Gain Control with Risk Management Framework

THE NIST RMF SIX STEP PROCESS

The National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) is a six step process as follows:

- **Categorize** both the information and the system based on impact.
- **Select** a baseline set of security controls.
- **Implement** the controls.
- **Assess** the effectiveness of the security controls.
- **Authorize** the system to operate.
- **Monitor** the ongoing state of protection the security controls are providing.

The RMF is a life cycle based approach. The Information Systems Security Manager (ISSM) will need to revisit various tasks over time to manage their Information System (IS) and the environment in which the system operates. Managing information security related risks is viewed as part of an organization-wide risk management activity. The RMF provides a disciplined and structured approach to mitigating risks in a highly dynamic environment of operation.

The security controls listed in the initial baselines are not a minimum, but rather a proposed starting point from which controls may be removed or added based on tailoring guidance.

Tailoring encompasses:

- Identifying/designating common controls in initial baselines
- Making risk based decisions on remaining baseline controls
- Selecting compensating controls
- Supplementing baselines with additional controls and control enhancement, if applicable.

Document in the System Security Plan (SSP) the relevant decisions made during the tailoring process, providing a sound rationale for those decisions. Tailor the controls as needed: tailor in controls to supplement the set of selected controls, and tailor out, or modify, the controls as applicable based on the system risk assessment.

Identify the security controls that are provided by the organization as common controls for all or multiple systems under the organization's control and document the controls in the SSP.

Control implementation can be characterized as:

System Specific – Security controls that provide a security capability for a particular system and are the primary responsibility of the Information system owner (ISO)/ISSM. (Example: IA-6, Authenticator Feedback, the system is configured to obscure the feedback of authentication information during the authentication process by displaying asterisks when a user types in a password.)

Common – Security controls that are inheritable by one or more organizational systems and are typically provided by the organization or the infrastructure (Examples: Physical and environmental security controls, Network boundary defense security controls, Organization policies or procedures, etc.). The benefits of common security controls include:

- Supporting multiple information systems efficiently and effectively as a common capability
- Promoting more cost-effective and consistent security across the organization and simplifying risk management activities
- Significantly reducing the number of discrete security controls that have to be documented and tested at the system level which in turn eliminates redundancy, gains resource efficiencies, and promotes reciprocity.

Hybrid – Security controls that are implemented in part as a common control and in part as a system specific control. If any of the information system components need system-specific infrastructure protections, in addition to common controls that apply, the control is implemented as a hybrid control (Example: Emergency power may be implemented as a common control for the facility in which the system resides, but the specific system requires additional availability protection based on the criticality of the information in the system to the organization's mission resulting in the implementation of a separate uninterrupted emergency power source).

Tailoring Security Controls

The second step begins with the selection of a baseline of controls and/or application of a DSS overlay that addresses the impact level designated in the first step. The overlay identifies security control specifications needed to safeguard classified information that is stored, processed, or transmitted. The overlay adopts a minimum baseline of Moderate-Low-Low (M-L-L). The DSS overlay applies to Standalone Systems (Single User Standalone (SUSA) and Multi User Standalone (MUSA)) and Isolated LAN (ISOL)/Peer-to-Peer (P2P).

The second step is further refined by the tailoring and supplementation of the baseline set of controls as needed. The baseline set was designed with a general purpose and it should be noted that the controls need some level of customization for a good fit. In the past, this step has been underutilized which could introduce unnecessary risk if not addressed properly.

Tailoring is necessary because baseline controls include assumptions that may limit the applicability or effectiveness of controls, as follows:

- Information systems are located in physical facilities
- User information is relatively persistent
- Information systems are multi-user
- Some user information is not shareable
- Information systems exist in networked environments
- Systems are general purpose
- Resources exist to implement controls.

When these general assumptions do not fit the information systems or the environment it is operating in, some controls will likely need tailoring to address security risks. Because of the general nature and purpose of the baselines, there may be situations in the security needs of the system that are not addressed by the baseline. Here are some possible examples:

- Insider threats
- Classified data on systems
- Advanced Persistent Threats (APT)
- Specialized protection requirements
- Connections across differing security domains.

