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

Technical Discussion on the Fuel Cyber Security Proposed Rulemaking

Thursday October 22, 2015

1:00pm-4:30pm

Matt Bartlett

Brian Smith

Documents at ML15288A514

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

Agenda

- Discuss the 13 technical issues
- Discuss tables and figures
- Work through screening examples
- Timeline and path forward

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

Technical Issues

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

- A cyber attack that:
  - directly results in a safety or security consequence of concern (active); or
  - compromises a function needed to prevent, mitigate, or respond to a safety/security event with a potential to cause a consequence of concern (latent).

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

Technical Issues

Question 2: What are the draft consequences of concern under consideration to address safety, security, emergency preparedness, and material control & accounting (SSEPMCA)?

- Nuclear criticality [safety].
- Releases of radioactive materials or chemicals resulting in significant exposures to workers or members of the public
- Loss, theft or diversion of significant quantities of special nuclear material (SNM)
- Radiological sabotage [security – limited to licensees with a DBT].
- Loss or unauthorized disclosure of classified information [security].
- Inability to maintain onsite and offsite communications during normal and emergency operations [emergency preparedness (EP)].
- See Table 1, "Consequences of Concern and Scope," for additional description on each of these areas.

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

Technical Issues

Question 3: What are the thresholds for determining if an event results in a consequence of concern?

- The threshold to determine a consequence of concern consists of any of the criteria listed below.
- The Title 10, "Energy," of the *Code of Federal Regulations* (10 CFR) 70.61 for high consequence nuclear criticality events [safety].
- The performance requirements in 10 CFR Part 70.61 for radiological or chemical exposures that result in high or intermediate consequence events, except intermediate consequences to members of the public or the environment [safety].
- The loss, theft, or diversion of significant quantities of SNM. The licensee's physical security and MC&A programs are required to prevent the loss/theft/diversion of significant quantities of SNM. The requirements in the regulations are based on the protection of specific SNM quantities of concern for the three categories of facilities (i.e., Cat I, II, and III) [security and MC&A].
- The loss or theft of classified information [security].
- The compromise of communications between the licensee and the NRC, local responders, or other government agencies. EP programs are required to facilitate the communications between licensees and the NRC and local responders. If these capabilities are compromised, protective actions may not prevent unnecessary exposures to members of the public [EP].

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

Table 1: Consequences of Concern

Consequences of Concern	Thresholds	Digital Assets Within Scope*
Nuclear criticalities are events in which large quantities of radiation are released and could endanger the life of workers. (safety)	10 CFR Part 70.61 performance requirements for high consequence nuclear criticality events.	Digital IROFS associated with preventing criticality accidents.
Releases of radioactive materials or chemicals resulting in significant exposures to workers or members of the public. 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. (safety)	10 CFR Part 70.61 performance requirements for radiological or chemical exposures that result in high or intermediate consequence events, except intermediate consequences to member of the public or the environment.	Digital IROFS associated with 10 CFR Part 70 high and intermediate consequence events, except intermediate public and environmental; AND Operational and process controls whose compromise from a cyber attack could directly cause a consequence of concern (based on analysis).
Loss/theft/diversion of significant quantities of SNM. (security and MC&A, including DBT)	Physical security and MC&A programs are required to prevent the loss/theft/diversion of significant quantities of SNM. The requirements in the regulations are based on the protection of specific SNM quantities of concern for the three categories of facilities (i.e., Categories I, II, and III). Physical Security Program and MC&A Program; 10 CFR Part 73 DBTs.	Digital assets used in implementing the Physical Security Program and order responses and the MC&A Program; AND For those licensees with a DBT, physical security digital assets used in protecting against the DBT as documented in the Physical Security Plan.
Loss or unauthorized disclosure of classified information. (security)	Information security programs are required to prevent the loss or theft of classified information. Standard Practices and Procedures Plan and Physical Security Plan	Physical security digital assets used in implementing the Standard Practices and Procedures Plan and Physical Security Plan.
Inability to maintain onsite and offsite communications during normal and emergency operations. (EP)	EP programs are required to facilitate the communications between licensees and the NRC and local responders. If these capabilities are compromised, protective actions may not be taken in time to prevent unnecessary exposures to members of the	Digital assets used in implementing the EP Plan.

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

Technical Issues

Question 4: How does the NRC staff propose to prevent these consequences from occurring?

- Establishing a risk-informed, performance-based, and graded regulatory framework for the various types of fuel cycle facilities.
- Establishing appropriate cyber security regulations informed by:
  - The power reactor cyber security rule (10 CFR 73.54) and the lessons learned during its implementation;
  - The consideration of the uniqueness of fuel cycle facilities;
  - Insights learned from site visits; and
  - Industry standards.

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

Technical Issues

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

The NRC intends to develop cyber security requirements for fuel cycle facilities, taking into account the safety significance of digital assets at these facilities and the risk resulting from a compromise of these assets. This approach will require the protection of those digital assets important to assuring the health and safety of the public and the environment.

The staff envisions that the licensees will perform an analysis to identify those digital assets within the scope of the rule. Question 11 provides additional information on how to perform the consequence analyses.

Licensees implement SSEPMCA programs to comply with existing risk-informed regulations in 10 CFR Parts 40, 70, 73, 74, and 95. The existing integrated safety analysis (ISA) and EP, security, and MC&A programs would be utilized to inform the cyber security program, identify which digital assets could be within scope of the rule, and inform the screening process. Since these programs are risk-informed and consequence based, the NRC staff anticipates that utilizing these programs will result in identification of only those digital assets that are also risk-informed and consequence based. Each of these programs uses a risk-informed, consequence based structure.

- The ISA is implemented to prevent or mitigate significant exposure events (exposures in excess of the performance requirements) 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.
- The ISA requirements include prevention of nuclear criticalities. Criticalities are events in which large quantities of radiation are released and could endanger the life of workers.
- Physical security and MC&A programs are required to prevent the loss, theft or diversion of significant quantities of SNM. The requirements in the regulations are based on the protection of specific SNM quantities of concern for the three categories of facilities (i.e., Categories I, II, and III).
- Information security programs are required to prevent the loss/theft of classified information, which if compromised, could cause damage to the United States.
- EP programs are required to facilitate the communications between licensees and the NRC and local responders. If these capabilities are compromised, protective actions may not be taken in time to prevent unnecessary exposures to members of the public.

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

Technical Issues

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

- The staff is considering providing:
- A facility-type grading approach, as described in Table 2, "Draft Facility Type Approach Matrix for Cyber Controls," where the safety and security risks will be considered for each type of facility (e.g., Categories I, II, III, and source materials). The controls applied would be commensurate with the safety and security risks at each type of facility.
- A screening methodology that will reduce the number of digital assets that would require cyber security controls, which is illustrated in Figure 3, "Screening – Determine the Applicable Digital Assets," and Figure 6, "Screening of Digital Assets."
- The NRC staff does not plan to address specific cyber security controls within the proposed regulation, but rather the staff is planning to develop guidance that uses/endorses industry recognized and consensus standards which will allow for a more flexible approach to implementation of programs and controls. Licensees would be able to analyze and justify why certain controls are not applicable to certain digital assets. This approach would also allow licensees to take credit for existing controls and/or use alternative controls.
- Licensees would be able to apply controls to entire networks as opposed to individual digital assets on networks.
- This approach will be incorporated into a Regulatory Guide being developed concurrent with the proposed rule.

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	**Set II[1]**	**Set III[1]**	**Set IV[1]**
Category I Facilities	Safety	applicable - active consequence	applicable - latent consequence	-	-
	Security	applicable - add DBT overlay	-	-	-
	Emergency Preparedness	-	-	-	applicable
	Material Control & Accounting	applicable - applicable	-	-	-
Category III Enrichment Facilities	Safety	applicable - active consequence[2]	applicable - latent consequence[3]	-	-
	Security	-	applicable - physical protection of classified[6]	-	applicable
	Emergency Preparedness	-	-	-	applicable
	Material Control & Accounting	applicable - safety input[5] with active consequence[2]	applicable - safety input[5] with latent consequence[3]	-	applicable - no safety input
Category III Fuel Fabrication Facilities	Safety	applicable - active consequence[2]	applicable - latent consequence[3]	-	-
	Security	-	applicable - physical protection of classified	-	applicable
	Emergency Preparedness	-	-	-	applicable
	Material Control & Accounting	applicable - safety input[5] with active consequence[2]	applicable - safety input[5] with latent consequence[3]	-	applicable - no safety input[5]
10 CFR Part 40 Conversion / Deconversion Facilities	Safety	applicable - active consequence[2]	applicable - latent consequence[3]	-	-
	Security	-	applicable	-	-
	Emergency Preparedness	-	-	-	applicable
	Material Control & Accounting	-	-	-	-

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

Table 2: Draft Facility Type Approach Matrix for Cyber Controls (continued)

