



Section 1

Introduction to Organizational Security Risk Management



Section 1

Introduction to the RMF

Martin Yanev

Introduction to the Course

- The goal of this Course is to provide a comprehensive understanding of the strategic risk management process as well as the underlying principles and a standard risk management framework
- Risk management entails a formal set of steps that are carried out to protect an organization's assets from harm that may be caused by inadvertent or deliberate acts of destruction.
- Risk management involves a systematic architecture comprising all the necessary controls to prevent unauthorized use, loss, damage, disclosure, or modification of organizational information
- In this Section, we also discuss the general uses for the framework and the contexts in which it applies.





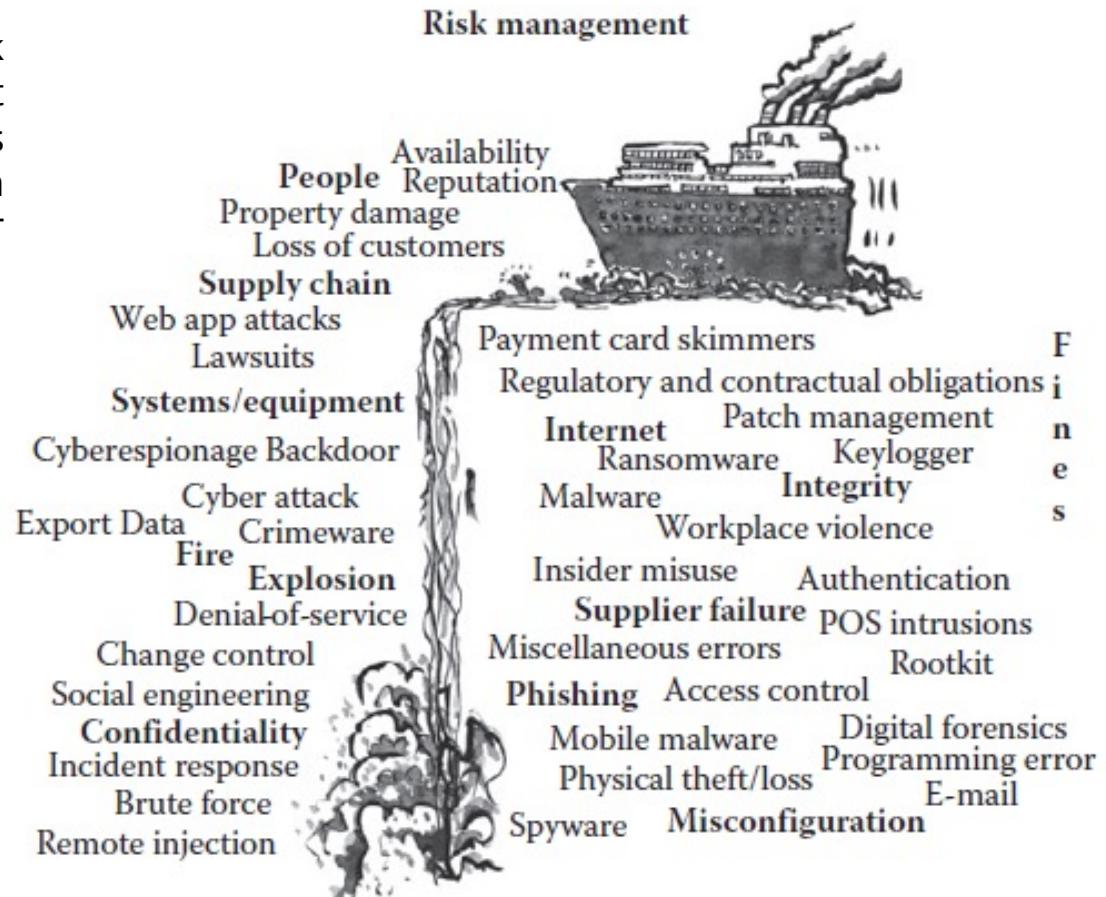
Section 1

Risk Is Inevitable

Martin Yanev

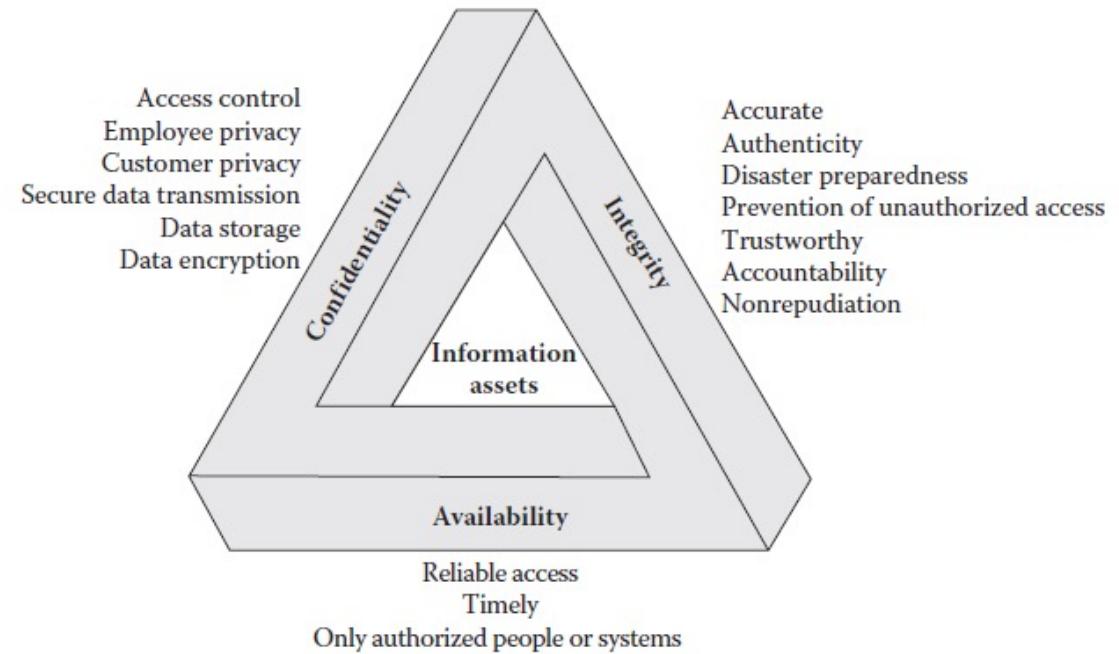
Risk Is Inevitable

Risk is a fundamental element of human life in the sense that risk is always a factor in any situation where the outcome is not precisely known (Figure). In addition, the necessary calculations that we make about the probability of some form of harm resulting from an action that we take are generally a given in our decision processes.



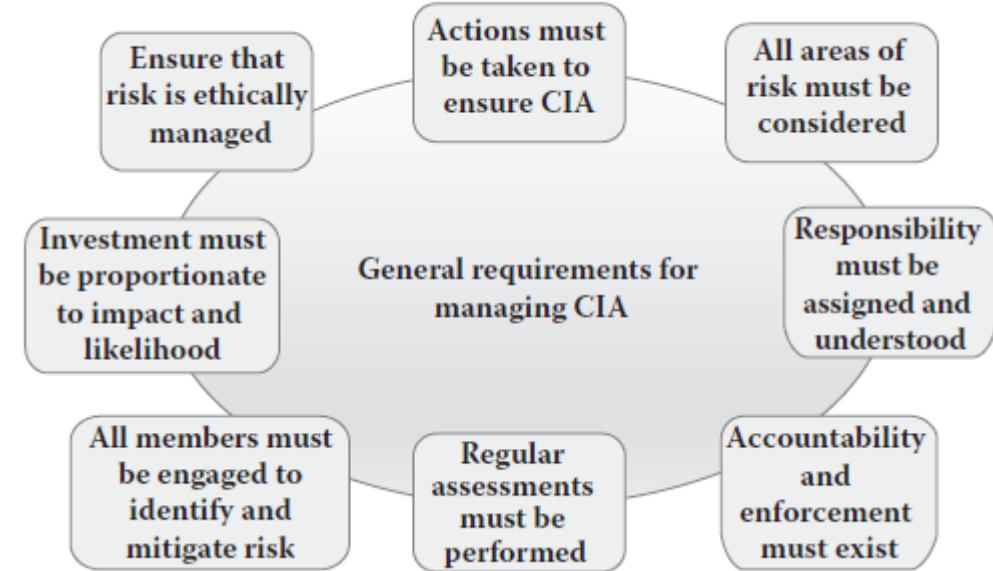
The confidentiality, integrity, and availability (CIA) triad

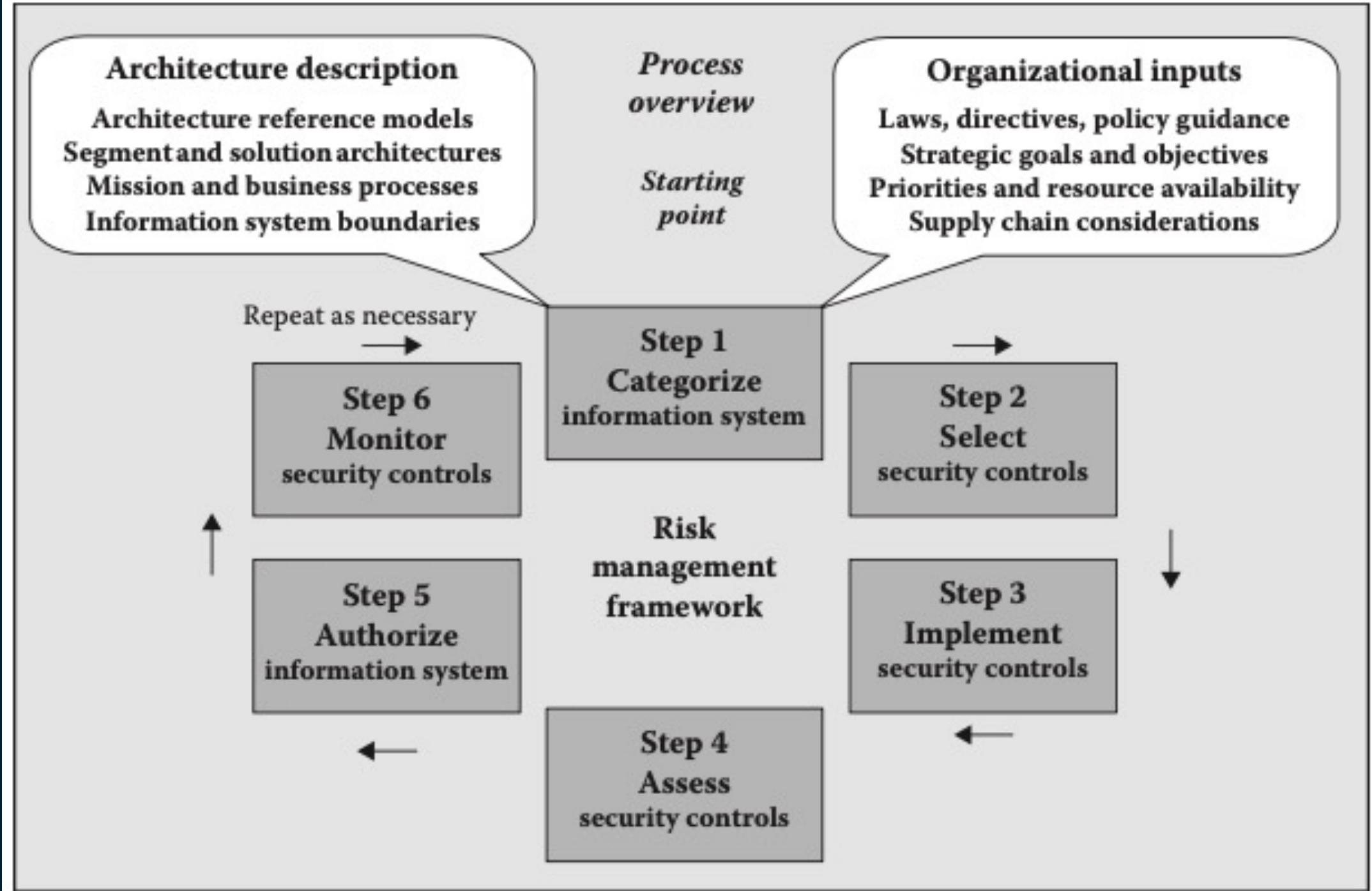
ICT assets are something of value to the business. The risk management process specifically ensures the assurance of three generic protection criteria, as shown in Figure. These three criteria assure against meaningful loss of **confidentiality**, loss of **integrity**, and loss of **availability** (CIA)



Requirements for meaningfully managing CIA

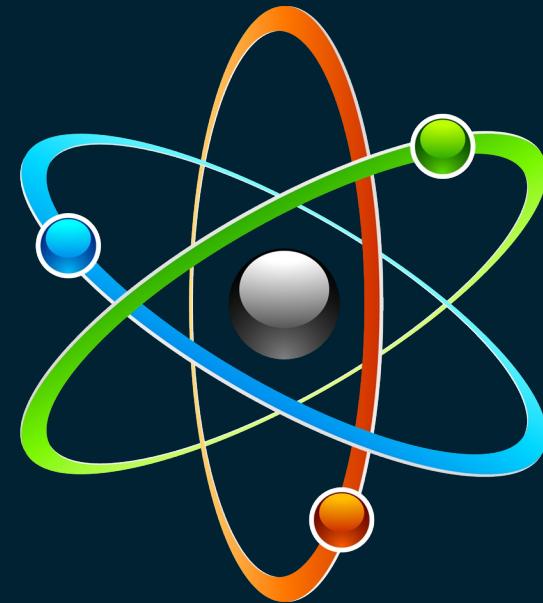
Because every organization is unique and implements security differently, the actual process to identify, evaluate, and ensure that the meaningful risks in each of the CIA areas are properly managed generally involves the same eight requirements,





Atomic Level

- The atomic-level components of the risk management process are a set of substantive security controls that ensure the requisite level of assurance against loss. These security controls should be traceable directly to the individual policies that defined their need.
- One problem is that the term “risk management” is rather nebulous. So, the overall process itself requires a definition of what risk management means. A concise statement and commitment to the work is needed in order to make the practice standard.



Strategic Governance and Risk Management

Strategic Governance and Risk Management

- Starting from the assumption that a standardized risk management process should be applied organization-wide (which is what we believe), risk management is a strategic issue, rather than a narrow technical concern.
- The reason to adopt an organization-wide risk management approach is to avoid the dysfunctional effects of a typical piecemeal solution where every department is managed by its own commonly accepted business practices.
- One problem is that those approaches are often not coordinated effectively in the operational environment



Strategic Governance and Risk Management

- The alternative approach to piecemeal risk management is a formally defined and instantiated architecture of comprehensive risk management best practices, which are specifically aimed at optimizing risk controls within the company .
- Risk management is basically built around information. In effect, risk management gathers and utilizes information from all sources, in order to decrease the possibility of future risks.
- In addition to providing the information that helps guide strategic decision-making about risks, the risk management process also makes certain that a commonly accepted and systematic set of policies and procedures are in place to handle known risks.



Elements of Risk Management

In simple terms, the risk management process assesses the likelihood that any given action will adversely impact something of value to any given entity. That includes things of personal value such as money, health, or even life. Once those risks are known, the risk management process deploys all of the measures that are necessary to ensure that consequent harm does not occur.



Elements of Risk Management

- Because identification and understanding are such important aspects of risk management, assessment provides the fundamental focus of the process.
- Given its focus on the support of substantive decision-making, an important underlying factor in risk evaluation is the uncertainty principle.
- It goes without saying that it is easier to identify and evaluate risk in less complex environments.
- The issue of threat management is important to our existence as a nation because ICT is the platform on which our modern society rests.



Elements of Risk Management (Cont.)

- The key concept is “commonly accepted.” A commonly accepted model of best practice establishes a standard point of reference.
- Another underlying issue is how to get the most effective assurance out of the organization’s limited resources.
- A coherent set of best practice methods, which let decision-makers benchmark existing and planned risk management resource usage, using the most expert advice available, is an important strategic management tool.



Elements of Risk Management

The NIST's RMF was designed to offer a structured, yet flexible, means for analyzing and deciding how to alleviate the risks that arise from the information systems within an organization.



