ATO) is granted or denied
    - Systems denied ATOs may re-apply after addressing issues
    - ATOs are time-limited, typically expire after 3 years
  - Review and subsequent actions are documented

OUTPUT: Authority to Operate

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Discussion on Technical Issues Document Questions

What is the purpose of authorizing an information system to operate (approval of SSP)?

(Question 21)

What is the purpose of a Plan of Action and Milestones (POAM) and how should the licensees track the actions? (Question 22)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Step 6: Monitor Security Controls

INPUT: Authority to Operate

- Manage Changes to System/Environment
  - Minor system changes
    - Follow Configuration Management processes
    - Update SSP as necessary
  - Major system changes
    - Significant system changes trigger full re-authorization
    - Examples: Operating system version upgrade, major firmware release, significant component replacement
    - Licensee must define “major change” in Configuration Management Plan
- Ongoing Assessments
  - Periodic risk/vulnerability assessments
  - Core security controls must be tested annually
  - 1/3 of non-core security controls must also be tested annually

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Step 6: Monitor Security Controls (continued)

- Ongoing Remediation
  - Flaw remediation based on findings from periodic risk/vulnerability assessments
  - POAM Management
    - POAM items entered into licensee Corrective Action Program (CAP)
    - Where no CAP exists, licensee must review and update POAMs every 90 days
    - SSP updated when POAM items addressed
- Key updates
  - SSPs, POAMs, other key documentation updated based on minor system changes, policy updates

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Step 6: Monitor Security Controls (continued)

- Security Status Reporting
  - POAM status updates
  - Results of periodic Risk/Vulnerability Assessments
  - Results of Flaw Remediation efforts
- Ongoing Risk Determination/Acceptance
  - AO reviews security status reporting
  - Organizational risk profile updated accordingly
  - Ongoing risk decisions

Continuous monitoring until Authority to Operate expires

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

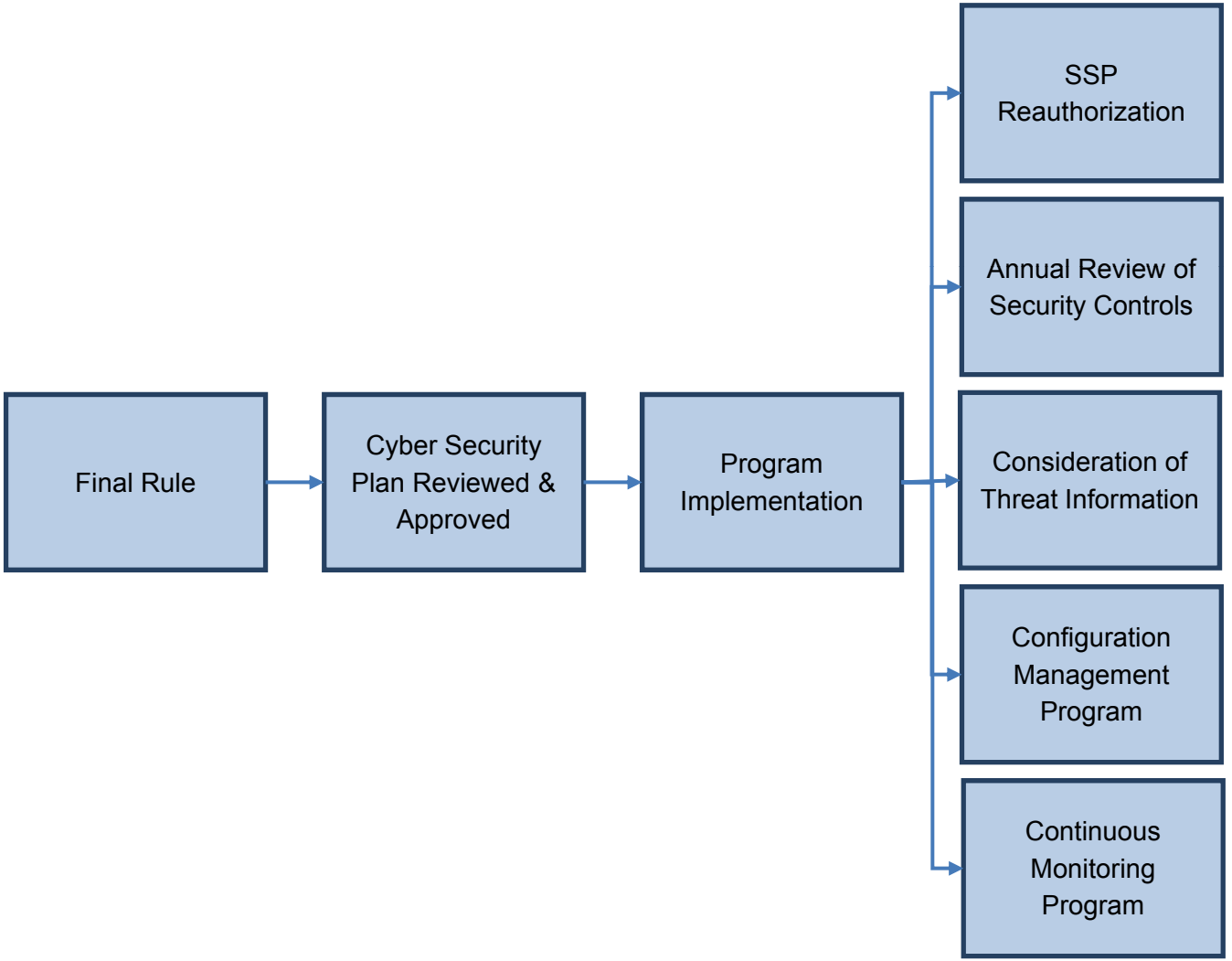
Discussion on Technical Issues Document Question