[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"; Set II ≈ "moderate control baseline"; Set III ≈ "low control baseline"; Set IV are limited programmatic controls

[2] Active consequence – asset function needed to prevent a cyber attack from directly causing a consequence of concern

[3] Latent consequence – asset function needed to prevent, mitigate, or respond to a safety/security event associated with a consequence of concern

[4] DBT overlay – additional cyber security controls specific to the design basis threat

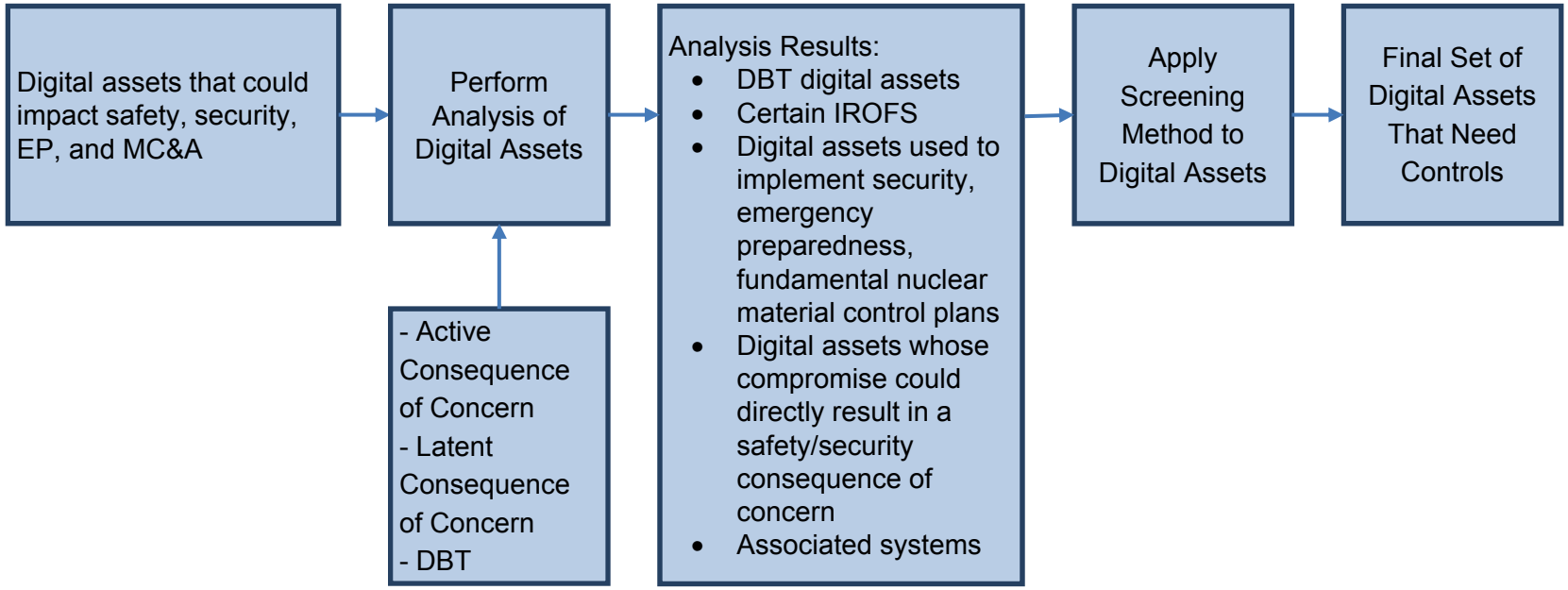
[5] MC&A safety input – asset provides an MC&A input to a within scope safety asset

[6] 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

Figures (#3)

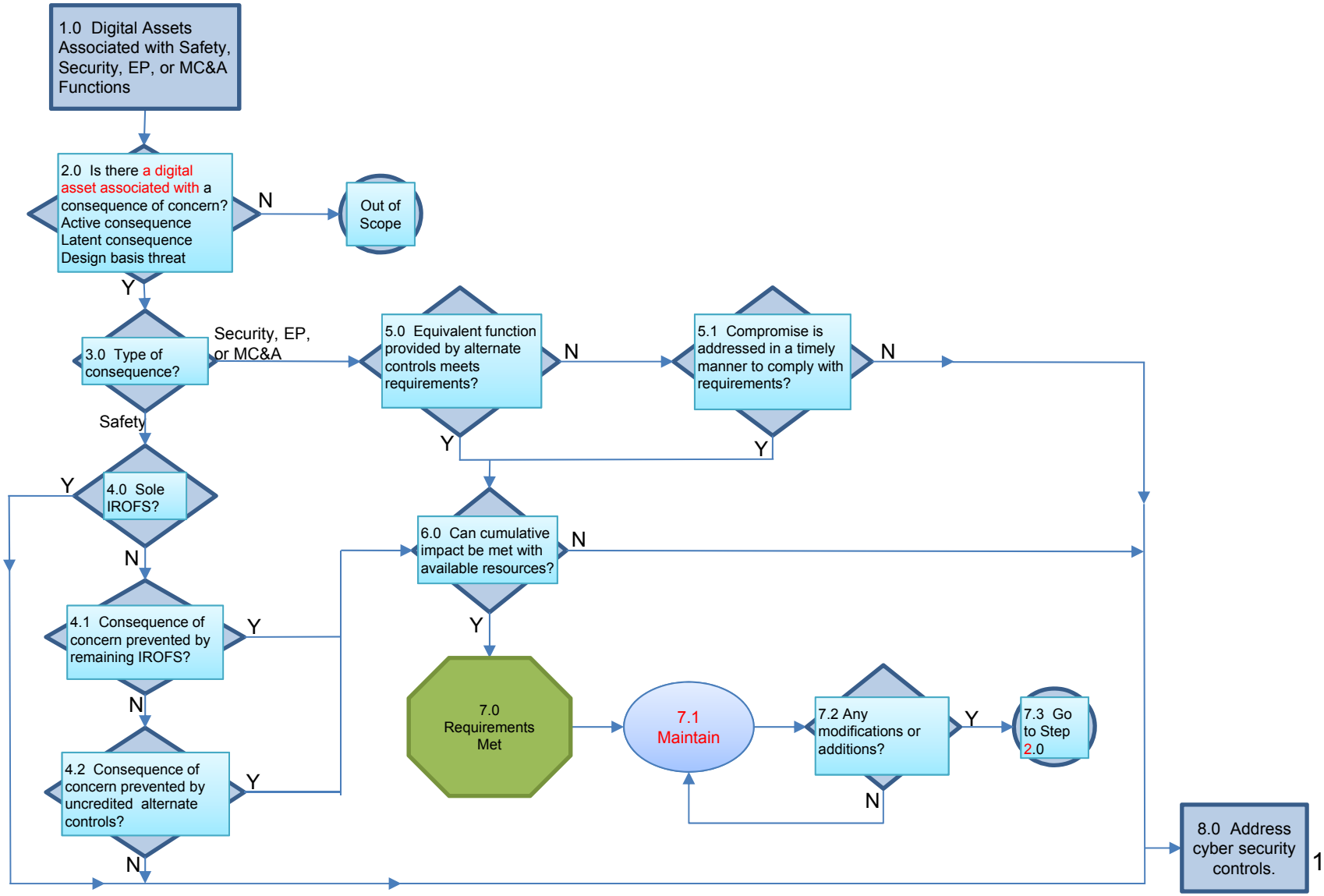
Screening - Determine the Applicable Digital Assets



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

Figures (#6)

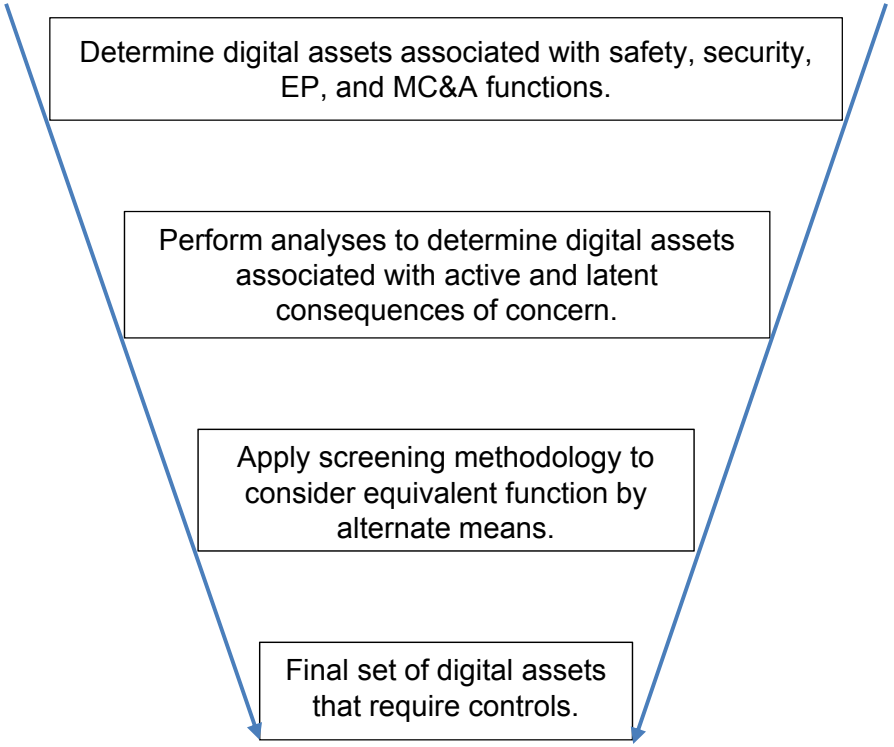
Draft Screening Methodology for Identification of Digital Assets