The tailoring process involves the following steps:

- Designate common controls.
- Apply scoping considerations.
- Select compensating controls.
- Supplement the baseline controls.
- Provide implementation specifications.

DESIGNATING COMMON CONTROLS

What are Common Controls?

Common controls are security controls that can support multiple information systems efficiently and effectively as a common capability. They are the security controls that are inherited as opposed to the security controls individually selected. Different systems often share some controls that are identical and can be managed centrally for the entire organization. This can eliminate the need for redundant development and operation of security controls by multiple ISOs. Additionally, common controls provide for uniformity that would just not be possible if each were implemented on their own.

When common controls are declared, some of the workload of security planning is consolidated, making the process more consistent, more cost effective and easier to achieve and maintain compliance and authorization. Common controls are not a subset of the security controls found in NIST Special Publication (SP) 800-53 Security and Privacy Controls for Federal Information Systems and Organizations (Rev 4). In fact, any type of security control or protective measures used to meet the Confidentiality, Integrity, and Availability (CIA) of the information system can be a common control if it can be shared effectively. Common controls increase consistency across systems and are more cost effective for both management and analytics. Additionally, they force a clear definition of responsibility, can be centrally managed, and are a precursor to other tailoring measures.

NOTE: Common controls can have one status for one system and another status for another system and should be selected on the basis of context, not simply by the language in the control.

Types of Common Controls

When controls apply to a single system, they are system-specific controls (not common). However, when they can apply to more than one system, they can be considered common controls. When some part of a control applies to a single system, while other parts of a control can apply to more than one system, they can be considered hybrid controls.

All security controls should be declared as either common, system-specific, or hybrid.

NOTE: The PM family of controls are considered to be foundational to the rest of the security controls and are NOT considered to be candidates for common controls. However, the first control in each of the other families addresses Policy and Procedure, which are good candidates for common controls. (e.g., AC-1, AT-1, AU-1, CA-1).

Understanding When to Use Common Controls

The organization should build a portfolio of common controls first to determine the boundaries of the security the controls provide for the information system. This task will reveal what remains to be addressed by the system specific-controls, which common controls need to be tailored for the organization's specific threat profile, and what tools are needed for continuous monitoring. Use the following questions to frame the task:

- What are all of the common controls for this information system?
- What areas of operation/components cannot be addressed by common controls?
- Which controls are acceptable based on the threat profile?
- Which controls need to be enhanced in order to meet security requirements?
- How many of the controls overlap or do the same things?

Inheritance of Common Controls

The implementation of common controls can provide a security capability that is inheritable by multiple systems. For example, the information system hosted in a data center will typically inherit numerous security controls from the hosting provider, such as

- Physical and environmental security controls
- Network boundary defense security controls.

Other inheritance scenarios include company, facility, or departmental-level policies or procedures that can be leveraged by all systems within the organization, organization-side security monitoring capabilities, public key infrastructures (PKI), etc. Organizations implementing common controls are referred to as Common Control Providers (CCPs).

It is possible for an information system to inherit just part of a control from a CCP, with the remainder of the control provided within the system boundary. Also, it is possible to inherit a control from two or more CCPs. For example, an information system whose system boundary spans multiple sites (i.e., a primary site and an alternate processing site) will most likely inherit physical and environmental security controls from the data center providers at both sites. In order for a system to inherit a particular security control, the following should be true:

- The control is implemented and managed outside the boundary of the inheriting system
- The CCP has designated the particular control as inheritable
- The CCP has an Authorization to Operate (ATO) or equivalent evidence that the control is in fact in place

Specific Common Control Challenges

Common controls present unique challenges that must be managed and maintained properly due to the complexity involved. Just as common controls can reduce the operational effort of the security controls, they can also increase the management of said controls. Common controls can touch many components of the system or even multiple information systems, and for that reason, any change in one common control can have a cascading effect on multiple sites. This could result in a change in security posture for one facility but not another. Additionally, when building a common control portfolio, the ISO/ISSM needs to understand who owns each common control and how the provider interacts with the system. Common controls are part of the organization's shared infrastructure whether the applications are hosted in the cloud, on-premises, or some combination. The ISO/ISSM must be diligent in determining how the common control interacts organization wide and ensure responsibilities are assigned to a system, an ISO, or a group.