What is meant by Step 6 in the risk management framework (monitor security controls)?

(Question 23)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Figure 4 - Cyber Security Program with Ongoing Evaluations and Improvements



Discussion on Technical Issues Document Question

What does the NRC staff mean by a phased implementation of the rule? (Question 12)

Instead of a single implementation date, the staff currently envisions implementation with two milestones, as follows:

- Milestone 1 (completion of step 2 in the Risk Management Framework (RMF))
  - Develop programmatic elements;
  - Identify digital assets in scope, apply screening methodology for latent consequence digital assets, and select security controls and develop SSPs, including applicability evaluations;

- Milestone 2 (completion of step 5 in the RMF)
  - Implementation of security controls to digital assets;
  - Independent assessment; and
  - Authorization to operate.

See Figure 2, "Phased Implementation Approach," for a draft diagram of the phased implementation approach.

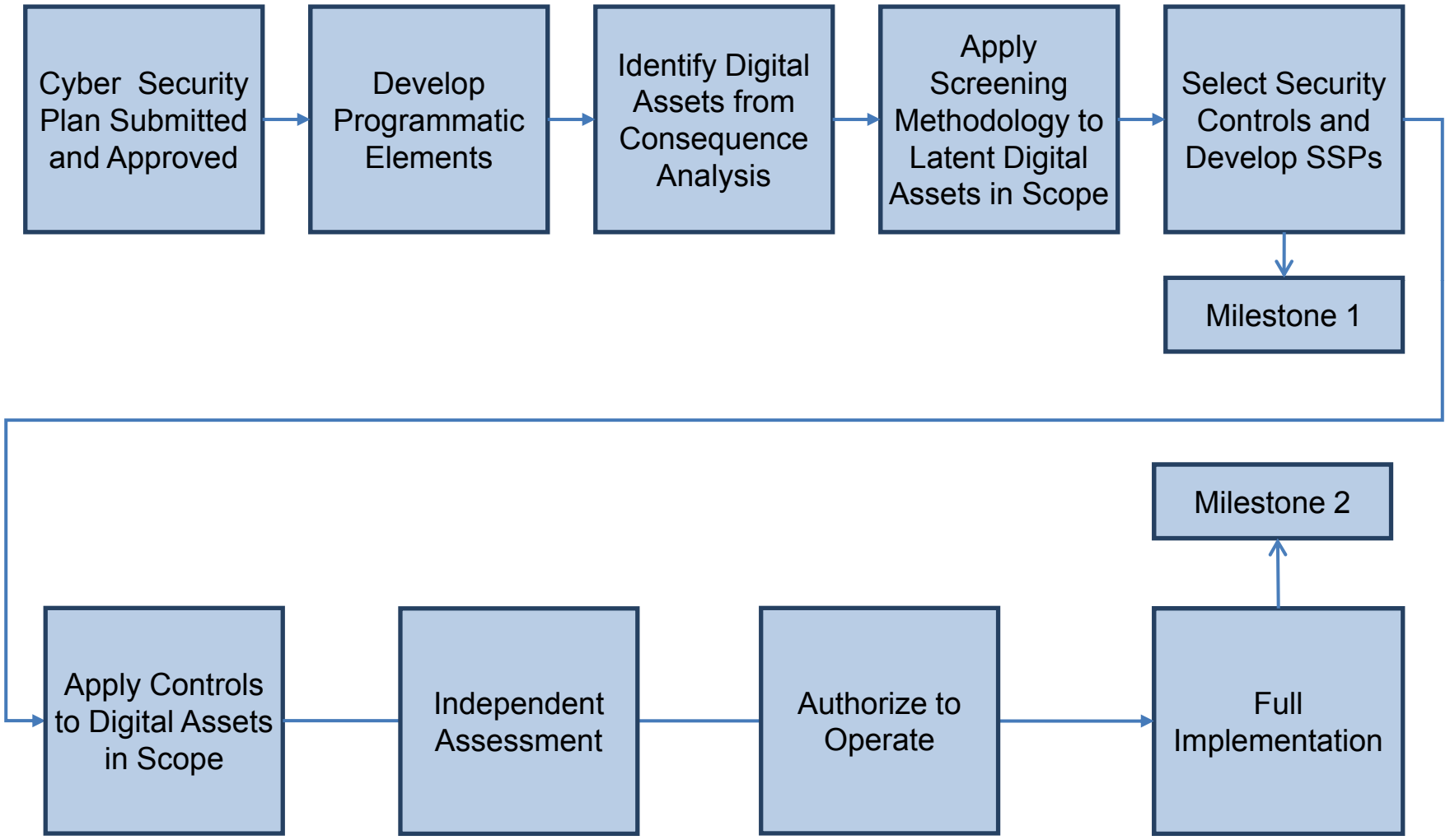
Phased implementation is a lesson learned from the power reactor rule implementation.