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

Figures (#7)

Screening of Digital Assets



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

Technical Issues

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

- The initial set of digital assets for analysis is expected to include:
  - Digital assets associated with operational and process controls whose compromise from a cyber attack could directly cause a consequence of concern.
  - Digital assets associated with items relied on for safety (IROFS) used to prevent or mitigate high or intermediate consequence events, except intermediate consequence events to members of the public or the environment.
  - Digital assets associated with physical security functions (including information security and cyber security), including those assets associated with implementing the physical security plan, the Standard Practices and Procedures Plan, and the cyber security program.
  - Digital assets required to support the licensee's strategy to protect against the DBTs.
  - Digital assets used in implementing the EP plan.
  - Digital assets used in implementing the MC&A program.
  - Digital assets associated with support systems and equipment which, if compromised, would adversely impact SSEPMCA functions.
- The staff intends to develop a screening process that will reduce the scope of digital assets by allowing licensees to take credit for alternate controls. This draft screening process is illustrated in Figure 3, "Screening – Determine the Applicable Digital Assets," and Figure 6, "Screening of Digital Assets."
- The remaining subset of digital assets would have cyber security controls applied as described in Table 2, "Draft Facility Type Approach Matrix for Cyber Controls."
- Additional description of digital assets currently anticipated to be within the scope of the proposed rule can be found in Table 1, "Consequences of Concern and Scope."

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

Technical Issues

Question 8: How does the NRC staff plan to use consensus standards in the guidance associated with the rule (Regulatory Guide)?

- The staff plans to utilize applicable National Institute of Standards and Technology (NIST) standards, with limited exceptions where necessary.
- The Regulatory Guide will provide specifics as to what digital assets need to be protected. The Regulatory Guide will also contain a screening methodology that considers the impact of the loss/compromise of the digital assets and the availability of any alternative controls. This screening will reduce the number of digital assets that require controls to be applied.
- The risk management framework in NIST 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems," calls for a risk assessment to be performed for the information/digital assets being protected. In this case, the Regulatory Guide will provide a risk assessment by facility type for each of the different SSEPMCA categories of digital controls (i.e., ranking of controls). Instead of using the recommended baseline controls in NIST 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," the Regulatory Guide will contain the baseline controls for each SSEPMCA category at a specific facility type. An additional overlay of controls will be included for those digital assets identified to address the DBTs.
- The Regulatory Guide will provide guidance on the programmatic elements of the licensee's cyber security program (e.g., training and configuration management) and the risk management framework.

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

Technical Issues

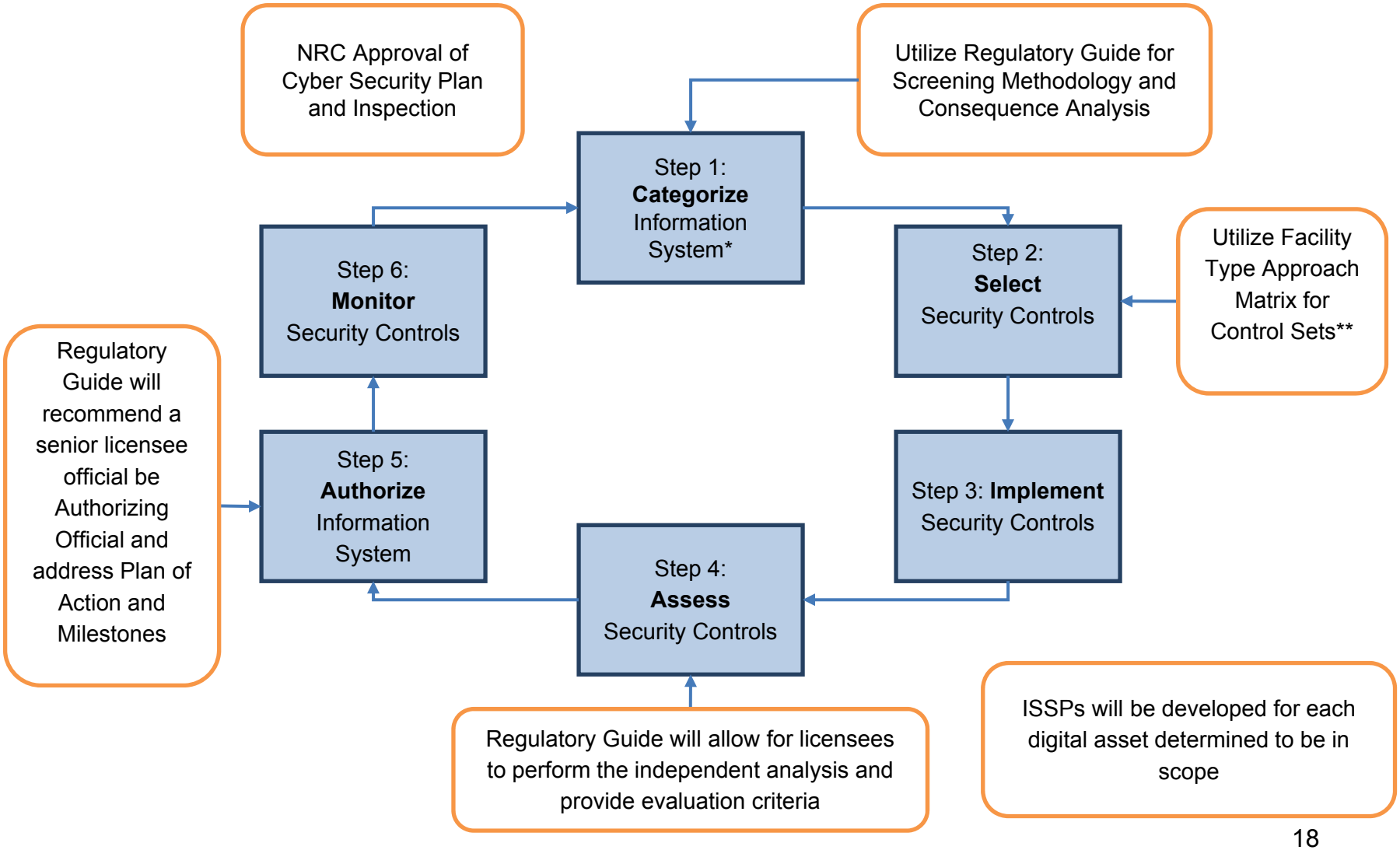
Question 9: How will the risk management framework in NIST 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems," be modified in the Regulatory Guide?

- See Figure 5 for the risk management framework.
- Step 1 - The NIST risk management framework calls for a risk assessment to be performed of the information system/digital assets being protected. In this case, the Regulatory Guide will provide a risk assessment by facility type for each of the different SSEPMCA controls (i.e., ranking of controls).
- Step 2 - Instead of using the recommended baseline controls in NIST 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," the Regulatory Guide will contain the baseline controls for each SSEPMCA category at a specific facility type. An overlay of controls will be included for those digital assets identified as being in place to address the DBTs. The Regulatory Guide will provide guidance on how the applicability evaluation of controls will be conducted.
- Step 2 - The Regulatory Guide will recommend that an Information System Security Plan (ISSP) be developed for each digital asset within scope. The ISSP may be utilized to document the evaluation of applicable controls and how each applicable control will be implemented.
- Step 4 - The Regulatory Guide will provide guidance that will allow the licensees to perform the independent analysis of security control implementation. Guidance on the performance of the evaluation will also be provided.
- Step 5 - The Regulatory Guide will recommend that a senior licensee official be designated as the authorizing official. The Regulatory Guide will also address plans of action and milestone documents.

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

Figures (#5)

Risk Management Framework



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

Technical Issues

Question 10: How are the DBTs factored into the determination of digital assets within scope of the rule?

- Similar to 10 CFR 73.54, the NRC staff envisions that the proposed rule will require Category I licensees to provide high assurance that computer and communications systems and networks are adequately protected against cyber attacks, up to and including the DBTs. Category I licensees will need to do an evaluation to identify which digital assets are required to support the licensee's strategy to protect SNM from threats up to and including the DBTs of radiological sabotage and theft and diversion. The staff envisions that these digital assets, due to their consequences of concern, will require the highest level of cyber security controls.
- Note: Digital assets on a classified network regulated by another government agency would not be within scope and would not require additional controls.