Risk Types and Risk Handling Strategies

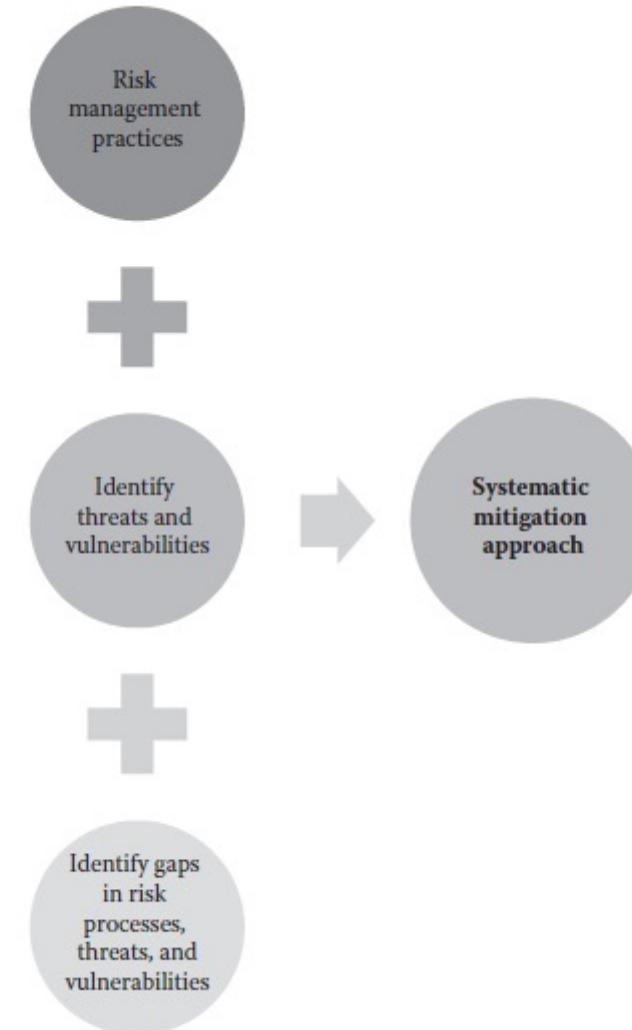
Risk Types and Risk Handling Strategies

- An important feature of the RMF is that it provides a practical basis for developing and maintaining comprehensive risk management controls for all aspects of a business's information assets.
- The goal of the RMF initiative is to define and communicate a commonly accepted and standard basis for building risk management best practice.
- It is designed to enable ICT managers to leverage their levels of risk awareness to a higher status. It allows companies to identify gaps in their risk management processes.
- Organizations have to document that they have considered the risk to their assets and have control measures in place to protect themselves against it.



Risk Types and Risk Handling Strategies

An important feature of the RMF is that it provides a practical basis for developing and maintaining comprehensive risk management controls for all aspects of a business's information assets. The objective of the RMF is to provide a common sense basis to develop, implement, and measure effective risk management practices. It is implemented through an organization-wide participative process and any business that has faced compliance issues with FISMA or NIST should be able to easily follow the RMF process.



Risk Types and Risk Handling Strategies

- The RMF applies equally to building assurance as well as the long-term maintenance of assurance for information assets, embodied in organizational ICT systems
- Since the RMF touches on every aspect of how to assess and manage risk, it forces companies through a step-by-step evaluation of their needs and responsibilities with respect to their ICT function.
- In essence, an optimum approach is engineered out of the RMF model for each individual organization.
- Then, explicit control specifications are defined for each of the applicable areas of security risk management using the control recommendations of NIST SP 800- 53 Revision 4.





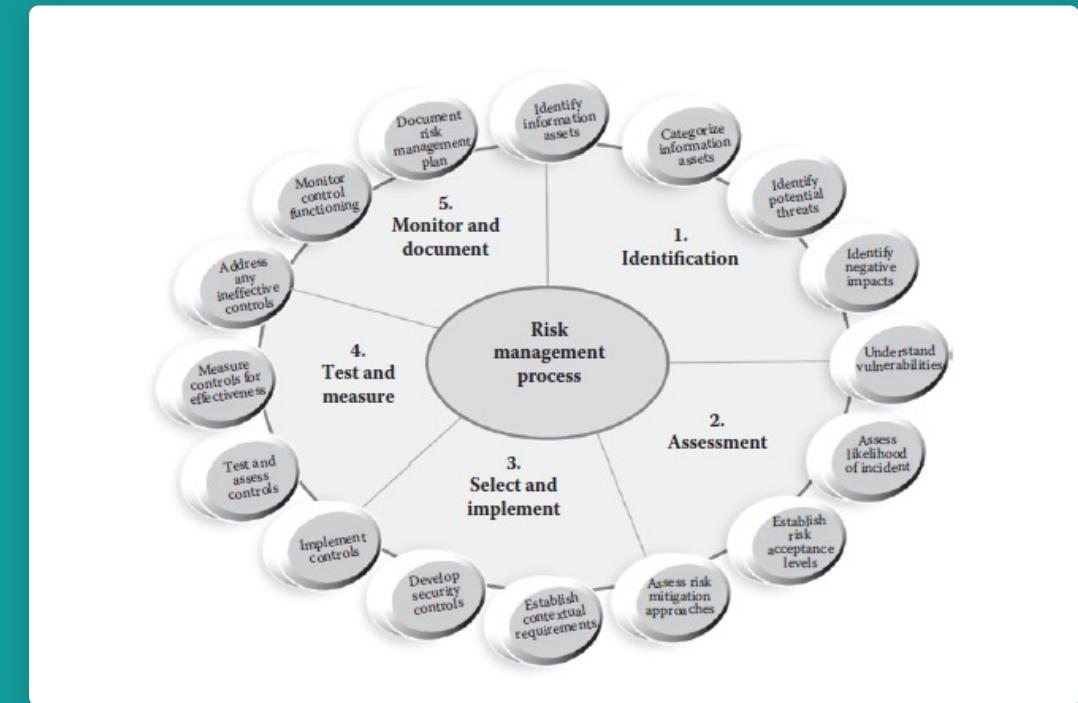
Section 1

Overview of the Risk Management Process

Martin Yanev

Overview of the Risk Management Process

The steps to establish a standard risk management process involve five generic organizational functions: identification, assessment, control selection and implementation, test and measure, and continuous monitoring



Establishing the Risk Management Planning Process

- The risk management plan shapes the risk management process. The primary role of the risk management plan is to create the framework for the detailed policies and procedures that will comprise the risk management process for the particular organization.
- The top-level risk management plan provides the strategic context that is needed to ensure that the organization's overall business objectives and goals are understood and then factored correctly into the decisions that are made about risk.
- Finally, the concepts associated with risk management have to be defined in clear organizational-specific terms. That definition is necessary in order to align the organization's overall security objectives with its business objectives.



Identifying and Categorizing the Risk Environment

Identifying and Categorizing the Risk Environment

- The next step in establishing effective risk management is to acquire comprehensive knowledge of the threat environment. That knowledge requires an all-inclusive record of the organization's assets, a statement of the acceptable levels of risk for each asset, and the constraints that will be placed on the protection of the asset by the available resources, technology, or existing policies.
- Another approach to risk management is the coordinated approach. Because it is meant to provide comprehensive protection, the coordinated approach offers more effective risk management.



Identifying and Categorizing the Risk Environment

- The most common way to conduct the deployment is *ad hoc*.
- Another approach to risk management is the *coordinated approach*



Risk Assessment

Risk Assessment

- All risk assessments provide two specific pieces of knowledge
 - (1) the probability of occurrence
 - (2) the estimate of the consequences
- Risk assessments are built around tangible evidence.
- Risk assessments typically target the various standard areas of threat—electronic, human, and physical.



Designing for Effective Risk Management

Designing for Effective Risk Management

- Context
- Scope and Boundaries
- Roles and Responsibilities
- Definition of Priorities
- Sensitivity of the Information



Context

Every risk management process has to be designed to fit its particular environment. Environmental considerations are the factors that have to be understood in order to fit the risk management process into the overall operating circumstances of the organization. Accordingly, the design should describe all technical and environmental factors that might impact the risk management process.



Scope and Boundaries

Once the context about the scope or area of coverage is understood, the actual assurance has to be explicitly defined. The definition should be the result of a formal planning exercise. Formal planning is required because tangible organizational resources are involved. And failure to define an accurate and realistic scope for the risk management process could result in deficient protection and wasted resources.



Roles and Responsibilities

The definition of roles and responsibilities is a critical step in designing the risk management function since they tie both personnel and financial resources to the activities that will be performed. It is also important to explicitly clarify the duties that are associated with each of those roles.



Definition of Priorities

In addition to identifying and relating the various resource elements, each of these elements has to be categorized in terms of their general priority. Priority is directly related to the criticality of the resource. It is essential to be able to know the priority of each component in order to decide how many resources to commit to its protection.



Sensitivity of the Information

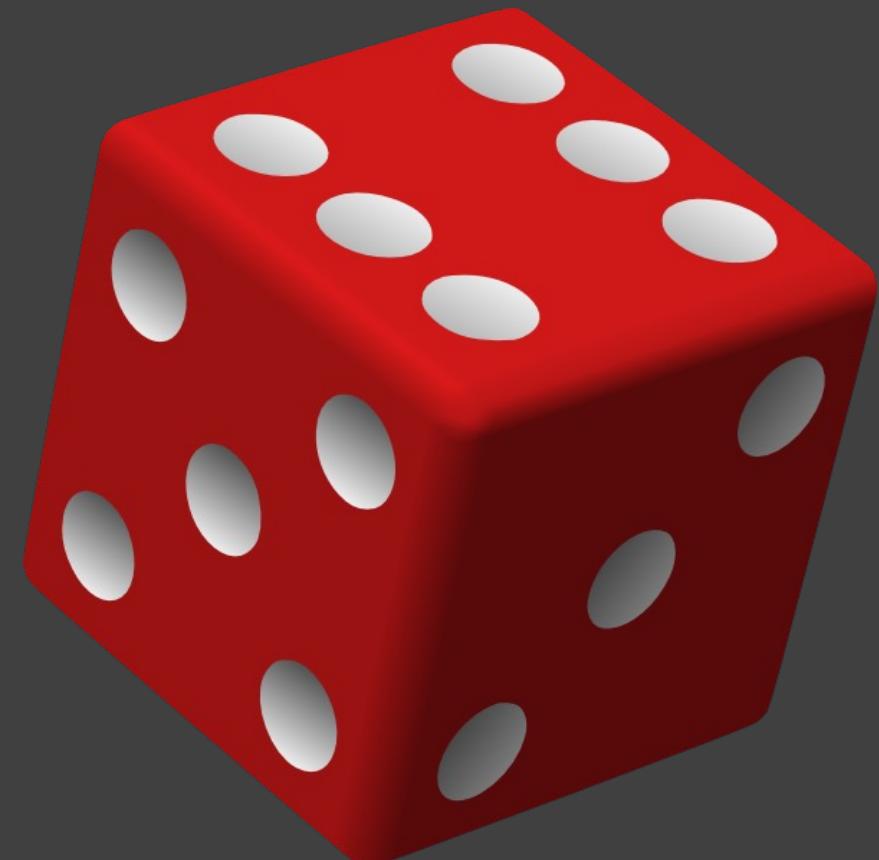
It is essential to specify the sensitivity of each item of information within the system. That is because the sensitivity of the information determines the levels of CIA required. Thus, this specification provides the necessary basis for determining the extent and rigor of the controls. The specification also provides the basis for deploying the selected risk controls that will be used to secure each component.



Evaluating Candidates for Control

Evaluating Candidates for Control

- In order to ensure that the analysis is comprehensive, data flow diagrams or similar information flow diagrams such as unified modeling language (UML)-based use-case diagrams are employed to help visualize and describe the target space.
- Subsequently, the implications of each threat must be analyzed. This analysis is typically based on assigning a criticality score.
- A focus on priority differs from the typical low-hanging fruit approach. Nevertheless, the implementation process has to be based on some kind of quantitative or rational method for assigning priorities.



Implementing Risk Management Controls

Implementing Risk Management Controls

- The controls for risk management differ in their purpose and specificity. It is important to keep this difference in mind when designing and then assigning control activities because the people who will actually be executing each control need to know exactly how to perform all of the tasks that are necessary to make the control effective.
- As a consequence, it is important to ensure that management types are not asked to perform highly technical tasks, just as it is equally critical that technical people are not asked to perform managerial activities.



Implementing Risk Management Controls (Cont.)

→ Management Controls

- Management controls are behavioral and based on policies designed to employ the organization's risk management procedures. Examples of management controls are incident response, security assessment, and planning controls.

→ Technical Controls

- Just as with the management process, the technical controls should also be well defined, understood, and followed. From a risk management standpoint, obvious technical controls are those that underlie the access control system.

→ Risk Type

- Risks represent a threat to some aspect of organizational functioning. Moreover, the management of risk is a complex process with lots of inherent detail. As mentioned previously, in order to implement the risk management process, it is necessary to classify and understand the nature of the threats that are present in the organization's current operating environment. In general, threats can be classified into two categories, *known* and *unknown*.



Implementing Risk Management Controls

- The management risk category encompasses the potential risks to the organization's information assets or documentation, as well as any of the risks that are associated with the assignment of roles and responsibilities and the risks represented by a failure to do proper contingency or configuration management planning.
- Operational risks are much more focused and detailed.
- The technical controls risks include the predictable threats to electronic systems; however, they also include any electronic controls over media and the physical and personnel security environment.



Assessment and Effectiveness of Risk Controls

Assessing the Effectiveness of Risk Controls

Forms of process assessment and measurement are important elements of good management practice. Assessment tells decision-makers whether or not their operational objectives are being met, that the results they are getting are in line with expectations, or even whether a process is under control. Risk management is no different than any other management activity in that regard.



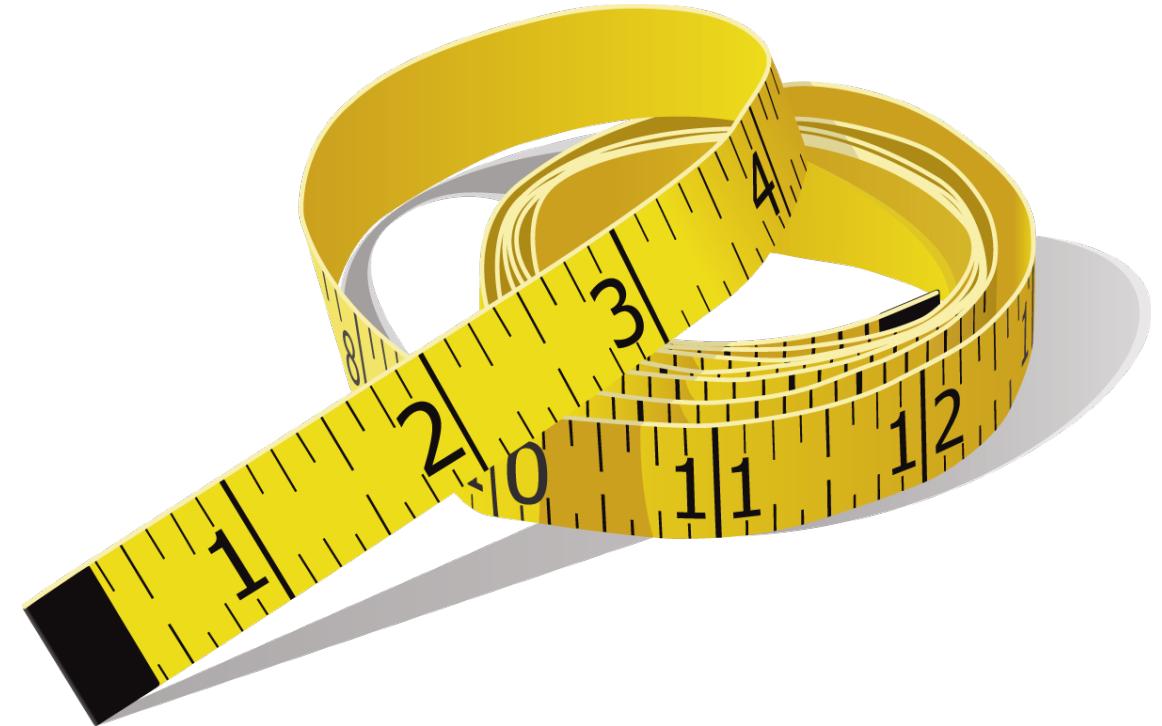
Qualitative Measurement

→ Qualitative measurement does not utilize actual metrics, but rather focuses on relative differences. Graphic scales are commonly used in qualitative analysis. Numbers may also be used, but they are merely markers for comparison value, not actual representative quantities. The end result of a qualitative risk assessment is a matrix of threats that differentiates between different relative levels of likelihood and impact.