Redundancy is another factor that should be vetted during the assessment phase, the fourth step in the RMF process. More than one control can address the same security risk, such as multiple sets of application permissions that provide users with access to services, or different physical access control safeguards that deal with access to different components each with their own unique or slightly nuanced way of addressing the physical access control risks. Analyzing common controls to address any redundancy requires attention to the function and effectiveness of the control in light of the organization's unique security posture.

Common Control Provider

The common control provider manages risk related to common controls and how they manage changes to those controls when new threats or vulnerabilities are found. The CCP is responsible for:

- Documenting common controls in a security plan
- Ensuring that common controls are developed, implemented, and assessed for effectiveness by qualified assessors with a level of independence required by the organization
- Documenting assessment findings in a security assessment report
- Providing a Plan of Action and Milestones (POA&M) for all common controls deemed less than effective (i.e., having unacceptable weaknesses or deficiencies in the controls)
- Receiving authorization for the common controls from the Authorizing Official (AO) and
- Monitoring common control effectiveness on an ongoing basis.

The common control provider needs to have the capability to rapidly broadcast changes in the status of common controls that adversely affect the protections being provided by and expected of the common controls. In addition to documenting system-specific security controls, the organization's common control portfolio analysis needs to document how the controls will be managed.

APPLYING SCOPING CONSIDERATIONS

Some controls may not be applicable or appropriate for use in a specific system or operating environment. These controls may need to be modified or replaced by another control, or even eliminated entirely from the baseline. When this is done, any protections lost by changing controls must be included in risk assessment documentation and may need consideration for other methods of mitigation. Under NIST guidance, we are allowed the flexibility to make "explicit risk-based decisions" on how to make scoping changes in order to achieve the needed security requirements. Any scoping changes that are made should be documented in detail in the SSP to explain the nature of the change, the risk analysis involved, and the rationalization for accepting the final risk posture after the change.

The following areas should be considered for scoping:

Control Allocation and Placement

Security controls are applicable only to system components that provide or support the information security capability addressed by the controls. Some of the controls that are included in the baselines may not apply to some systems or may not apply to some system components.

Operational Environment

Assumptions about the existence of certain operational/environmental factors are built in to some controls. The baseline may need tailoring when these factors are significantly changed or absent. The following is a list of common operational/environmental factors to consider:

- Mobility – The basic assumption is that systems are in fixed locations and non-mobile facilities. If the systems are mobile, the security controls may need tailoring.
- Single-User Systems and Operations – For systems that are intended to be used by a single user over time, controls that deal with shared access, concurrent access, and other multi-user issues may not be required.
- Data Connectivity and Bandwidth – Systems that are not networked or have limited networking or bandwidth requirements may not need controls that deal with connectivity. A careful analysis of connectivity may be required.
- Limited Functionality Systems or System Components – Items that may be considered as information systems or system components that have limited capabilities (printers, scanners, cameras, phones, tablets, and more) may also have limited requirements for some controls.
- Information and System Non-Persistence – Many controls assume there will be some level of persistence involved with both data and the systems themselves. If there is little or no persistence, controls may not be needed. This will particularly apply to controls dealing with storage and backup, but the growing use of virtual machines may also require some attention in this area.

- Public Access – There may be large differences in the security requirements of systems that allow public access and those that do not. The areas of Access Control and Identification and Authentication may require close attention.