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

Technical Issues

Question 11: How is the consequence analysis performed?

- The consequence analysis is part of the screening methodology, illustrated in Figure 6, "Draft Screening Methodology for Identification of Digital Assets." Detailed guidance is in the early stages of development, however, the goal is for a licensee to identify assets whose function could be compromised by a cyber attack and could result in an active or latent consequence of concern.
- The licensee should identify those digital assets that perform or support an SSEPMCA function. This information may come from:
  - ISA;
  - Process hazards analysis;
  - Security orders and plans;
  - Emergency Plan;
  - Fundamental Nuclear Materials Control Plan;
  - Previously unconsidered malicious digital impacts;
  - Vulnerability analysis; or
  - Other safety or security information.
- Because much of the analysis required by NRC regulation does not take malicious actions into account, additional considerations may be necessary. A single cyber attack can cause
- multi-node compromise, which is more challenging to analyze than multi-node failure. Given these complexities, it may be more efficient to individually identify the potential on-site sources that could result in a consequence of concern, then consider the established barriers preventing that consequence. If those barriers can be breached by a digital compromise, the assets associated with that compromise would need cyber security controls applied unless an alternate means of preventing the consequence of concern is identified.

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

Technical Issues

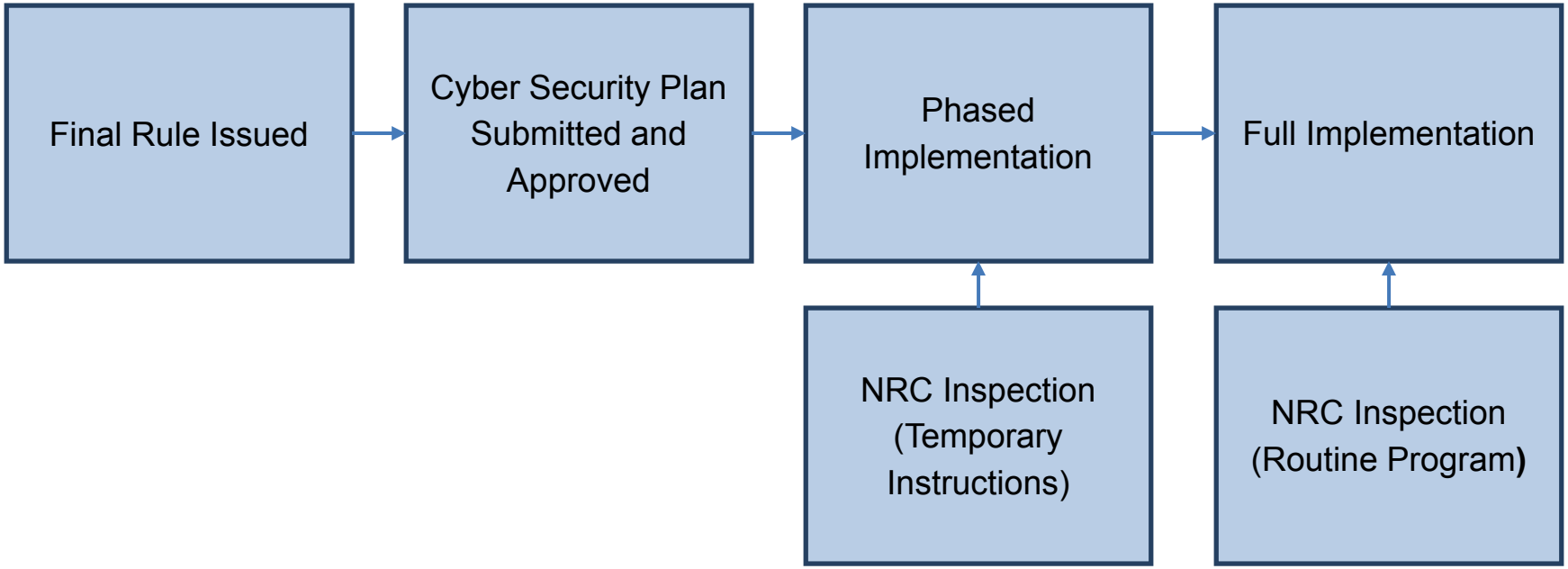
Question 12: What does the NRC staff mean by a phased implementation of the rule?

- Instead of a single implementation date, phased implementation over time as follows:
  - Develop programmatic elements;
  - Identify digital assets in scope, apply screening methodology, and select security controls and develop ISSPs, including applicability evaluations;
  - Application of controls to digital assets; and
  - Full implementation.
- 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.

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

Figures (# 1)

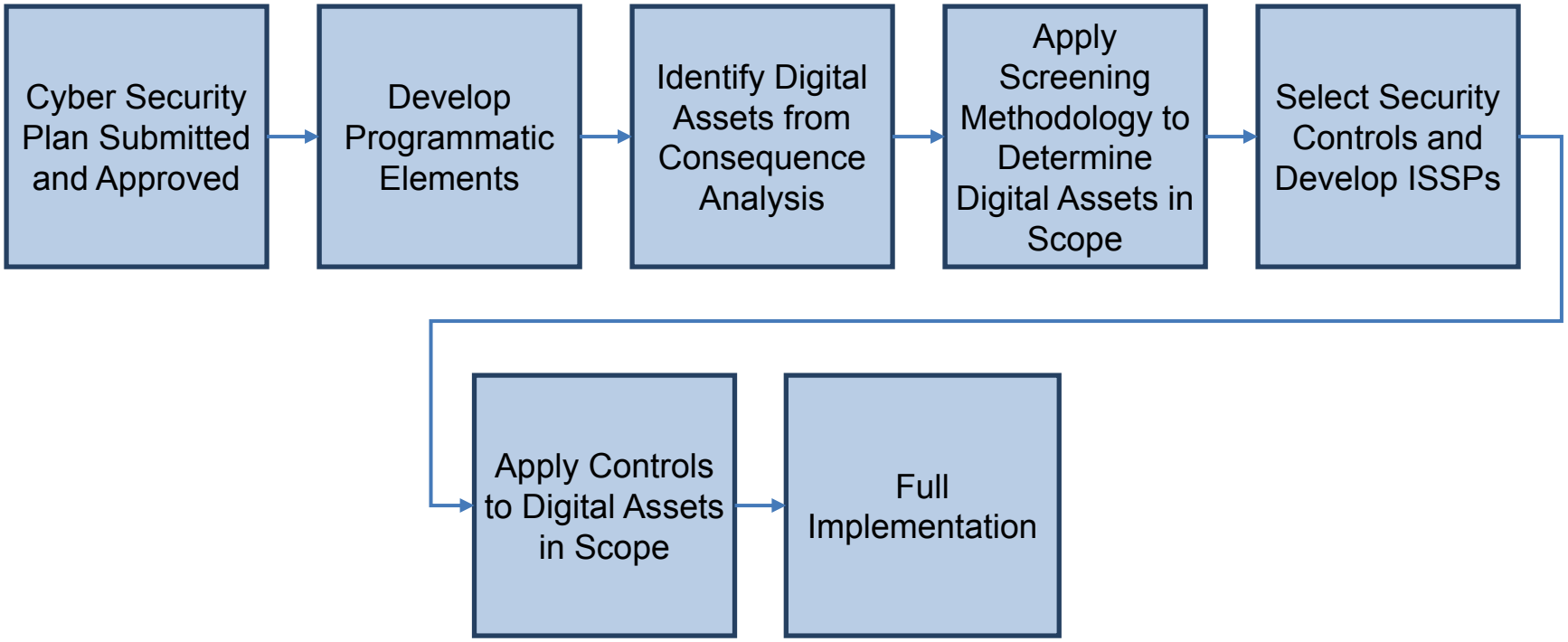
General Overview of Implementation and Oversight



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

Figures (#2)