Quantitative Measurement

- If there is a need for a more granular understanding of the risk situation, then quantitative analysis methods can be used. The value of quantitative methods depends upon the quality of the data being used. For instance, in the case of something like an actuarial estimate, hard evidence like the accuracy of records of birth and death and the causes of injury and loss, coupled with other factors, can be used to build predictive mathematical models





Section 1

Sustainment

Martin Yanev

Sustainment: Risk Assessment and Operational Evaluation of Change

- Because the business environment is constantly changing, it is necessary to do continuous operational assessments of the risk environment in order to assure the validity of the risk management controls for the organization. Operational planning should be aligned with business goals and their accompanying strategies.
- Consistency of measurement is a critical factor because stakeholders have to share a common understanding of the precise nature of the threats that the organization faces in order to trust the management response



Sustainment: Risk Assessment and Operational Evaluation of Change

Section 1

- The activities that are involved in operational assessment are planned and implemented in the same way as other types of organizational assessment activities.
- Planning for operational risk assessments involves the establishment of a standard schedule for each assessment as well as a defined process for problem reporting and corrective action.
- Operational risk assessment does not typically entail the sort of strategic planning focus that was involved in the formulation of the security strategy.





Section 1

Evaluation of the Risk Management Function

Martin Yanev

Evaluating the Overall Risk Management Function

- The real proof of a risk management program's success lies in the operational outcomes of the controls that have been deployed for risk management. The test is whether the controls have achieved the desired business outcomes when it comes to risk mitigation.
- Control performance audits and assessments can be used to verify that the operational controls are functioning as designed and intended



Evaluating the Overall Risk Management Function

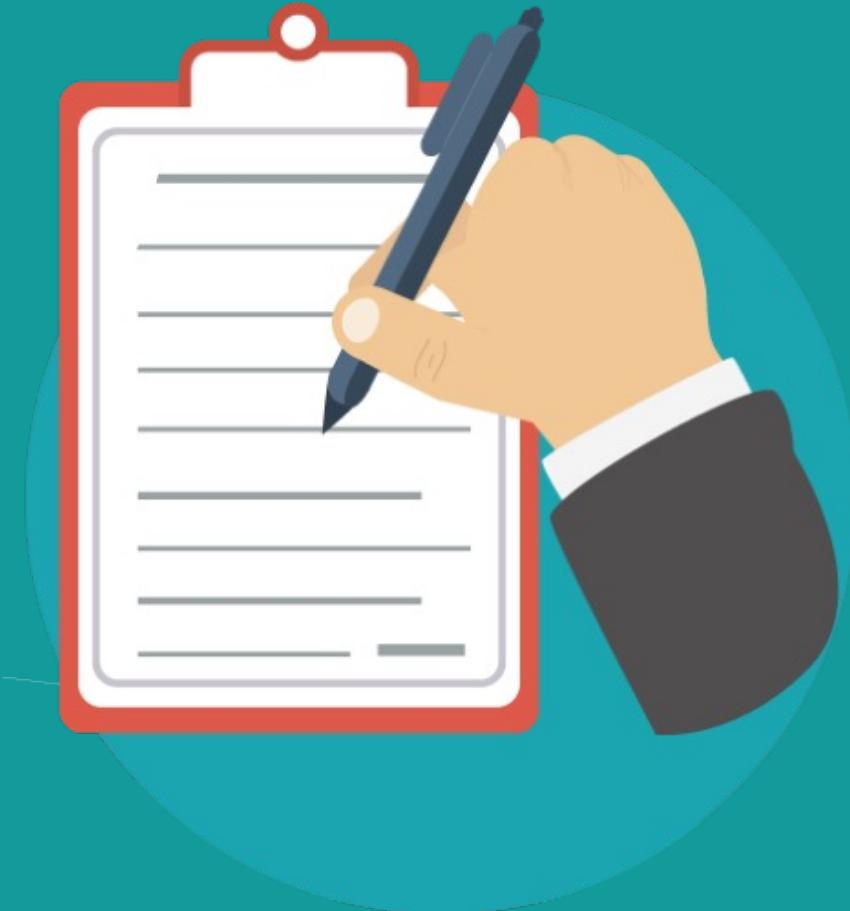
Two types of audits are commonly used, a ***time-based*** audit and an ***event-based*** audit. It is generally a good idea to utilize both types of audits in practice, in order to ensure complete assurance.

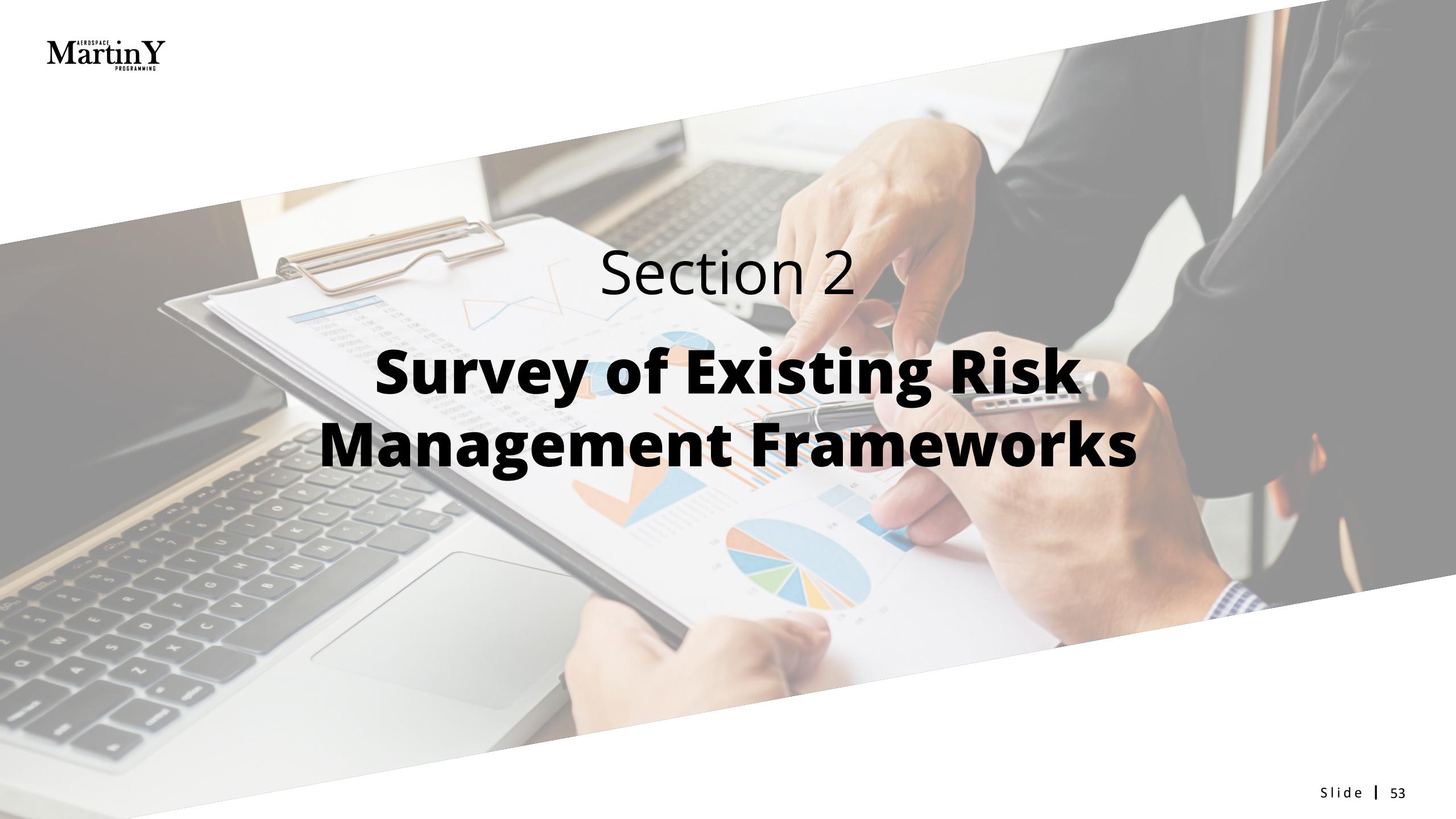
- A time-based audit is one that occurs at regular intervals, ranging typically from 1 to 3 years.
- An event-based audit is much less comprehensive, but much more focused on a particular aspect of the risk management process.



Section Summary

this Section presented an overview of the role of the standardization process in ensuring a consistent response to a given issue of importance. This includes a discussion of why information assets are difficult to protect as well as applying commonly acknowledged best practices to ensure an informed response.





Section 2

Survey of Existing Risk Management Frameworks

Survey of Existing Risk Management Models and Frameworks

- This Section provides a comparative assessment of existing models and frameworks for cybersecurity. The aim is to relate the practice of risk management within the larger collection of standard processes that have been developed to implement organizational cybersecurity.
- Risk control is an important aspect of ensuring organization-wide security. However, the risk management process is only one element of the potential set of standardized processes that might be utilized in a secure organization, as shown in Figure

Bell-LaPadula Model
Biba Integrity Model

COSO
Enterprise Risk Management—Integrated Framework

NICE Cybersecurity Workforce Framework 2.0

NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF)
HITRUST Common Security Framework (CSF)

ISO/IEC 27000
ISO 31000:2009
IEC 31010:2009

NIST Risk Management Framework (NIST RMF)
NIST SP 800-53 Revision 4, *Security and Privacy Controls*
NIST SP 800-30, *Guide for Conducting Risk Assessments*
NIST SP 800-37, *Guide for Applying the Risk Management Framework*

Standard Best Practice

- The aim of standard best practice is to provide expert advice and a consensus in a professional area such as cybersecurity protection. As such, the RMF serves to establish the single point of reference, which can be used to evaluate whether an organization's information protection is both adequate and capable.
- However, the RMF standard itself essentially integrates a collection of best practice recommendations for how to conduct the process, rather than a handCourse for the establishment of risk management controls.





Section 2

Making Risk Management Tangible

Making Risk Management Tangible

→ The goal of risk management is to add value to the business by protecting its critical assets. Capable risk management links technology processes, resources, and information to the overall purposes of the enterprise

→ **Effectiveness:**

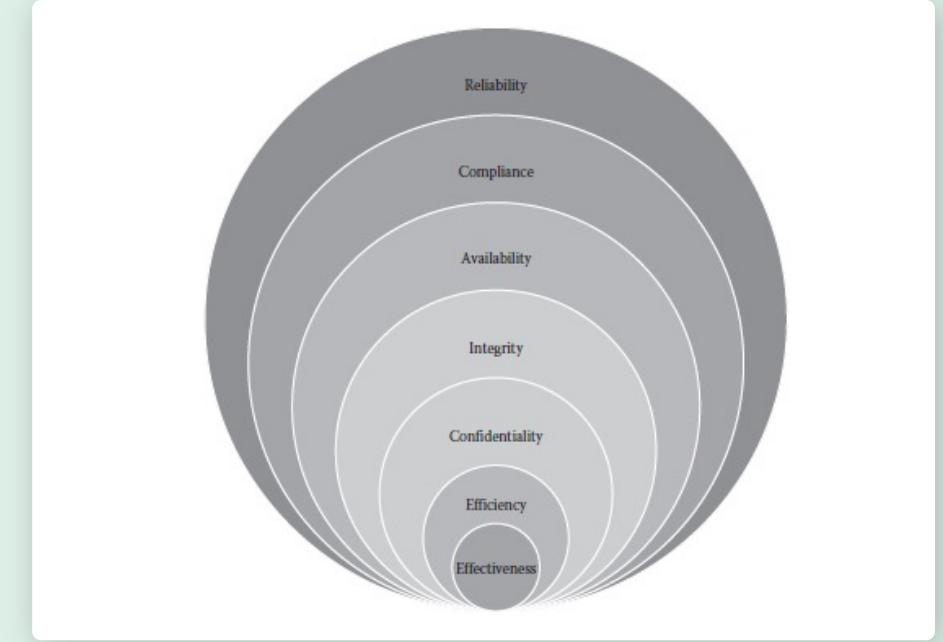
- The operation of the risk management process should be effectively integrated with and relevant to the business process that it supports.

→ **Efficiency:**

- the risk management process should underwrite the mitigation of known threats in the most optimal (productive and economical) way possible.

→ **Confidentiality:**

- risks to sensitive information must be identified and mitigated in a manner that will ensure effective protection from unauthorized disclosure.



Making Risk Management Tangible (Cont.)

→ Integrity:

- The risks that may impact the accuracy and completeness of information must be mitigated in accordance with the values and expectations of the business purpose.

→ Availability:

- Risks that would make information required by the business unavailable must be identified and addressed. This requirement applies to all present and future situations. It also applies to the safeguarding of the necessary resources and associated capabilities to carry this out.

→ Compliance:

- All risk management controls must comply with the laws, regulations, and contractual arrangements to which the business process is subject, that is, externally imposed business criteria.

→ Reliability:

- The risk management process must be provably robust and persistent and the continuity of the threat assessment and analysis function must be assured.



Section 2

Formal Architectures

Martin Yanev

Formal Architectures

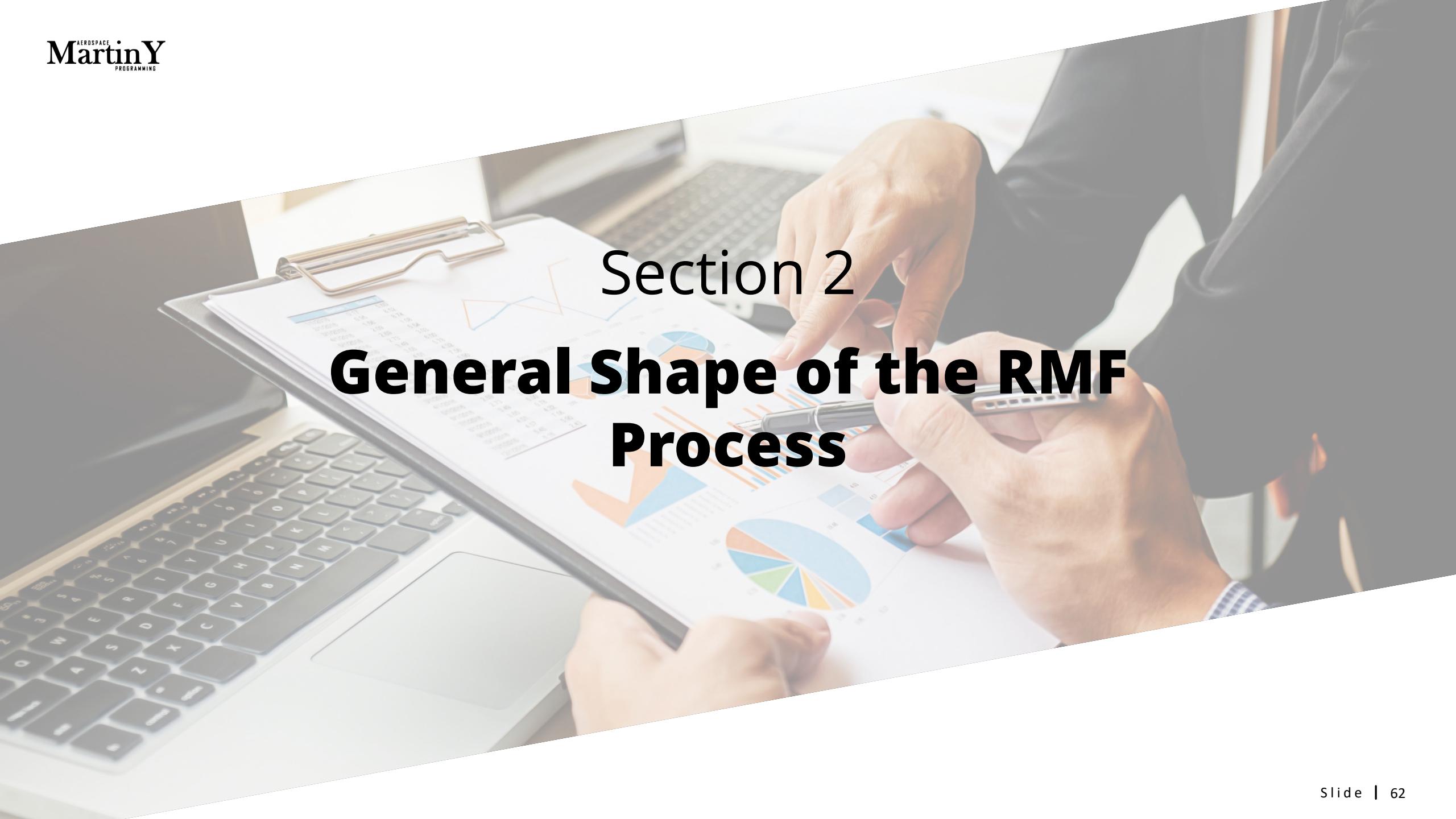
- The seven characteristics are leveraged by the design, development, maintenance, and operation of a formal, organization-wide risk management capability.
- The purpose of this capability is to ensure that managers know the exact status of all of the identified risks to the organization's critical data, applications, technology, IT facilities, and human resource assets



Formal Architectures

- Since they are central to the concepts in this text, we need to stop here to define security controls.
- Each control must generate sufficient evidence of its performance to be able to confirm its current operation.
- The RMF specifies a standard umbrella process to be followed in order to develop and document a security control system.