Security Objectives

While the overall security objectives are to protect CIA, individual controls may support only one or two of those objectives. Since the overall Impact level for any system uses the "high water mark" rule, it becomes possible for a baseline to include controls that are not needed or should have a lower level of importance. In those cases, the appropriate controls may be downgraded or eliminated to correspond to the lower impact level baseline. When this is done, the downgrading change must:

- Reflect the correct impact level for the CIA objectives that are supported
- Be supported by an assessment of risk
- Not adversely affect the level of protection.

The following controls and control enhancements are candidates for downgrading:

- Confidentiality: AC-21, MA-3 (3), MP-3, MP-4, MP-5, MP-5 (4), MP-6 (1), MP-6 (2), PE-4, PE-5, SC-4, SC-8, SC-8 (1)
- Integrity: CM-5, SC-8, SC-8 (1), SI-10
- Availability: CP-7

Technology

Controls that refer to specific technologies are applicable only if those technologies are implemented in the system. Controls do not require automated mechanisms to be developed if they do not already exist. If automated mechanisms are not available, compensating controls are used to meet requirements.

Mission Requirements

When a control interferes with or degrades mission/business functions, it may not be applicable or appropriate.

SELECTING COMPENSATING CONTROLS

Compensating controls are alternative controls to those in existing baselines and only selected after scoping considerations. The baseline NIST SP 800-53 controls must be considered first as they lay the foundation for the security posture. If it is determined in the Risk Assessment that the original control may not meet the requirement, document why the original control could not be used and how the new control provides adequate security protection. The organization then must assess and accept the risks involved with using a compensating control.

SUPPLEMENTING THE BASELINE CONTROLS

Supplementary controls are used for enhancing security without changing the baseline control selection when the risk assessment has determined that the information system would need additional protection for a solid security posture.

Additional security situations may require but are not limited to:

- Advanced Persistent Threat (APT) – SC-7 (13)
- Connections across security domains – AC-4 control enhancements
- Classified information –AC-16.

Alternative strategies include:

- Restrictions on types of technologies
- Limiting information or the manner of automation
- Prohibiting external access
- Prohibiting information on publicly accessible system components.

Good common control candidates that should be considered:

- AC-2 (0) (1) (2) (3) (4)
- AC-17 (0) (1) (2) (3) (9)
- AC-18 (0) (1) (3) (4)
- AC-19 (0)
- AC-23 (0)
- AT-2 (0) (2)
- AT-3 (0) (2)
- AT-4 (0)
- AU-6 (0) (1) (3) (5) (9)
- AU-7 (0) (1)
- AU-11 (0)
- AU-16 (0)
- CA-2 (0) (1)
- CA-3 (0) (2)
- CA-7 (0) (1)
- CA-9 (0)
- CM-2 (0) (1) (2)
- CM-3 (0) (4)
- CM-4 (0)
- CM-6 (0)
- CM-7 (0) (5)
- CM-8 (0) (2) (3)
- CM-9 (0)
- CM-10 (0)
- CM-11 (0)
- CP-7 (0)
- SI-2 (0) (1)
- SI-3 (0) (1)

PROVIDING IMPLEMENTATION SPECIFICS

To effectively implement the common controls, it is necessary to define the intent of a control and ensure security requirements are met. This is typically identified when developing the organization's risk-based cybersecurity strategy and documented in the SSP. Consider that the implementation of the common control may alter the security posture in subtle ways and could involve:

- Refinement of implementation details
- Refinement of scope
- The application of a control to different scopes based on the iteration.

The Last Word

Build your portfolio of common controls first and determine the boundaries of the security they provide for your information system. Once the rules of engagement for these common controls are defined, you will be in a better position to understand the scope of the system specific-controls you'll need to deploy, which common controls need to be tailored for your specific threat profile and what tools you'll need for continuous monitoring in your risk management framework based cybersecurity strategy.

REFERENCES:

The DAAPM

NISPOM

NIST 800-30

NIST 800-53

Visit www.dss.mil/rmf for the DSS RMF Resource Center for additional information.

Contact your local DSS Information Systems Security Professional (ISSP) if you have questions.