Phased implementation facilitates the early identification of issues and ensures a consistent application of the regulations.

The rule will include a date by which full implementation will be required.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Figure 2 - Phased Implementation Approach



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Program Management Cyber Security Controls

Selected Program Management controls to be deployed organization-wide in support of the information security program. These controls are not associated with specific security control sets.

Notes:
(1) Do not use this table without consulting the regulatory guide for specific guidance.
(2) These controls reference controls from NIST SP 800-53, Revision 4.

Control Number	Control Name	Selection for FCF Cyber Security Rulemaking
PM-1	Information Security Program Plan	X
PM-2	Senior Information Security Officer	X
PM-3	Information Security Resources	
PM-4	Plan of Action and Milestones Process	X
PM-5	Information System Inventory	
PM-6	Information Security Measures of Performance	X
PM-7	Enterprise Architecture	
PM-8	Critical Infrastructure Plan	
PM-9	Risk Management Strategy	X
PM-10	Security Authorization Process	X
PM-11	Mission/Business Process Definition	
PM-12	Insider Threat Program	X
PM-13	Information Security Workforce	X
PM-14	Testing, Training, and Monitoring	X
PM-15	Contacts with Security Groups and Associations	X
PM-16	Threat Awareness Program	X

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Cyber Security Control Sets

Notes:
(1) Do not use this table without consulting the regulatory guide for specific guidance.
(2) These controls reference controls from NIST SP 800-53, Revision 4.
(3) For Set I and Set II control applicability to 3S systems, please refer to Facility Control Matrix
(4) DBT control set denotes controls that apply only to security systems at Category I facilities

Below is a sample from the document "Cyber Security Control Sets for Fuel Cycle Facility Rulemaking"

Control Number	Control Name Control Enhancement Name	Control Sets		
		Set II	Set I	DBT
AC-1	**Access Control Policy and Procedures**	x	x	
AC-2	**Account Management**	x	x	
AC-2(1)	ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT	x	x	
AC-2(2)	ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS	x	x	
AC-2(3)	ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS	x	x	
AC-2(4)	ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS	x	x	
AC-2(5)	ACCOUNT MANAGEMENT | INACTIVITY LOGOUT		x	
AC-2(6)	ACCOUNT MANAGEMENT | DYNAMIC PRIVILEGE MANAGEMENT			
AC-2(7)	ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES			
AC-2(8)	ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT CREATION			
AC-2(9)	ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED / GROUP ACCOUNTS			x
AC-2(10)	ACCOUNT MANAGEMENT | SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION			x
AC-2(11)	ACCOUNT MANAGEMENT | USAGE CONDITIONS		x	
AC-2(12)	ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE		x	
AC-2(13)	ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS		x	
AC-3	**Access Enforcement**	x	x	
AC-3(2)	ACCESS ENFORCEMENT | DUAL AUTHORIZATION			x
AC-3(3)	ACCESS ENFORCEMENT | MANDATORY ACCESS CONTROL			
AC-3(4)	ACCESS ENFORCEMENT | DISCRETIONARY ACCESS CONTROL			
AC-3(5)	ACCESS ENFORCEMENT | SECURITY-RELEVANT INFORMATION			
AC-3(7)	ACCESS ENFORCEMENT | ROLE-BASED ACCESS CONTROL			
AC-3(8)	ACCESS ENFORCEMENT | REVOCATION OF ACCESS AUTHORIZATIONS			
AC-3(9)	ACCESS ENFORCEMENT | CONTROLLED RELEASE			
AC-3(10)	ACCESS ENFORCEMENT | AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS			