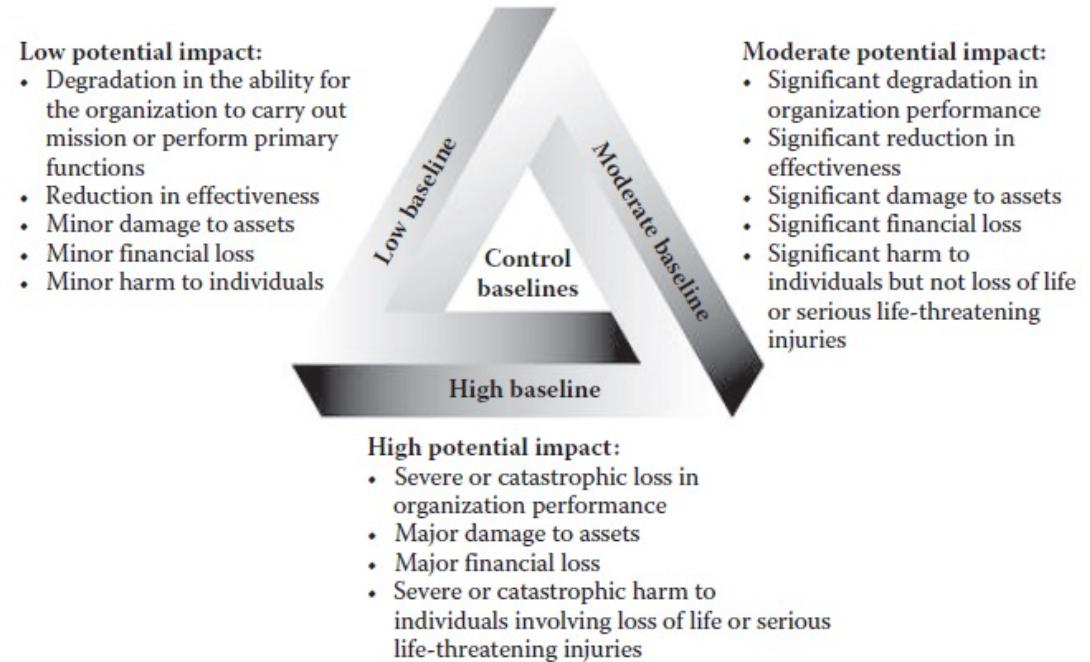


Section 2

General Shape of the RMF Process

General Shape of the RMF Process

- The RMF guideline is structured on one simple and pragmatic assumption: information assets should be secured and managed using a well-defined process to guide the classification, deployment, testing, and sustainment of the risk management program. Accordingly, the generic RMF process requires the organization to characterize the threat environment.
- It must then formalize a control set from a standard model, implement each control, and document their effectiveness, and monitor the controls moving forward.



General Shape of the RMF Process

- Management can use this evaluation or audit assessment to map where the organization is in relation to the best practice ideal established by the framework.
- This first step of the process forces the organization to outline and examine all of the risks and organizational requirements associated with protecting its ICT operation from meaningful threats.
- Measures that can be defined from these factors will tell management whether the risk management process has achieved its performance goals.



Section 2

RMF Implementation

RMF Implementation

- The RMF process is meant to be generic or in simple terms; it is applicable to almost any conceivable threat situation worldwide.
- For the purposes of implementation, the RMF process demands that the organization should develop and document a clear policy statement of the architectural reference models that will guide the actual implementation process, the solution architectures that will result and the mission, and the business processes that will be affected.
- The organization then identifies and prioritizes the threats that it faces and the vulnerabilities that those represent, using a comprehensive assessment of the organization's threat environment as the point of reference.



RMF Implementation

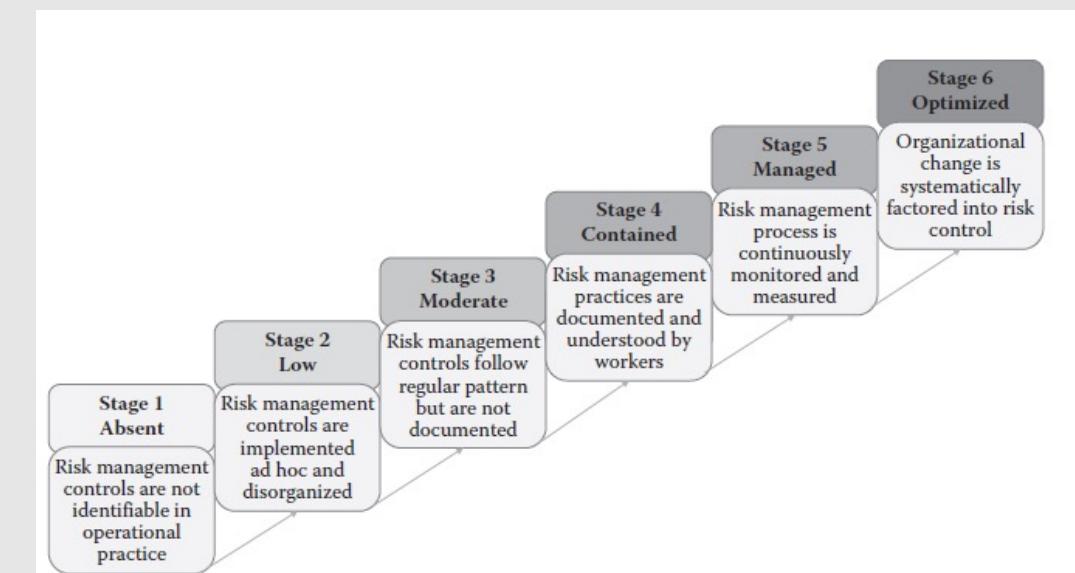
- The boundary setting element is particularly important since there is an obvious direct relationship between the resources required to establish the security level specified and the extent of the territory that must be secured.
- Following the actual implementation of the selected controls, the organization performs a detailed assessment of their performance.
- the RMF model is intended to guide the execution and sustainment of standard risk management practice.
- In conventional practice, the effectiveness of a formal control process has traditionally been expressed in terms of a maturity rating scale.



RMF Implementation

Our maturity scale might be describable in terms of the following stages

- **Absent:** risk management controls are not identifiable in operational practice
- **Low:** risk management controls are implemented ad hoc and disorganized
- **Moderate:** risk management controls follow regular pattern but are not documented
- **Contained:** risk management practices are documented and understood by workers
- **Managed:** risk management process is continuously monitored and measured
- **Optimized:** organizational change is systematically factored into risk control





Section 2

International Organization Standards

Other Frameworks and Models for Risk Management

- The NIST RMF represents a measured response to the well-understood desire to organize and systematize risk management practice into a single coherent reference model that embraces all aspects of ensuring assets against known threats
- The process steps that are specified in the RMF architecture span the gamut of standard threat identification and mitigation activities.
- **ISO 31000:2009**, Risk management—Principles and guidelines, and IEC 31010:2009, Risk management—Risk assessment techniques
- **COSO** Enterprise Risk Integrated Framework
- **HITRUST CSF**



International Organization for Standardization 31000:2009

→ ISO 31000:2009 Risk management—Principles and guidelines is a membership supported standard and provides a working set of principles, an architecture, and an implementation process for managing risk. It can be used by any member organization regardless of its size, activity, or industry sector and it applies to any type of risk.

→ **The current family includes the following:**

- ISO 31000:2009, Risk management—Principles and guidelines
- ISO/TR 31004:2013, Risk management—Guidance for the implementation of ISO 31000
- IEC 31010:2009, Risk management—Risk assessment techniques
- ISO Guide 73:2009, Risk management—Vocabulary



ISO 31000:2009

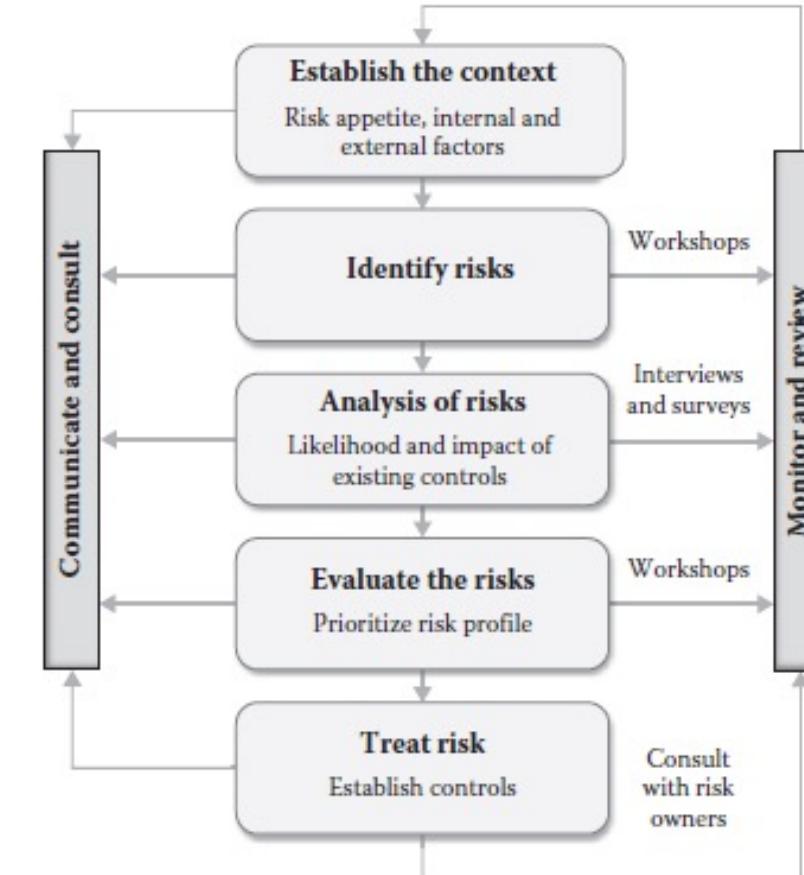
Thus, ISO 31000:2009 is intended for a broad stakeholder group including:

- Executive level stakeholders
- Enterprise risk management groups
- Risk analysts and management officers
- Line managers and project managers
- Compliance and internal auditors
- Independent practitioners

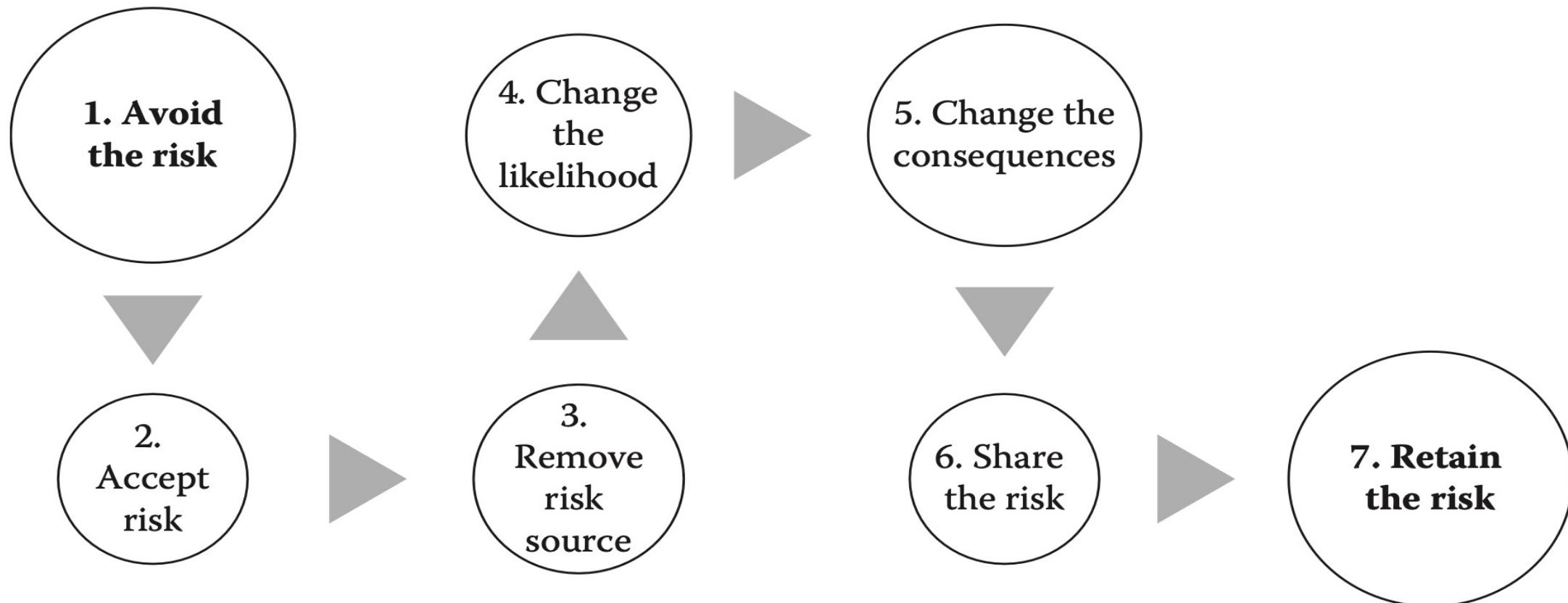


ISO 31000:2009

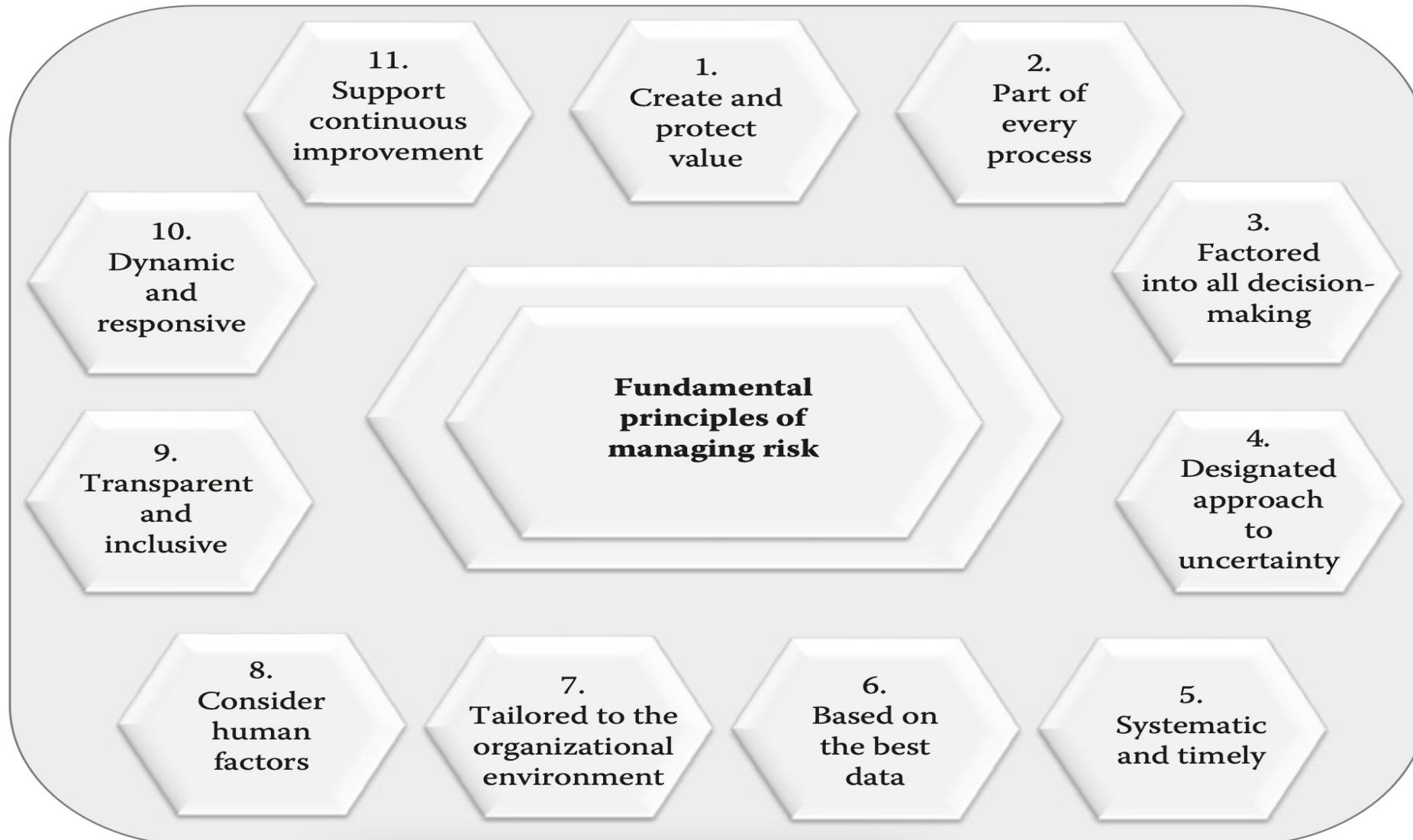
- The implementation strategy for the standard reflects that intention. In ISO 31000, attention is paid to the integration of existing risk management processes



Managing The Risk



ISO Foundational Principles of Risk





Section 2

OSI 31000 Implementation Process

ISO 31000 Implementation Process: Establishment

- ISO 31000 style risk management is implemented in two stages. In the first stage, Establishment, the organization embeds formal risk management into its operational management system.
- This involves establishing an effective RMF and then using that framework to support the operation of the risk management process.
- Finally, the organization has to pay close attention to its human factor issues, in that risk management benefits have to be communicated to the members of the organization in such a way that support for the operational RMF is ensured.