Phased Implementation Approach



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

Technical Issues

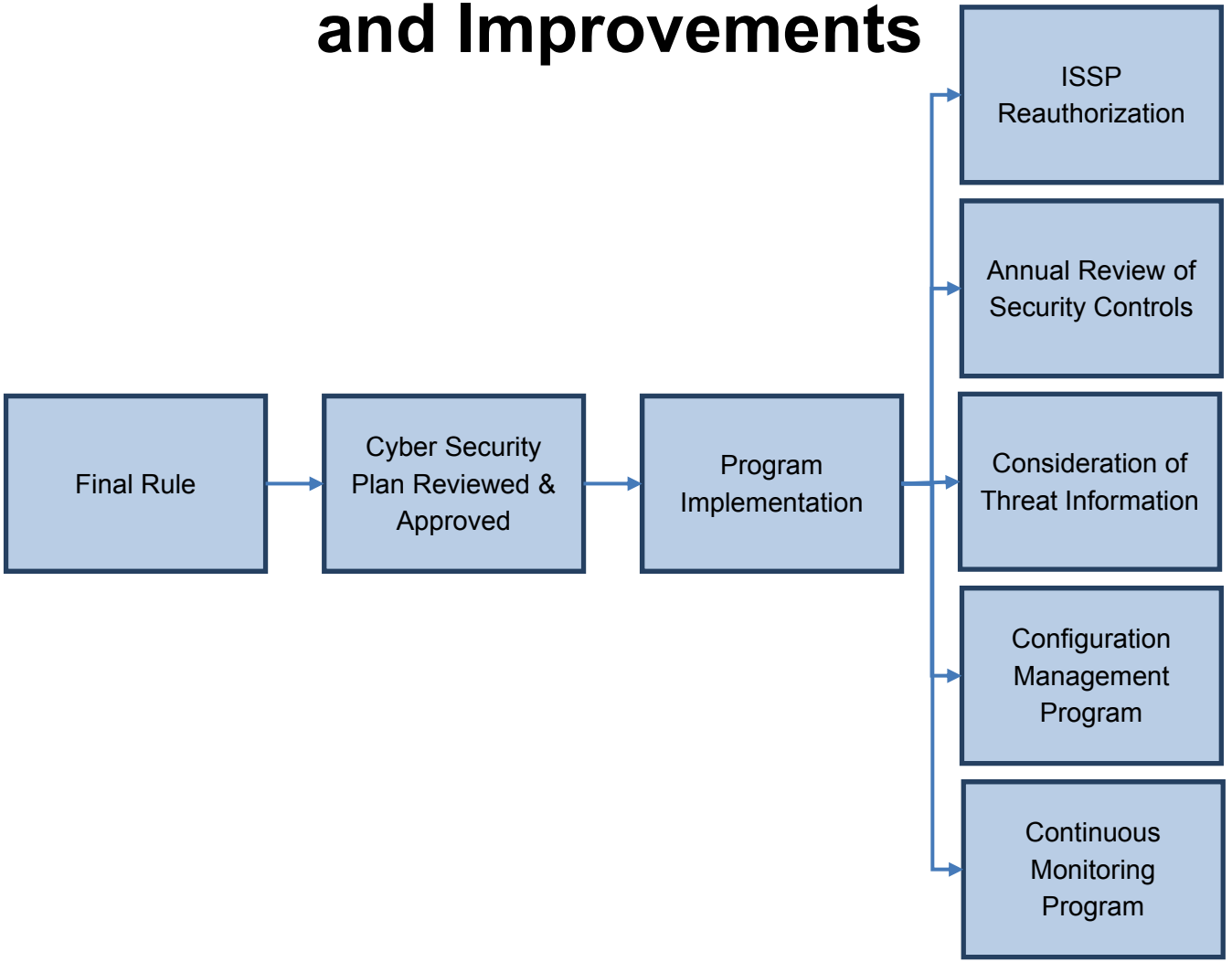
Question 13: How is the NRC staff keeping safety/security in mind to ensure that there are no unintended consequences?

- The proposed approach would not require the ISA or existing Standard Practices and Procedures Plan, Physical Security Plan, EP Plan, or MC&A Plan to be modified as a result of the new cyber requirements. The existing ISA and EP, security, and MC&A programs would be utilized to inform the cyber security program, identify which digital assets could be within scope of the proposed rule, and inform the screening process.
- Applying cyber security controls will prevent a cyber attack from directly causing a consequence of concern and protect digital assets needed to prevent, mitigate, or respond to a consequence of concern.

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

Figures (#4)

Cyber Security Program with Ongoing Evaluations and Improvements



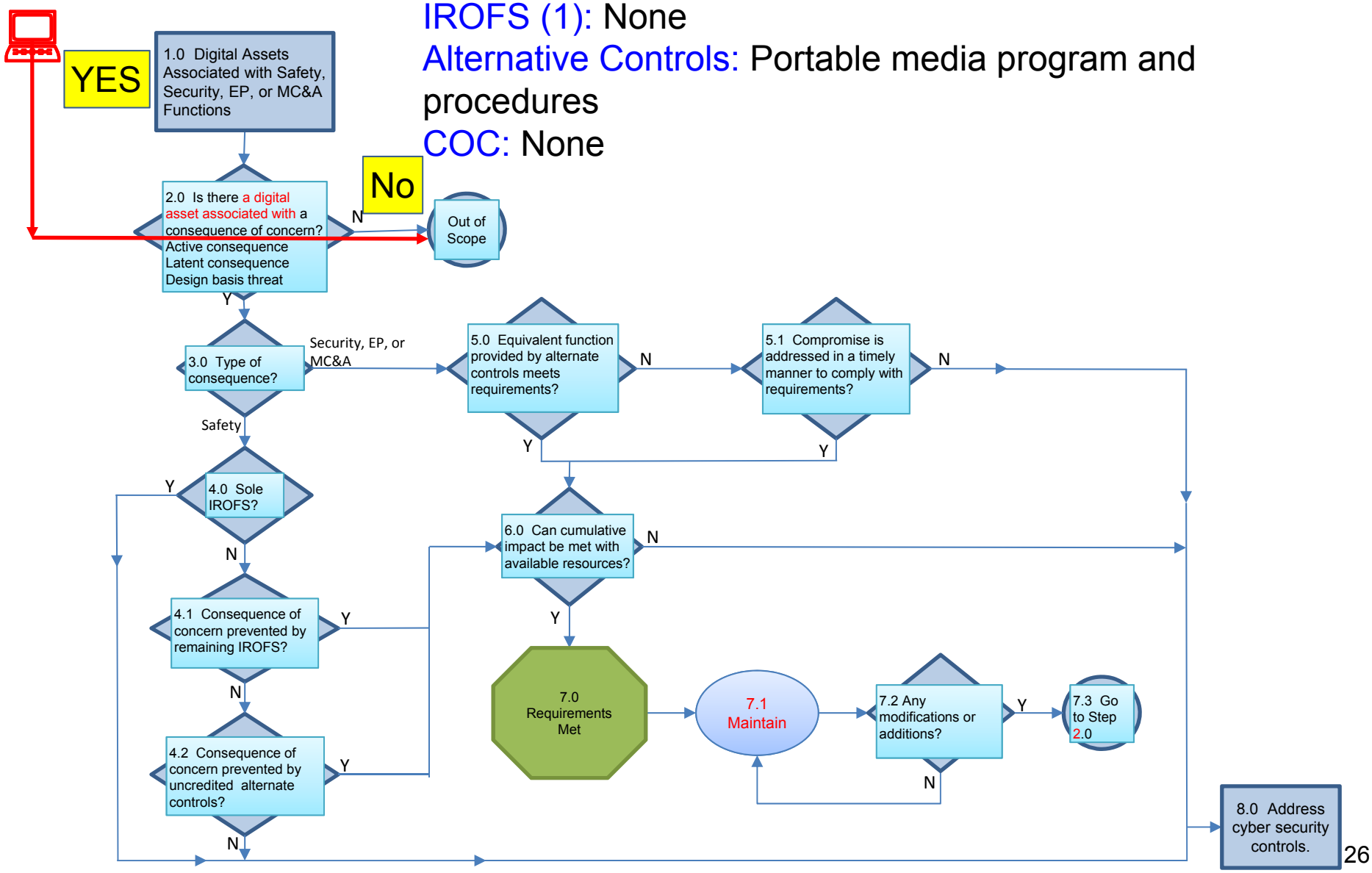
Screening Example 1: Attack with no consequence