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Cyber Security Control Parameters

Notes:
(1) Do not use this table without consulting the regulatory guide for specific guidance.
(2) These controls reference controls from NIST SP 800-53, Revision 4.

Below is a sample from the document "Cyber Security Control Parameters for Fuel Cycle Facility Rulemaking"

Control Number	Control Name Control Enhancement Name	Parameters
Program Management Controls		
PM-1	Information Security Program Plan	P1: At least yearly
PM-2	Senior Information Security Officer	-
PM-4	Plan of Action and Milestones Process	-
PM-6	Information Security Measures of Performance	-
PM-9	Risk Management Strategy	P1: At least yearly
PM-10	Security Authorization Process	-
PM-12	Insider Threat Program	-
PM-13	Information Security Workforce	-
PM-14	Testing, Training, and Monitoring	-
PM-15	Contacts with Security Groups and Associations	-
PM-16	Threat Awareness Program	-
Access Controls		
AC-1	Access Control Policy and Procedures	P1: all employees and contractors P2: at least yearly P3: at least yearly
AC-2	Account Management	P1: (licensee-defined) P2: (licensee-defined) P3: (licensee-defined) P4: at least every 90 days
AC-3	Access Enforcement	-

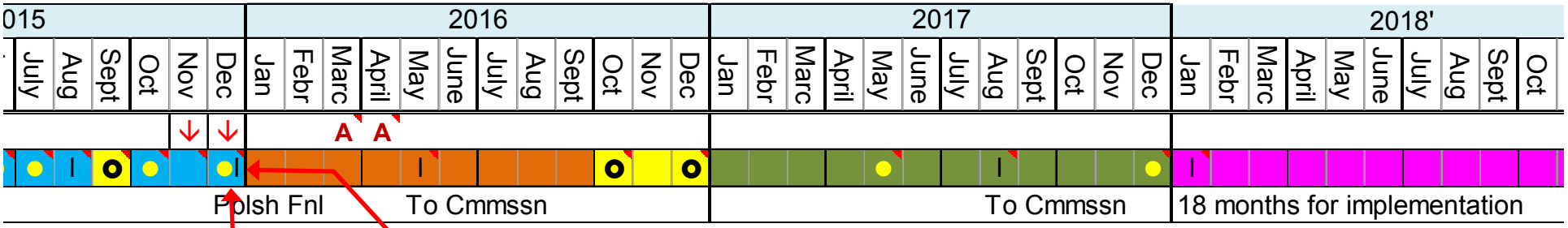
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NRC Staff Approach to Drafting Rule Language

- Two approaches being considered:
  - Similar to 10 CFR 73.54
  - Similar to the risk management framework
- Identification of consequences of concern and corresponding thresholds
- Establishment of a framework for the screening of digital assets and the application of cyber security controls
- Inclusion of Program Management Controls
- Goal is to utilize existing reporting requirements, but fill gaps if necessary

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Regulatory Basis



= Reg. Basis/Draft Guidance	↓ = Change occurred below arrow
= Proposed Rule/Draft Guidance	V = Site Visit
= Final Rule/Final Guidance	A = ACRS Meeting
= Public Interaction	
= Implementation	
= Meeting occurs	
I = Marks a milestone with text	

December 10, 2015, (today) public meeting

Finalize regulatory basis, December 2015

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Meeting Outcome Questions

- Was the meeting helpful?
- Did we address your concerns adequately?
- What concerns remain?
- What are the areas where we do not agree?

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Conclusions

- Technical issues discussed today are draft
- Screening focus on consequence of concern and allows for alternate controls
- Controls based on facility type matrix, NIST, and NRC guidance
- Additional opportunities for interaction