ISO 31000 Implementation Process: Establishment

- In the second stage, the operational elements of the RMF have to be established.
- A set of general risk management policies and practices can then be defined for every phase of the risk management process organization wide.
- Typically, the first step in the execution of the plan is to identify priority risks. This first involves defining the organization's risk criteria.





Section 2

COSO Enterprise Risk Management Framework

COSO Enterprise Risk Management Framework

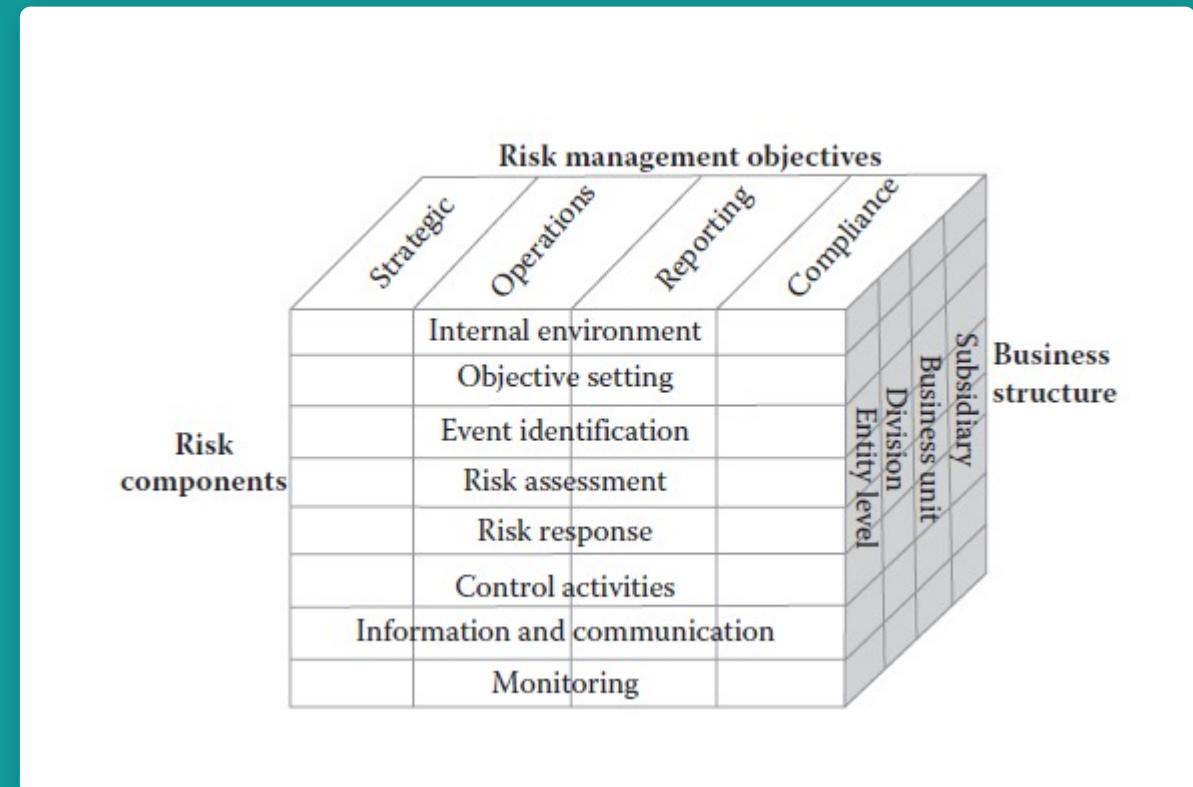
- The COSO Enterprise Risk Management Framework describes a continuous process that an entity undertakes as a normal part of doing business.
- Risk management is applied through strategy and goal setting, but it is not simply a strategic process that is developed at the C-suite level. It involves people across the enterprise and at every level of an organization. In this framework, risk management is best understood and applied by means of a portfolio approach to characterizing the organizational threat environment.



COSO Enterprise Risk Management Framework

The COSO Enterprise Risk Management Framework consists of eight interrelated activities.

1. Internal environment
2. Objective setting
3. Event identification
4. Risk assessment
5. Risk response
6. Control activities
7. Information and communication
8. Monitoring



COSO Enterprise Risk Management Framework

The role of management is to establish strategic goals, align appropriate strategies, and implement an associated set of actions.

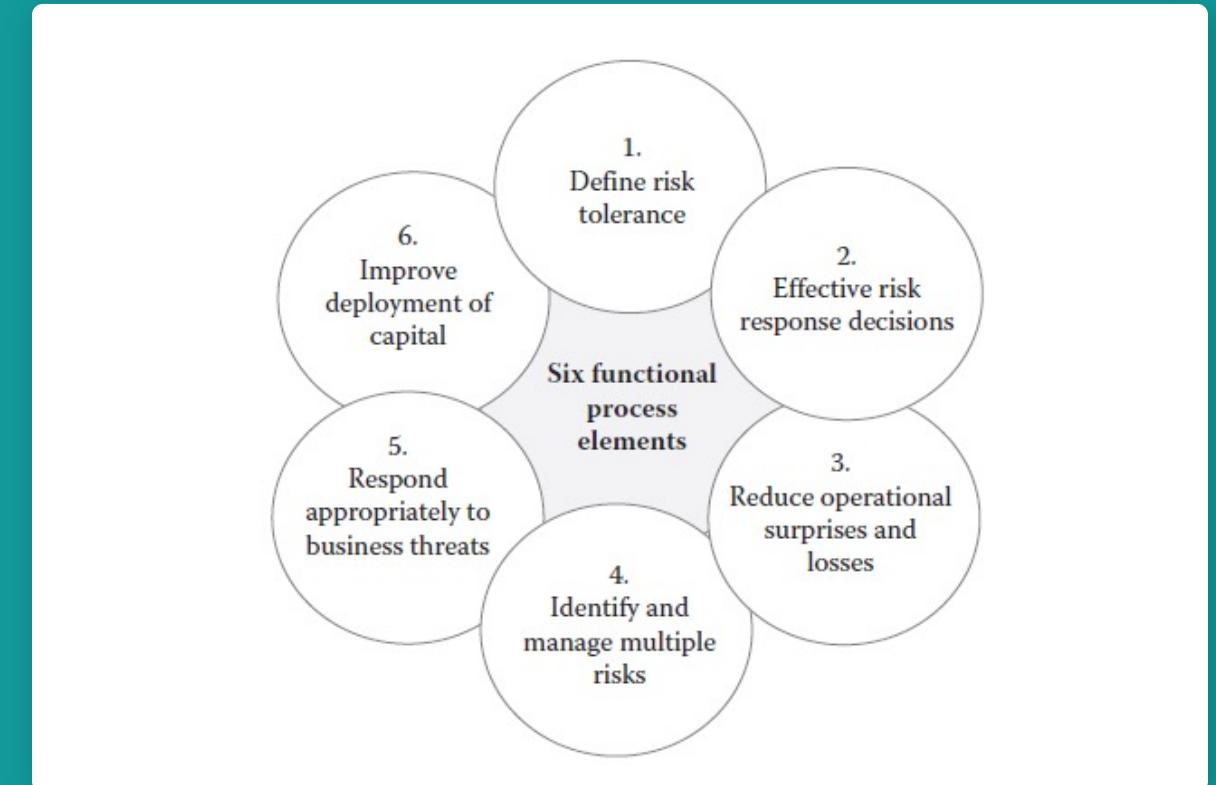
- 1. *Strategic planning and management*: the framework supports the achievement of the organization's strategies and decision-making purposes in support of its goals.
- 2. *Operations*: decisions made within the framework help to ensure the effective and efficient use of organizational resources.
- 3. *Reporting*: the framework creates the formal channels for reliable assessment and reporting.
- 4. *Compliance*: the framework ensures compliance with all applicable laws and regulations.

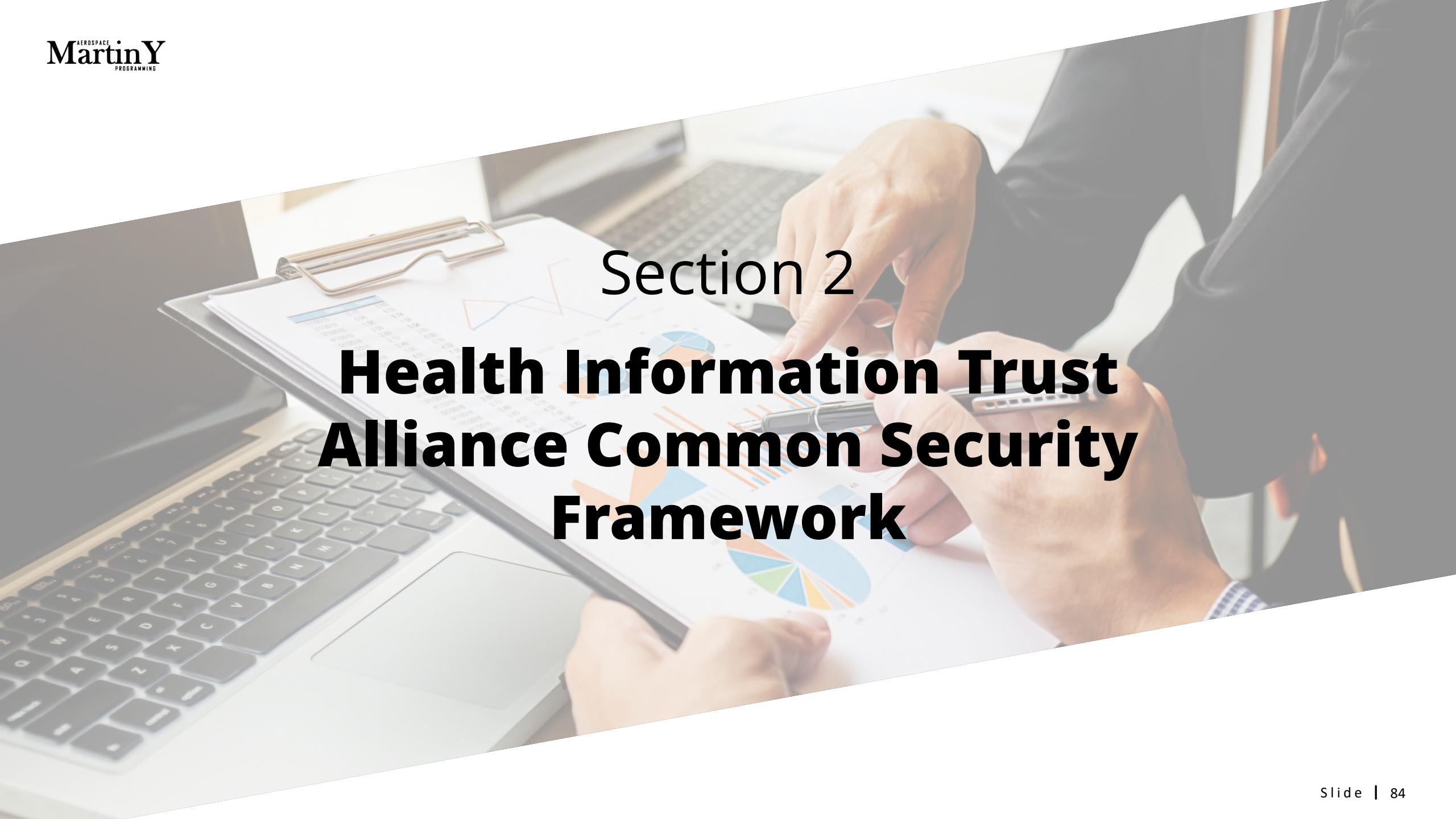


COSO: Six functional elements

The COSO enterprise risk management process requires six functional elements

1. Definition of the precise level of risk tolerance
2. Enhancement of the effectiveness of risk response decisions
3. Reduction of operational surprises and losses
4. Identification and management of multiple risks that are potentially cross-enterprise
5. Assurance of an appropriate response to opportunities as they present themselves
6. Improvement in deployment of capital