Event: Portable media malware corrupts MC&A database

IROFS (1): None

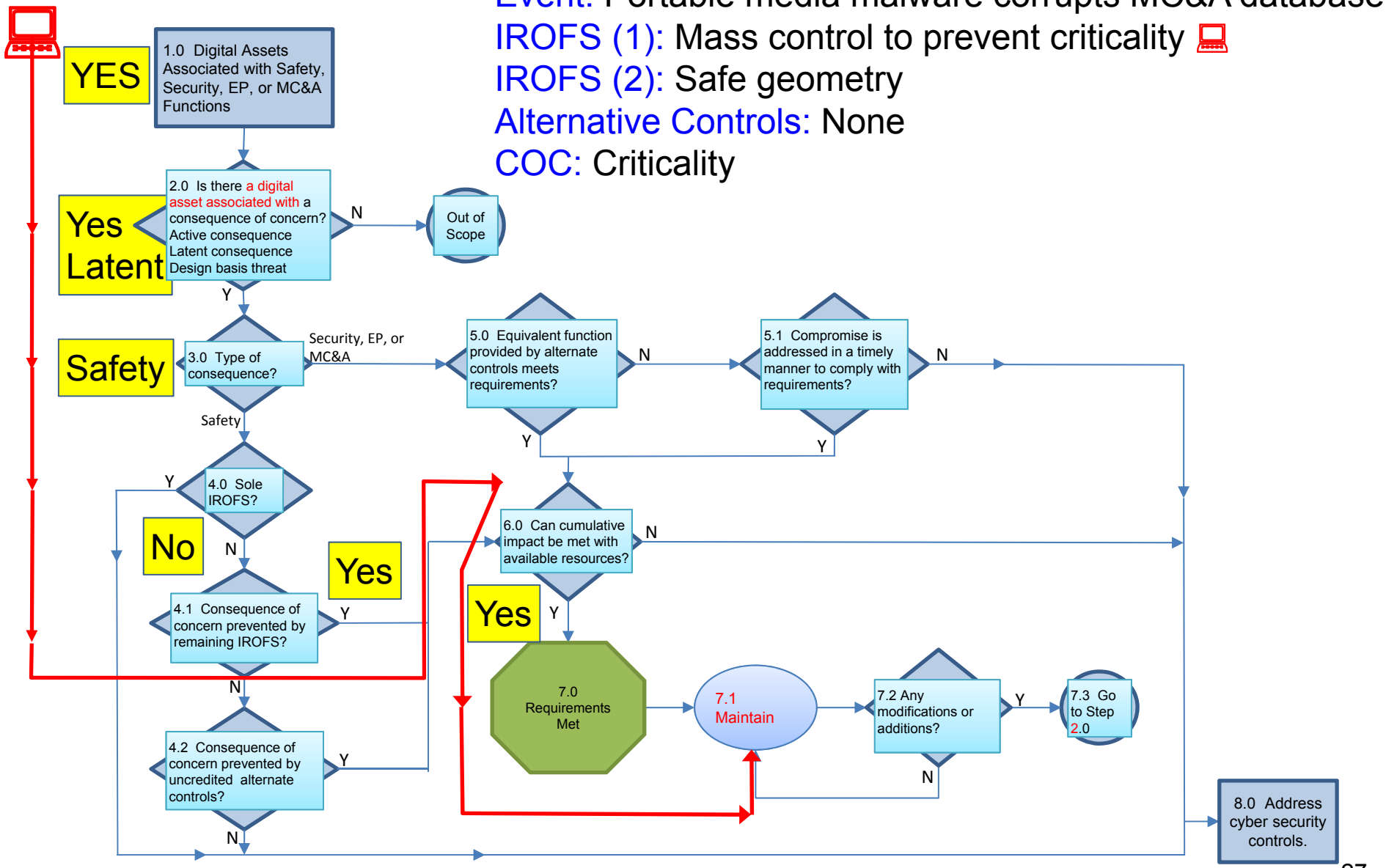
Alternative Controls: Portable media program and procedures

COC: None



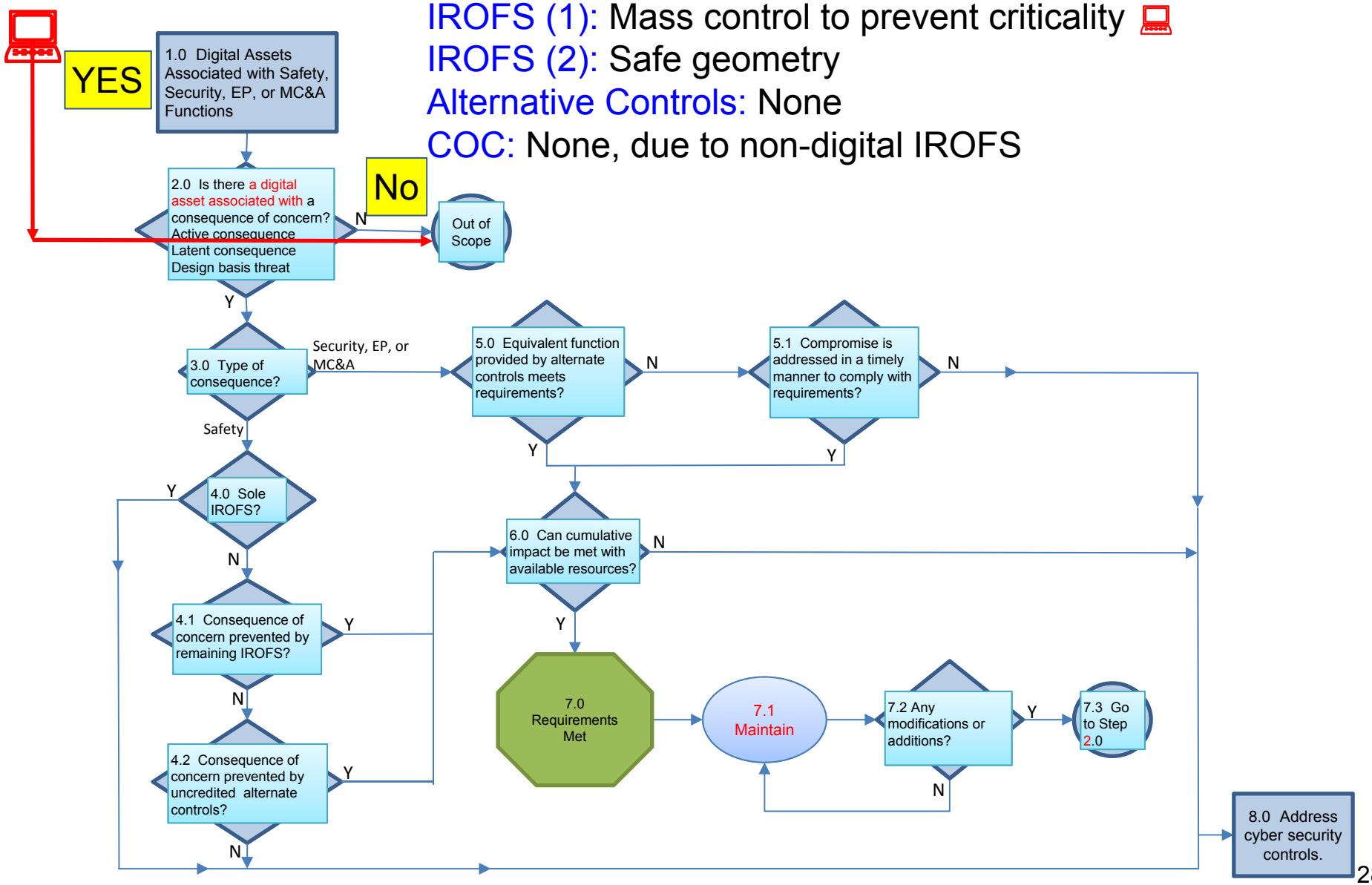
Screening Example 2: Digital combined with non-digital IROFS

Event: Portable media malware corrupts MC&A database
IROFS (1): Mass control to prevent criticality
IROFS (2): Safe geometry
Alternative Controls: None
COC: Criticality



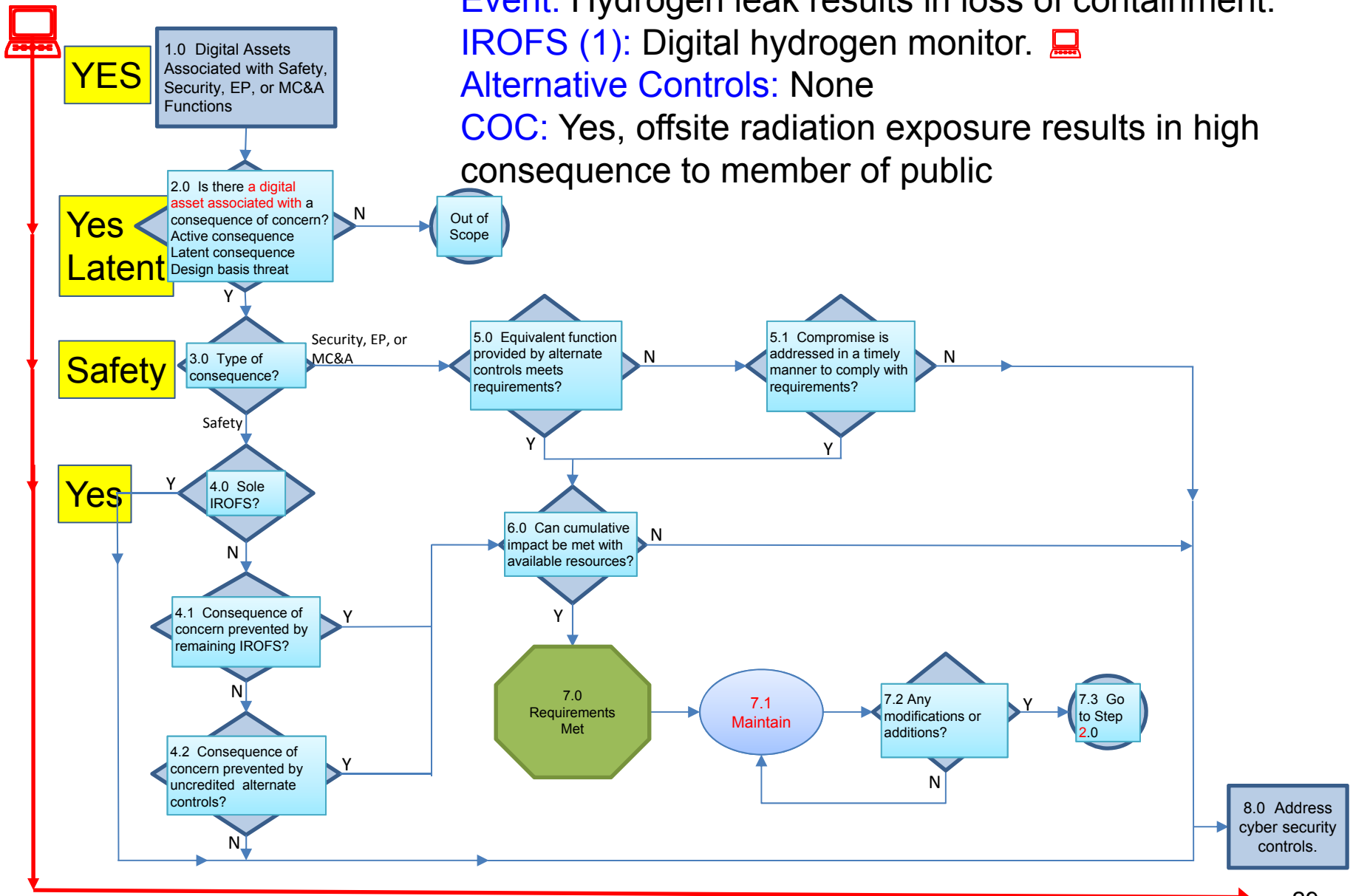
Screening Example 2: Digital combined with non-digital IROFS