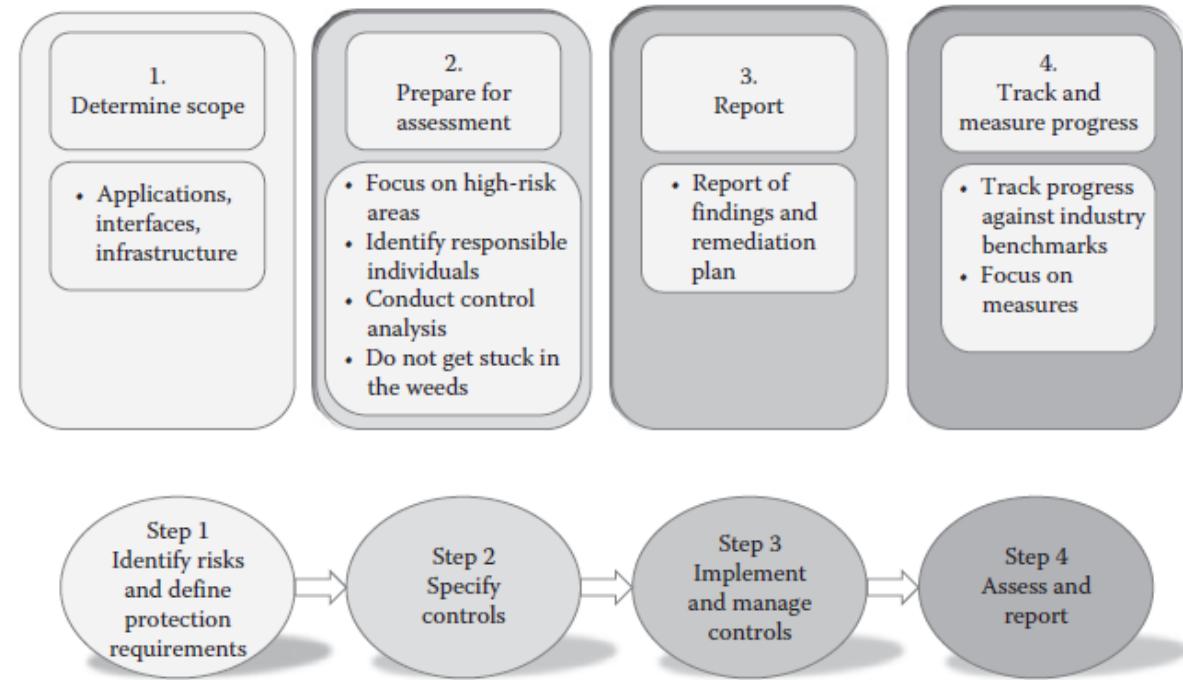


Section 2

Health Information Trust Alliance Common Security Framework

Health Information Trust Alliance Common Security Framework

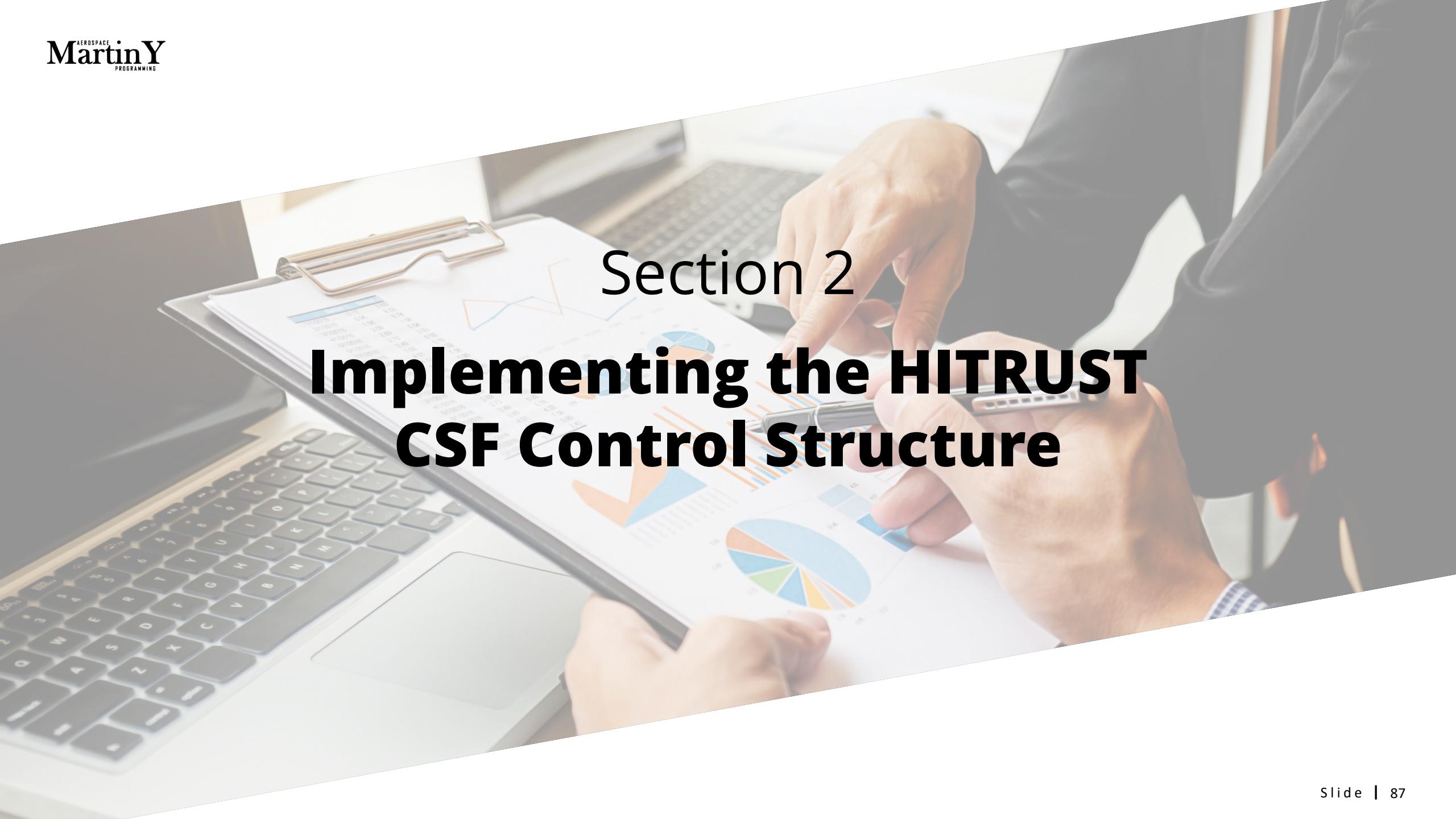
- The HITRUST CSF is the product of a for-profit U.S.-based corporation called the Health Information Trust Alliance. The HITRUST CSF was developed by a consortium of leaders and experts in health care, information technology, and information security to specifically address ICT risk issues in the health-care industry.
- HITRUST CSF has come to represent an ideal example of a sector-specific risk model.



Health Information Trust Alliance Common Security Framework

- The HITRUST CSF is a standard architectural model that seeks to normalize security control implementations in health-care organizations.
- The development and maintenance of the CSF architecture is overseen by the HITRUST executive council. This executive council comprises representatives from a number of industry sectors.
 - The ICT product and service vendor community
 - Technology and IT infrastructure organizations
 - Professional ICT service firms
 - Health information networks and clearinghouses



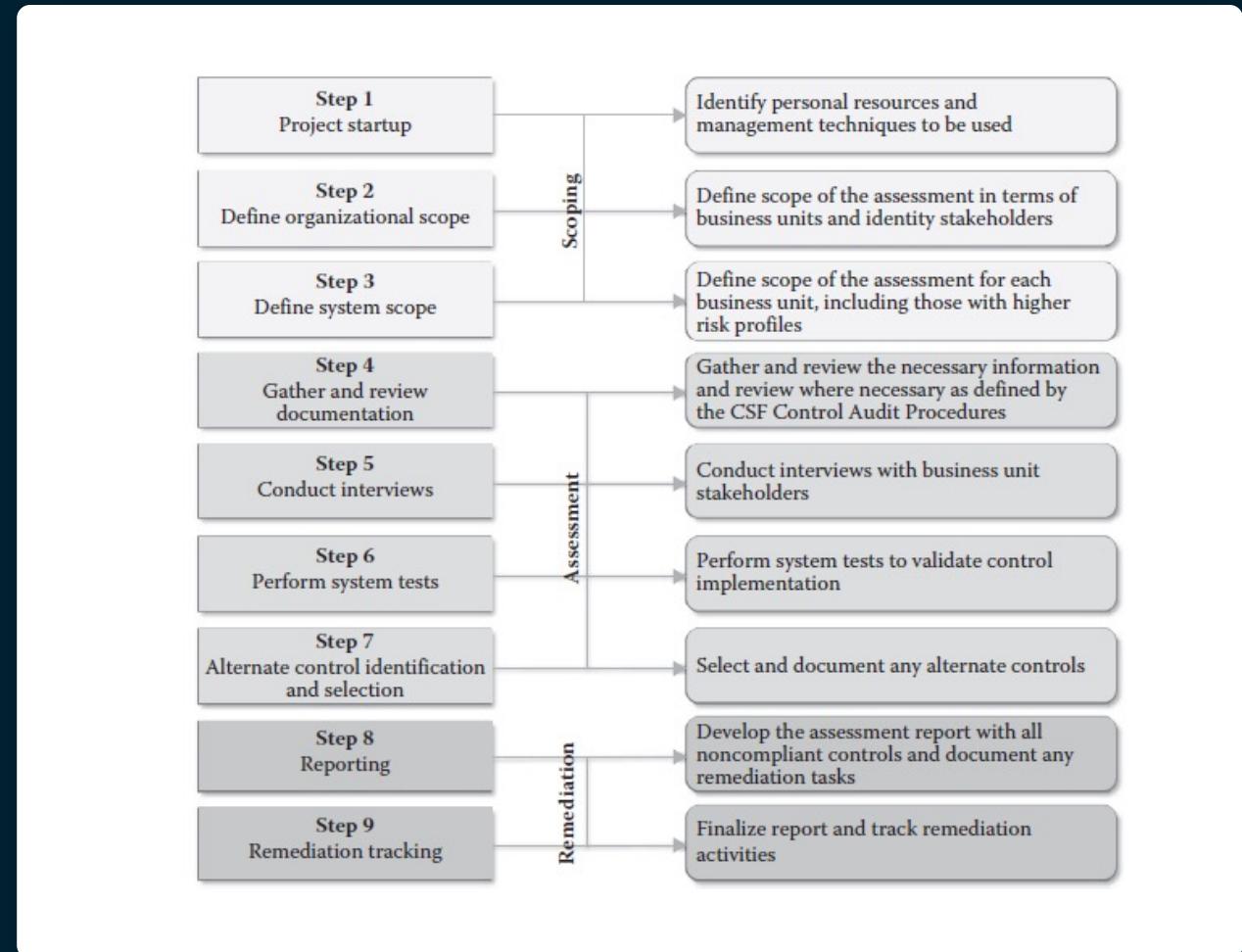


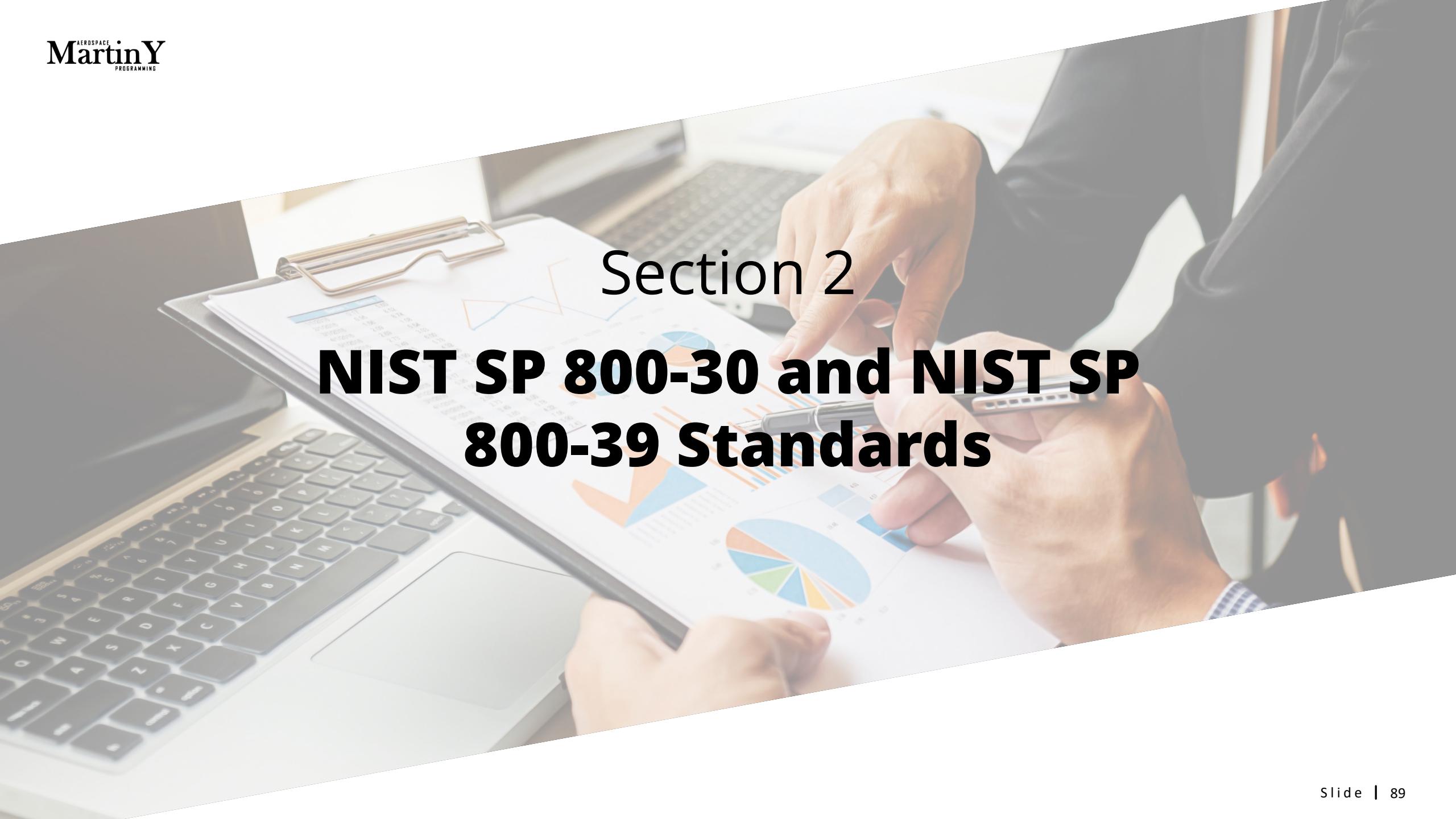
Section 2

Implementing the HITRUST CSF Control Structure

Implementing the HITRUST CSF Control Structure

- The control specifications of the CSF are similar to those of the three-level baseline concept adopted by NIST's computer security division for its SP 800 series security standards.
- The HITRUST CSF also offers an alternative service that provides compliance assessment and reporting for HIPAA.
- Under the CSF Assurance Program, organizations can proactively or reactively undertake an assessment that is performed against the requirements of the CSF.



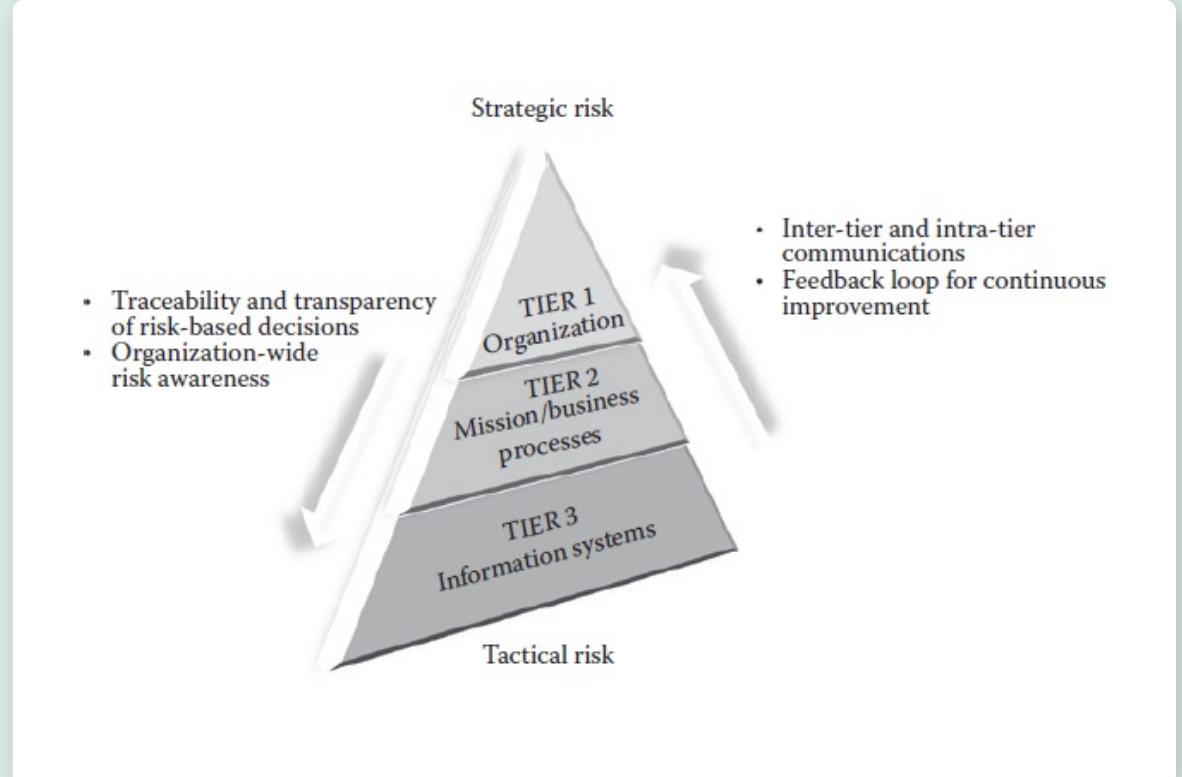


Section 2

NIST SP 800-30 and NIST SP 800-39 Standards

NIST SP 800-30 and NIST SP 800-39 Standards

- The NIST RMF provides a framework for the process of risk management; however, there is still the question of application. In that respect, NIST has updated SP 800-30 Revision 1, Guide for Conducting Risk Assessments, in order to provide guidance about the way to conduct standard risk assessments.
- According to NIST, risk assessment is a key component of a holistic, organization-wide risk management process (NIST, 2006). That process is defined in NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View.