Event: Portable media malware corrupts MC&A database
IROFS (1): Mass control to prevent criticality
IROFS (2): Safe geometry
Alternative Controls: None
COC: None, due to non-digital IROFS



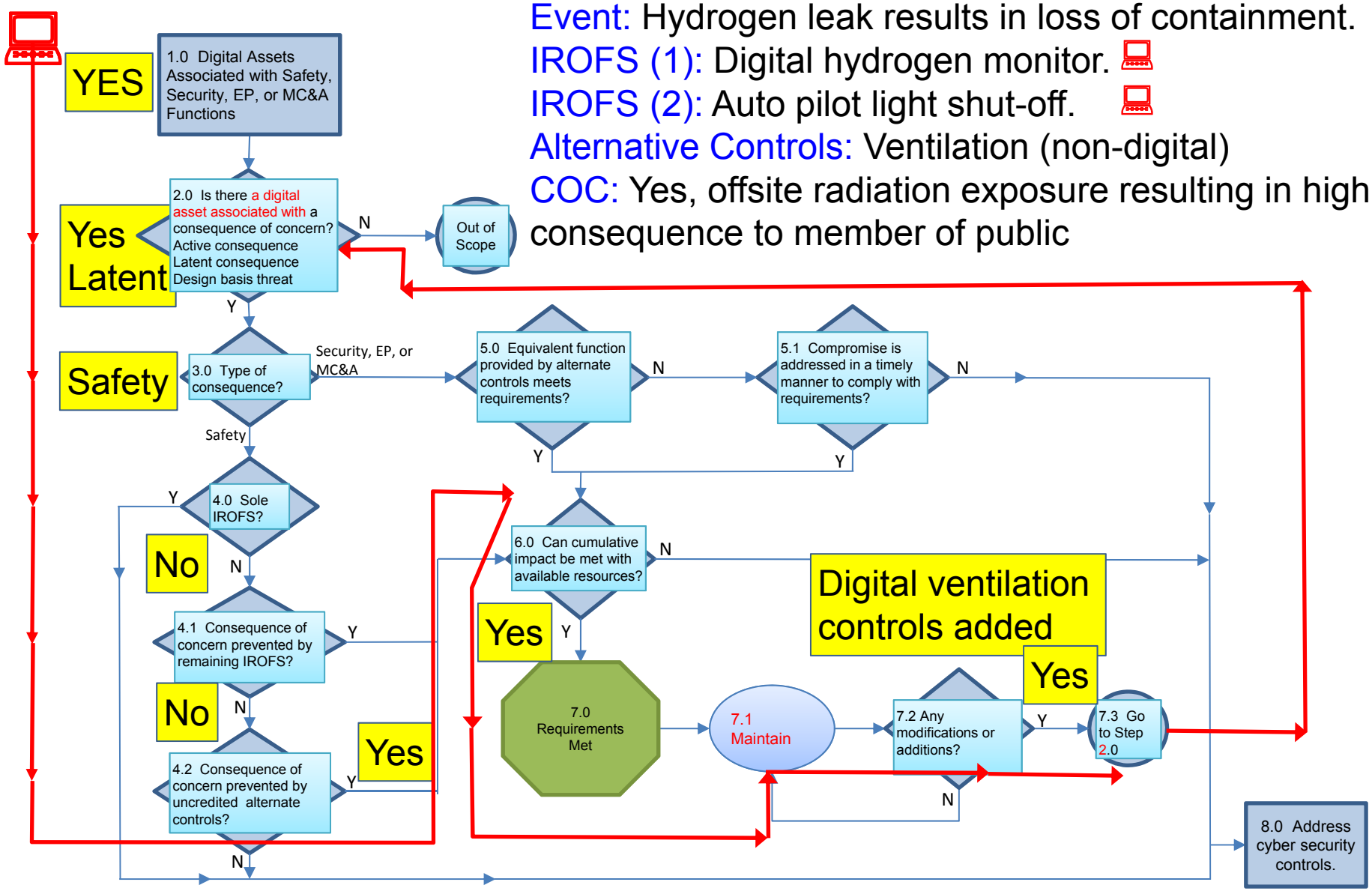
Screening Example 3: Sole digital IROFS

Event: Hydrogen leak results in loss of containment.
IROFS (1): Digital hydrogen monitor.
Alternative Controls: None
COC: Yes, offsite radiation exposure results in high consequence to member of public

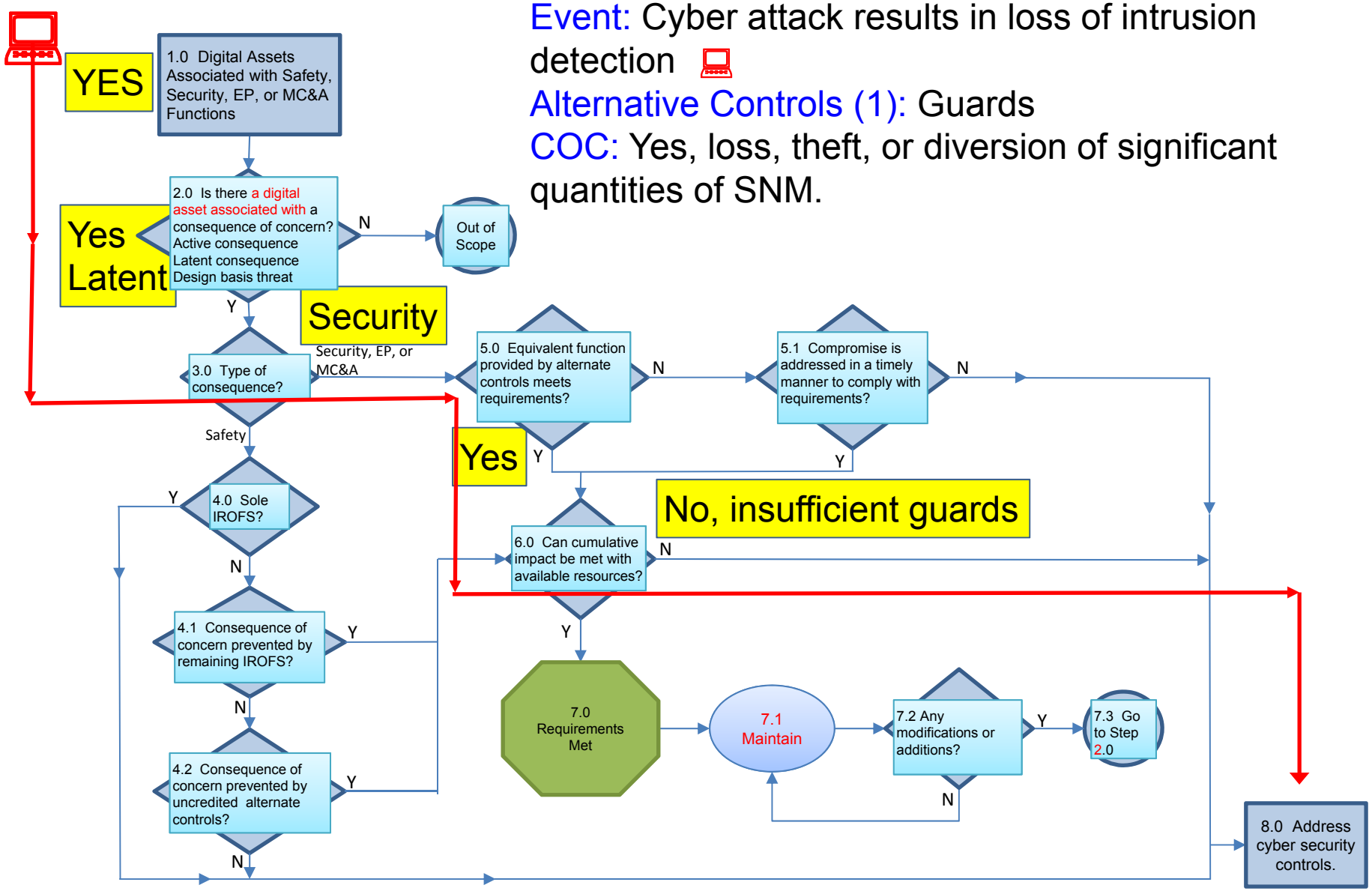


Screening Example 4: Two digital IROFS with alternate controls

Event: Hydrogen leak results in loss of containment.
IROFS (1): Digital hydrogen monitor.
IROFS (2): Auto pilot light shut-off.
Alternative Controls: Ventilation (non-digital)
COC: Yes, offsite radiation exposure resulting in high consequence to member of public



Screening Example 5: Security impact with alternative controls



Event: Cyber attack results in loss of intrusion detection

Alternative Controls (1): Guards

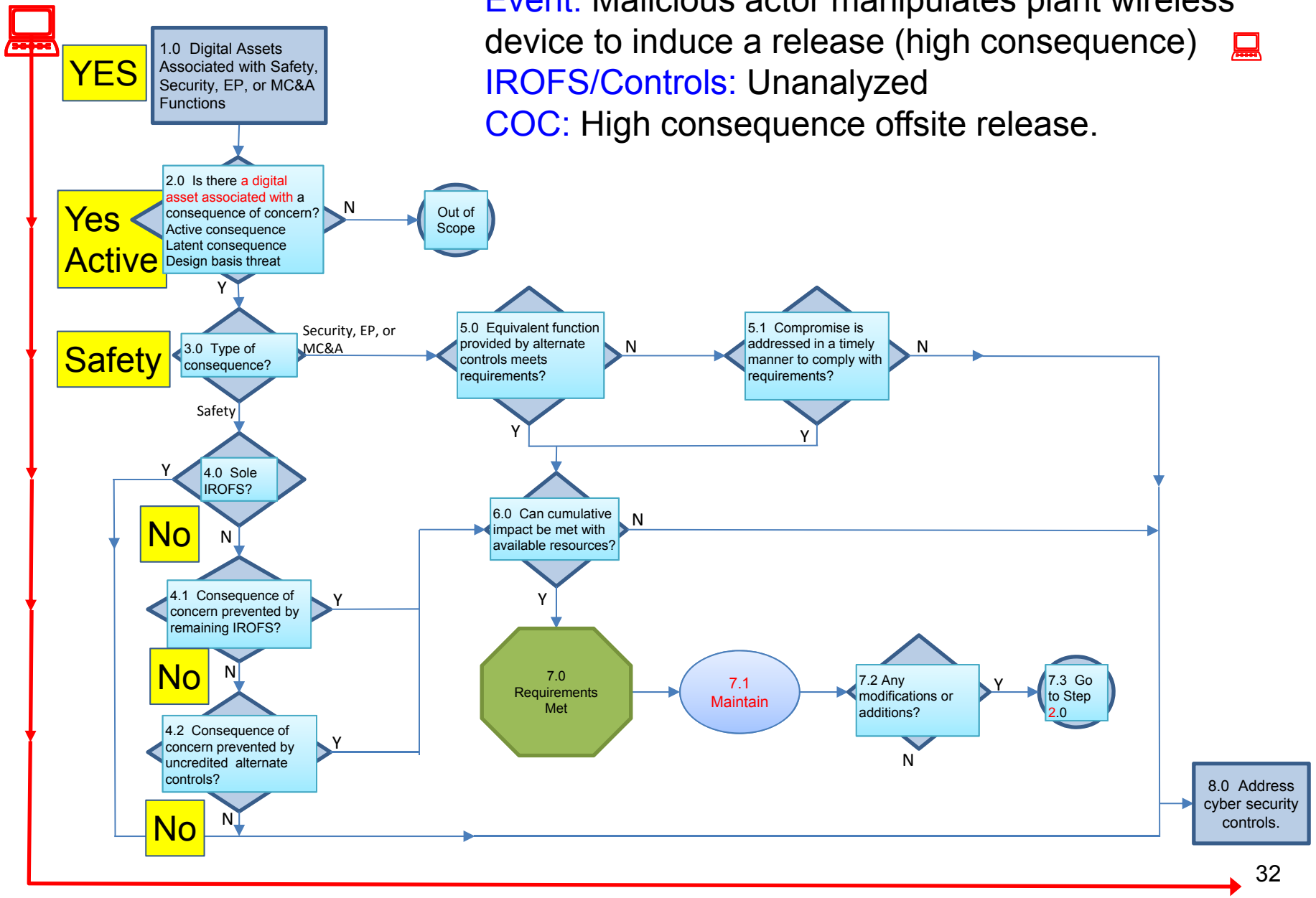
COC: Yes, loss, theft, or diversion of significant quantities of SNM.

Screening Example 6: Active consequence of concern

Event: Malicious actor manipulates plant wireless device to induce a release (high consequence)

IROFS/Controls: Unanalyzed

COC: High consequence offsite release.



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

Glossary of Terms

Consequence of concern:

Safety:

- A nuclear criticality event.
- Releases of radioactive materials or chemicals resulting in significant exposures to workers or members of the public. 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.

Security and MC&A:

- Loss/theft/diversion of significant quantities of special nuclear material.
- Radiological sabotage (limited to licensees with a DBT).
- Loss or unauthorized disclosure of classified information.

EP:

- Inability to maintain onsite and offsite communications during normal and emergency operations.

Active consequence digital asset:

Digital asset whose compromise could directly result in a safety/security consequence of concern.

Latent consequence digital asset:

Digital asset associated with SSEPMCA functions needed to prevent, mitigate, or respond to an event with the potential to cause a consequence of concern.

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

Glossary of Terms (continued)

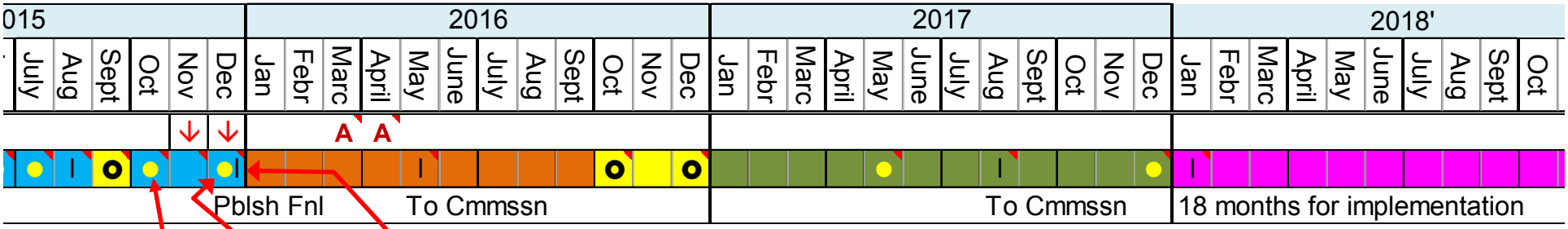
SSEPMCA function:
An action or activity that makes use of assets, personnel, policies, procedures, or programs to meet a licensing basis commitment to protect, assess, detect, respond, communicate, or provide control and accounting.

Performance-based regulation:
A regulatory approach that focuses on desired, measurable outcomes, rather than prescriptive processes, techniques, or procedures. Performance-based regulation leads to defined results without specific direction regarding how those results are to be obtained. At the NRC, performance-based regulatory actions focus on identifying performance measures that ensure an adequate safety margin and offer incentives for licensees to improve safety without formal regulatory intervention by the agency.

Risk-informed regulation:
An approach to regulation taken by the NRC, which incorporates an assessment of safety significance or relative risk. This approach ensures that the regulatory burden imposed by an individual regulation or process is appropriate to its importance in protecting the health and safety of the public and the environment.

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	

October 22, 2015, (today) public meeting

Proposal to move next public meeting to the week of December 7, 2015

Finalize regulatory basis, December 2015

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