NIST SP 800-30 and NIST SP 800-39 Standards

Risk management processes cited in that publication include methods to:

- **Frame risk:** identify and explicitly characterize the risk event
- **Assess risk:** determine the likelihood and impact of occurrence
- **Respond to risk:** develop effective risk mitigation approaches
- **Monitor risk:** ensure the ongoing effectiveness of a given solution



NIST SP 800-30 and NIST SP 800-39 Standards

- Assessment drives the decision-making in each of the phases of the RMF.
- The risk assessments in the Categorization phase integrate and evaluate all of the existing information about threat sources, threat events, vulnerabilities, and predisposing conditions.



NIST SP 800-30 and NIST SP 800-39 Standards

After the initial security control baseline is first put in place, risk assessment results are utilized to help the organization most effectively:

- Apply appropriate tailoring guidance to adjust the controls based on specific mission/business requirements, assumptions, constraints, priorities, tradeoffs, or other organization-defined conditions.
- Adjust the control baseline based on specific and credible threat information.



NIST SP 800-30 and NIST SP 800-39 Standards

- In addition to the risks associated with implementation, the ongoing strength of each of the selected security controls has to be evaluated.
- Organizations can use the results from security control assessments to inform the risk assessments that are conducted in RMF phase four.
- The organization then uses the risk assessment results to underwrite the authorization of the specific control system.



NIST SP 800-30 and NIST SP 800-39 Standards

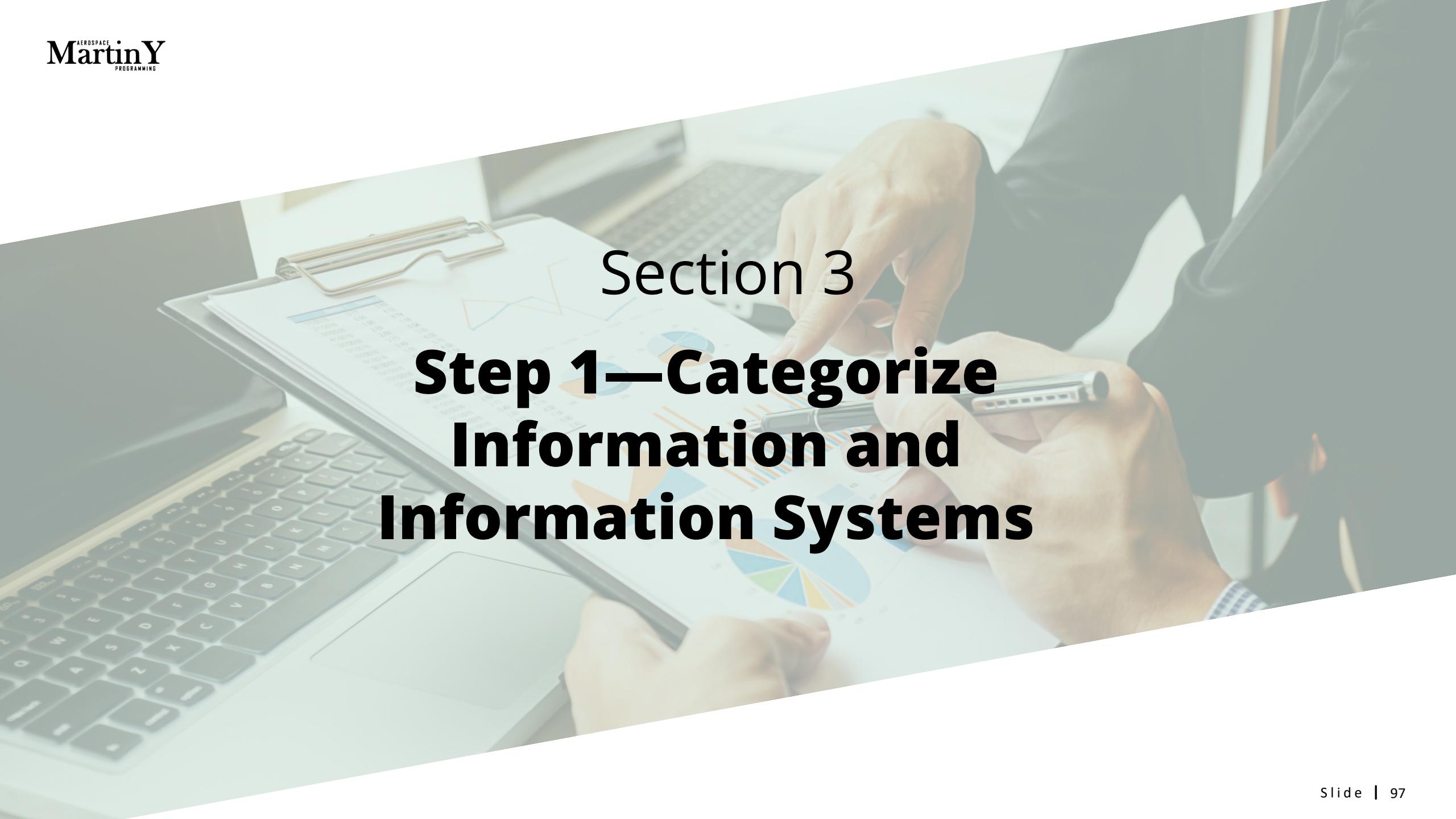
- Once the control system is authorized, its ongoing performance must be monitored.
- These monitoring processes evaluate the continuance of the following (NIST, 2006):
 - Effectiveness of security controls
 - Changes to systems and operational environments that might impact security
 - Compliance with laws, regulations, directives, policies, standards, and guidance



Section Summary

- The aim of standard best practice is to provide expert advice and a consensus in some professional area, for instance, cybersecurity protection. In this respect, the RMF serves to establish the single point of reference, which can be used to evaluate whether an organization's information protection is both adequate and capable. The goal of risk management is to add value to the business by protecting its critical assets.





Section 3

Step 1—Categorize Information and Information Systems

Introduction

- Security Categorization and Control Selection for National Security Systems (CNSS, 2014) will be explored, compared, and contrasted as a source of guidelines for organizations to perform the categorization of information systems process.
- The major focus of this Section centers on the tables available in NISTSP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories and FIPS PUB 199 as a means of implementing the security categorization and information classification process of the NIST RMF

FIPS 199
Standards for Security Categorization of Federal Information and Information Systems

NIST SP 800-60
Guide for Mapping Types of Information and Information Systems to Security Categories

Committee on National Security Systems
CNSSI No. 1253
Security Categorization and Control Selection for National Security Systems

NIST Risk Management Framework (NIST-RMF)
NIST SP 800-53 Revision 4, *Security and Privacy Controls*
NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
NIST SP 800-37 R1, *Guide for Applying the Risk Management Framework*

Section 3

Security Impact Analysis

Security Impact Analysis

- Before gaining an understanding of SIA, it is necessary to make two important points. The first deals with the cyclical nature of risk. As you learn about how to implement each of the steps of the NIST RMF, it is easy to view the process from the perspective that no process for risk management currently exists within the organization.
- **SIA serves a benefit in assisting ICT planners, designers, and developer to:**
- Identify potential risk areas (real and possible) of a proposed change
- Develop effective safeguards (design requirements) to address identified potential risks
- Develop effective security and privacy testing to integrate into overall testing, prior to promotion of changes into a production environment



Significant change to an ICT system

- SIA serves a benefit in assisting ICT planners, designers, and developer to:
- Identify potential risk areas (real and possible) of a proposed change
- Develop effective safeguards (design requirements) to address identified potential risks
- Develop effective security and privacy testing to integrate into overall testing.



Significant change to an ICT system

- An operating system or middleware component that results in application modifications to system ports, protocols, or services
- New or existing hardware platforms
- Cryptographic modules or services
- New or existing security controls



Significant change to an ICT system

Worthy of mention, the SIA process must not:

- Waive or bypass minimum regulatory or industry standard security or privacy control requirements, or other organizational policies or procedures
- Negate the direction of the CCB minimum requirements or policies, or bypass required CM phases or steps.
- Excuse systems of identified (or unidentified) security or privacy deficiencies.
- Act as a means for risk acceptance for identified (or unidentified) security or privacy deficiencies



Significant change to an ICT system

From an operational perspective, significant changes to the environment may include the following:

- Moving all or part of the system to a new facility
- The addition of new organizational missions or business functions
- An awareness, through credible threat information, that the organization is
- being targeted
- Conformance to new or modified laws, directives, policies, or regulations





Section 3

FIPS 199, Standards for Security Categorization of Federal Information and Information Systems

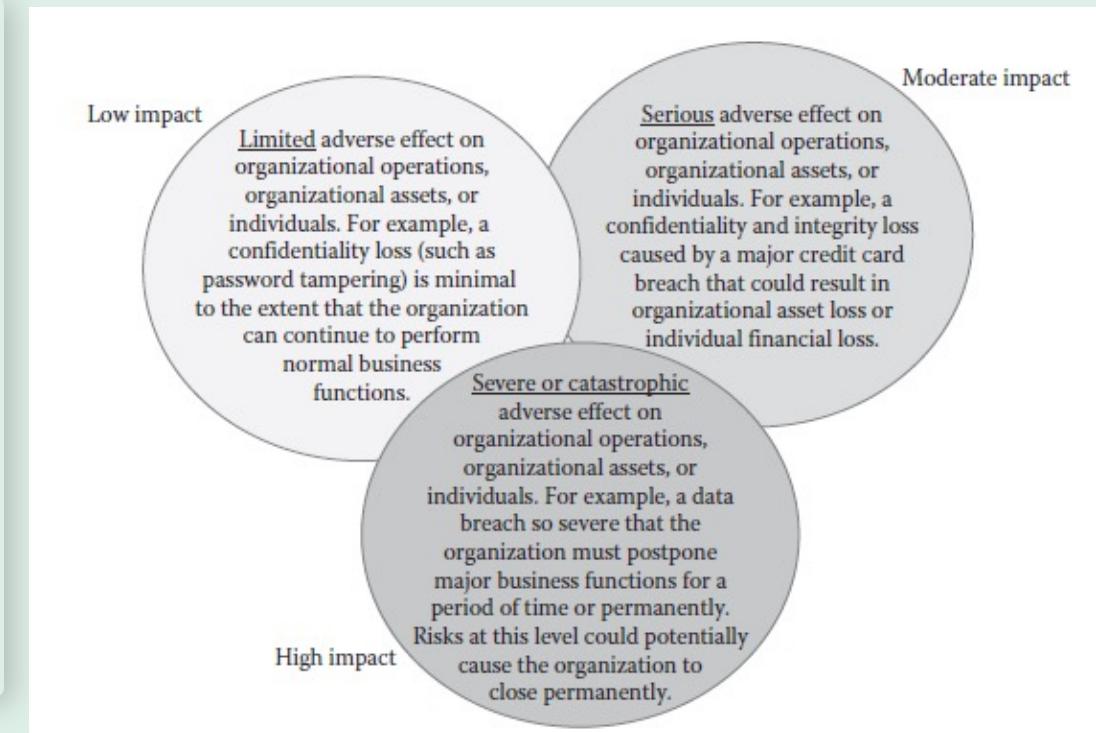
Martin Yanev

FIPS 199, Standards for Security Categorization of Federal Information and Information Systems

- Such a framework promotes the following:
- An effective means for management and oversight of the programs that support information security
- An effective and consistent reporting mechanism providing details related to adequacy and effectiveness of information security policies, procedures, and practices to upper management, or in the case of federal systems, to the Office of Management and Budget (OMB) and Congress



→ FIPS 199 provides criteria for the security categorization of information **types** and information **systems**





Section 3

FIPS 199, Standards for Security Categorization of Information Types

Martin Yanev

FIPS 199—Security Categorization of Information Types

- In performing an analysis of an information type, the SC must take into consideration the data transit, data processing, or data storage. For each information type being analyzed, the potential impact values assigned to the three security objectives (confidentiality, integrity, and availability) are determined by using the values low, moderate, or high.

$$SC_{\text{information type}} = \left\{ \begin{array}{l} (\text{confidentiality, impact}), (\text{integrity, impact}), \\ (\text{availability, impact}) \end{array} \right\}$$

$$SC_{\text{customer information}} = \left\{ \begin{array}{l} (\text{confidentiality, HIGH}), (\text{integrity, MODERATE}), \\ (\text{availability, MODERATE}) \end{array} \right\}$$

$$SC_{\text{student information}} = \left\{ \begin{array}{l} (\text{confidentiality, HIGH}), (\text{integrity, HIGH}), \\ (\text{availability, MODERATE}) \end{array} \right\},$$

$$SC_{\text{administrative information}} = \left\{ \begin{array}{l} (\text{confidentiality, MODERATE}), \\ (\text{integrity, MODERATE}), \\ (\text{availability, LOW}) \end{array} \right\},$$

$$SC_{\text{registration system}} = \left\{ \begin{array}{l} (\text{confidentiality, HIGH}), (\text{integrity, HIGH}), \\ (\text{availability, MODERATE}) \end{array} \right\}$$



Section 3

CNSSI No. 1253, Security Categorization and Control Selection for National Security Systems

Martin Yanev

CNSSI No. 1253, Security Categorization and Control Selection for National Security Systems

- CNSS, a member of the Joint Task Force (JTF), sets cybersecurity policies, directives, instructions, operational procedures, guidance, and advisories for U.S. Government National Security Systems (NSS).
- it is important to note that CNSSI 1253 is not intended to be an alternative for what was just discussed of FIPS 199.



CNSSI No. 1253, Security Categorization and Control Selection for National Security Systems

To that extent, the major differences between this instruction and the NIST publications as they relate to categorization are as follows:

- The CNSSI 1253 standard does not adopt the high water mark concept (highest category of low, moderate, and high impact if multiple types are categorized) from FIPS 199
- The definitions for moderate and high impacts in this standard are refined from those provided in FIPS 199.
- The associations of confidentiality, integrity, and/or availability to security controls are explicitly defined in the standard.





Section 3

Implementation of Step 1: Security Categorization

Martin Yanev

Implementation of Step 1—Security Categorization

- Resulting from this step, each system's impact level is further used to select a set of baseline security controls for the information system from NIST SP 800-53
- Organizational management has the responsibility of ensuring that security categorizations are reviewed on an ongoing basis



NIST SP 800-60 defines a four-step process

On the basis of the premise that organizations enforce repetition, NIST SP 800-60 defines a four-step process for categorizing information and information systems. Those steps include:

1. Identify information types:
2. Select the security impact levels
3. Review provisional impact levels
4. Assign a system security category and overall impact level





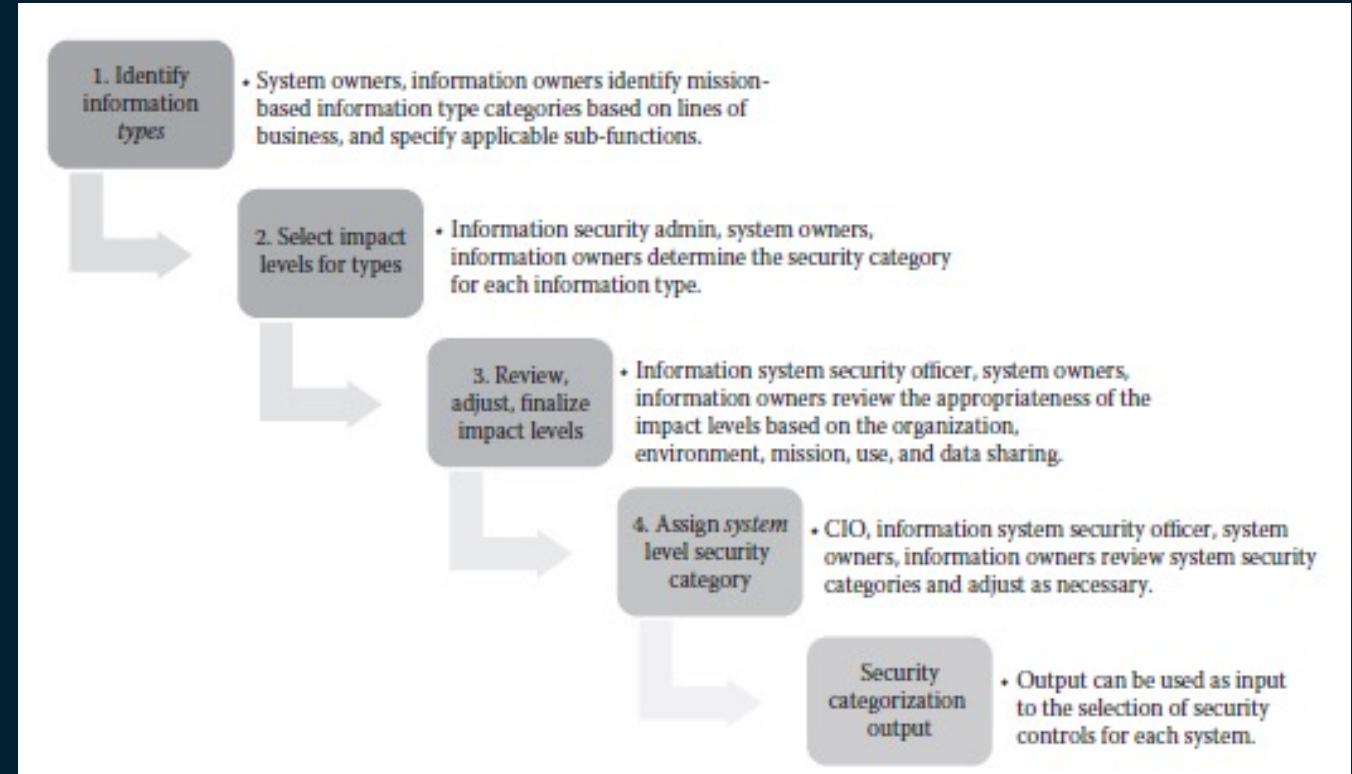
Section 3

Security Categorization from the Organizational Perspective

Martin Yanev

Security Categorization from the Organizational Perspective

→ As a means to adequately address its security needs, an organization must have a comprehensive approach for addressing risk throughout each of its business functions. Such an approach provides the benefit of greater visibility into the integrated network of operations that exist internally and externally through the organization supply chain, in addition to an understanding of all of the information flows through each of those operations.



Section 3

Security Categorization from the Organizational Perspective

- Providing clear definition of the types of external services provided
- Obtaining detailed descriptions of how the external services are protected and conform to the security requirements of the organization
- Achieving adequate assurances that the risk to the organization's operations, assets, and individuals resulting from the use of the external services is at an acceptable level





Section 3

Establish Relationships with Organizational Entities

Martin Yanev

Establish Relationships with Organizational Entities

- The underlying success in implementing the NIST RMF is largely dependent on a collaborative effort among all internal and external organizational entities that are directly impacted by the way in which information security practices are performed.
- It should be noted that the categorization process can only be successful if the appropriate level of collaboration exists between all affected individuals within the organization and its external service providers.



Develop an Organization-Wide Categorization Program

- Integrate the categorization process into the processes already established defining the system development life cycle
- Handle the emergence of new information types
- Conduct the categorization process for their individual information systems in accordance with organizational policies and procedures
- Document the decisions made during the categorization process into the organizations master system security plan
- Gain approval for decisions made during the categorization process
- Follow appropriate reporting procedures regarding categorization decisions
- Maintain the decisions made during the categorization process by implementing a review task for the purpose of continuously validating

Develop an Organization-Wide Categorization Program

- As changes are made to the information systems, considerations related to security categorization generally take place during the project initiation.
- As is the case with many international and domestic ICT standards and guidelines, every organization implements the NIST SP 800-60 categorization process based on the culture within their organization.





Section 3

Prepare an Organization-Wide Guidance Program

Martin Yanev

Prepare an Organization-Wide Guidance Program

- The organization's missions and lines of business are reviewed to identify information types that may not be included in NIST SP 800-60, Volume 2: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories.



Volume 2: Appendices

- Information type title and brief description of the new organization-specific information type
- Recommended security category
- For each security objective (confidentiality, integrity, and availability):
 - Discussion of the recommended security impact value assigned
 - Special factors affecting the impact value determination (NIST, 2009b)



Lead Organization-Wide Categorization Sessions

- It is vital that organizations take on the security categorization as an organization wide effort.
- In the less desirable circumstance that an organization chooses to implement the categorization process without conducting organization-wide categorization sessions, it still necessary for the identified impact levels for information systems to be consistent throughout the organization





Section 3

Security Categorization from Management Prospective

Martin Yanev

Security Categorization from the Management Perspective

- To manage organizational risk, the most effective approach is to implement a risk executive function. The underlying scope of the risk executive function is to provide appropriate senior management input and oversight for all risk management and information security processes within the organization (including but not limited to each of the steps of the RMF).
- it is important that senior management's oversight be in place within the security categorization process. We have already discussed the dependent nature of the subsequent steps of the RMF to the success of the categorization process.



Security Categorization from the System Perspective

- the organization may consider deconstructing the information system into multiple subsystems to more effectively allocate security controls to the system in Step 2 of the RMF.
- One approach is to categorize each subsystem individually. Many organizations attempt to steer away from this approach claiming that separately categorizing each subsystem changes the overall categorization of the entire information system;





Section 3

Preparing for System Security Categorization

Martin Yanev

Preparing for System Security Categorization

At a minimum, the required system-specific documentation includes:

- System requirements specifications
- System design specifications
- Database design documents such as the data dictionary, database schemas, and data requirements documents
- Samples of system reports and input forms, or software code if accessible
- Maintenance plans



Step 1: Identify System Information Types

Once the system boundary has been identified, the goal is to obtain as much information as possible on the following:

- Overall scope of the system
- Portions of the organization's mission, or business functions that the system supports
- Transmission of data across the system boundary
- Functions and processes performed by the system
- Types of users and their usage characteristics
- Individuals, external organizations, or other subsystems that share information with the subsystem being categorized
- Characteristics of the operational environment
- Applications supported by the subsystem and the information that they process,
- store, create, transmit, or delete

Step 1: Identify System Information Types

- As each data element is identified, the database documentation assembled at the outset of the process is used to gain insight into how that data element is used.
- Once data elements have been identified and documented, the next task in identifying information types is to match the data elements in the system to the available information types.

At a minimum, the description must contain the following:

- A brief title and description of the information type
- A recommended security category
- A recommendation for the appropriate security impact value and the special factors affecting the impact value determination, for each security objective.



Information type, title, reference, description	Security category						Adjustment rationale	
	Provisional			Final				
	C	I	A	C	I	A		
Corrective action, C.2.1.1, POAMs include information on noncompliant information systems within the organization								
Program evaluation, C.2.1.2, Analysis information on the status of the organization's information systems (internal or external)								
Program monitoring, C.2.1.3, Collection of data gathered to evaluate the effectiveness of the organization's information system (internal or external)								
Inventory control, C.3.4.2, List of the organization's information systems including contact information of the system owner, individual responsible for security, system components, interconnections								
Provisional system security category								
Adjusted system security category								
Information system security impact level								



Section 3

System Security Categorization: Step 2, Step 3 and Step 4

Martin Yanev

Step 2: Select Provisional Impact Values for Each Information Type

- The provisional impact values are low, moderate, or high. Confidentiality can also have an impact value of "not applicable" when the information type contains public information.
- The recommendation is then followed by a justification for how the impact type is determined for each of the three security objectives (confidentiality, integrity, and availability).
- Once each of the provisional impact types have been selected, the security category section of the system security plan table(s) must be updated

$$SC_{\text{information type}} = \left\{ \begin{array}{l} (\text{confidentiality, impact}), (\text{integrity, impact}), \\ (\text{availability, impact}) \end{array} \right\}$$

Step 3: Adjust the Provisional Impact Levels of Information Types

→ In this step of the categorization process, the organization must perform a review and adjustment on the provisional security impact levels for the security objectives of each information type

1. Perform a review of the provisional impact levels based on the organization, environment, mission, use, and data sharing in order to justify their appropriateness
2. Make an adjustment, based on the review, to the security objective impact levels as necessary using the special factors guidance found in NIST SP 800- 60, Volume 2, Appendices C and D
3. Prepare and document all adjustments that were made to the impact levels, providing an appropriate rationale or justification for each adjustment



Step 4: Determine the Information System Security Impact Level

- In reviewing the existing impact levels, the provisional system security category is chosen by considering the highest value assigned to each security objective among the system's information types.
- The Compliance Tracking Summary table within the organization's system security plan must provide the capability of recording the assigned impact levels for each security objective.
- It is important to remember that in determining the adjusted security category, each information type is considered as a means for identifying the high water mark for a given system.

$$SC_{\text{information system}} = \left\{ \begin{array}{l} (\text{confidentiality, impact}), (\text{integrity, impact}), \\ (\text{availability, impact}) \end{array} \right\}$$

$$SC_{\text{information system}} = \left\{ \begin{array}{l} (\text{confidentiality, HIGH}), (\text{integrity, HIGH}), \\ (\text{availability, LOW}) \end{array} \right\}$$



Section 3

Obtain Approval for the System Security Category and Impact Level

Martin Yanev

Obtain Approval for the System Security Category and Impact Level

- Consistent with each of the other steps of the NIST RMF, the information system's security impact level and security category must be approved based on the specific directives in the organization's categorization guidance documentation, before continuing to Select Security Controls, Step 2 in the RMF.
- The approval procedure will vary from organization to organization based on the defined governance structure.



Maintain the System Security Category and Impact Levels

- We said at the outset of this Section that it is often the case that the process of security categorization is triggered through CM and requests for changes to existing information systems.
- In the event modifications to the information system do affect the system's impact level, the system categorization decisions previously made must be reviewed.
- It is important to remember that if the review does result in a change to the system security impact level, the changes must be updated in the system review documentation and security plan.



Section Summary

- This Section used as a basis the three key security requirements required by most information systems: availability, integrity, and confidentiality. Referring to them as “objectives,” they are the pivotal aspects of an information system security program and the necessary properties that must be evident within an information system.

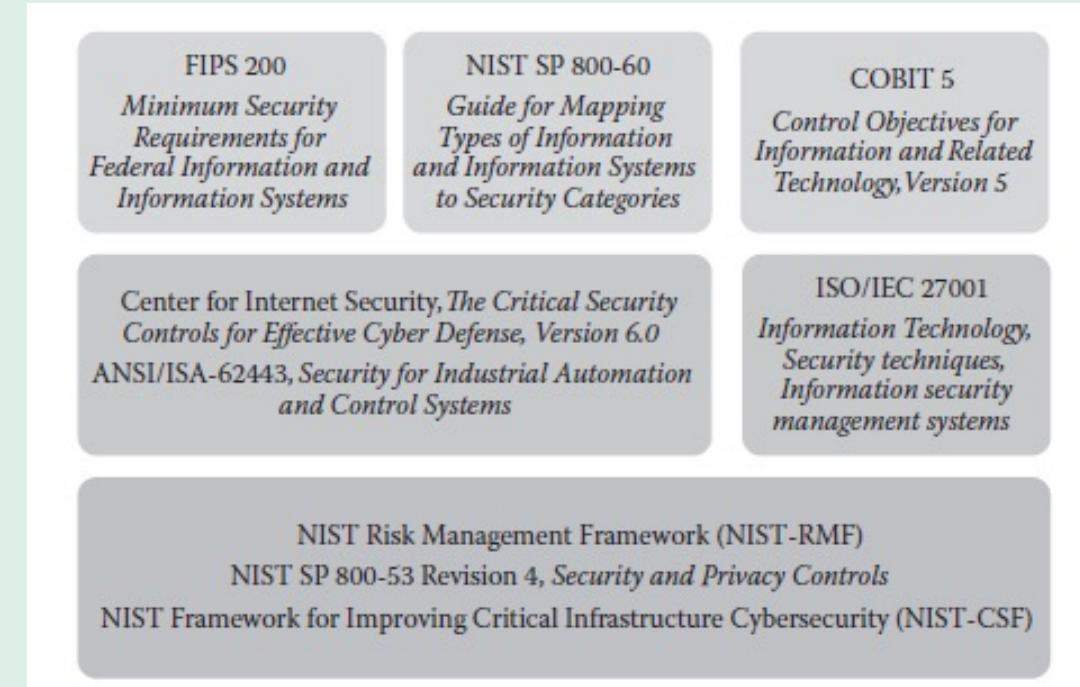


Section 4

Step 2—Select Security Controls

Step 2—Select Security Controls

- A security program, whether at the organization or system level, should include an appropriate mixture of security controls: management, operational, and technical.
- **Management controls** are techniques that are normally addressed by management in the organization's information and communication technology (ICT) security program and focus on managing the entire program and identified risks that may inhibit the organization's ability to mitigate threats and vulnerabilities.
- **Operational controls** are those that are operated by people, as opposed to a technology or systems. These controls often depend on the technical expertise of network and security teams in addition to other management and technical controls.
- **Technical controls** are those that the system executes.



Section 4

Understanding Control Selection

Understanding Control Selection

- The second step in the security control formulation and development process, as defined by the NIST RMF, identifies the security controls necessary to satisfy an ICT system's security requirements and includes tasks associated with documenting those controls in the system security plan.
- The entire set of security controls selected to support an ICT system typically includes both system-specific controls management functions
- The task of identifying common controls can be performed at the organizational level, with a directory or inventory of controls made available to the management overseeing the identification process.



Understanding Control Selection

- Based on the scope and complexity of an ICT system, many security controls are generally considered to be good candidates for inheritance from common control providers.
- Guidelines are based on three criteria, one each for (1) low-impact (2) moderate-impact, and (3) high-impact systems.
- In some instances, organizations may find that a baseline security control applies for a system,
- In still other cases, considering system-specific controls may also lead organizations to select supplemental security controls beyond the minimum requirements specified in the appropriate baseline for the system.



Understanding Control Selection

- The documentation related to security controls must also include criteria related to the reductions or additions made to the security control baselines.
- The completion of security control selection signifies a pivotal point within the organization's security/risk management process.



Section 4

Federal Information Processing Standard

Federal Information Processing Standard Publication 200

- The minimum security requirements, defined by FIPS 200, cover 17 security related areas with regard to protecting the confidentiality, integrity, and availability of systems and the information processed, stored, and transmitted by those systems.
- A new 18th security-related area was added in NIST SP 800-53 (Revision 3), called Program Management. This new addition requires the development of an organization-wide information security program plan.



- | | |
|------------------------|--|
| 13. Personnel security | <ul style="list-style-type: none">• Assurance of the trustworthiness of individuals holding positions of authority within organization's interface with the ICT system.• Assurance that an organization's information ICT systems are adequately protected during and after personnel terminations and transfers.• Policies that enforce formal sanctions on personnel that fail to comply with organizational security policies and procedures. |
|------------------------|--|

 14. Risk assessment |

- | | |
|---------------------|---|
| 14. Risk assessment | <ul style="list-style-type: none">• Scheduled assessments to the risk on the organization's operations (including mission, functions, image, or reputation), organizational assets, and individuals, as a result of operation of the ICT systems. |
|---------------------|---|

 15. Systems and services acquisition |

- | | |
|--------------------------------------|---|
| 15. Systems and services acquisition | <ul style="list-style-type: none">• Resources provided that are necessary to adequately protect the organizations ICT systems.• Implementation of system development life cycle processes that incorporate information security.• Appropriate restrictions to software usage and installation.• Assurance of adequate security measures employed by third party providers. |
|--------------------------------------|---|

 16. System and communications protection |

- | | |
|--|--|
| 16. System and communications protection | <ul style="list-style-type: none">• Ability to monitor, control, and protect organizational communications at the external boundaries and significant internal boundaries of the organizations ICT systems.• Implement architectural design processes, software development techniques, and systems engineering principles that promote effective information security. |
|--|--|

 17. System and information integrity |

- | | |
|--------------------------------------|--|
| 17. System and information integrity | <ul style="list-style-type: none">• Ability to identify, report, and correct information and information system flaws in a timely manner.• Implementation procedures that provide adequate protection from malicious code within the organization's ICT systems.• Ability to monitor information system security alerts and take appropriate actions as necessary. |
|--------------------------------------|--|

7. Identification and authentication	<ul style="list-style-type: none">Identification of system users, processes initiated by a user, or devices and verification that those users, processes, or devices are allowed access to the organization's ICT systems.
8. Incident response	<ul style="list-style-type: none">Establishment of operational incident handling capabilities for the organization's ICT systems that provide proper preparation, detection, analysis, containment, recovery, and user response activities.Implementation of processes that track, document, and report incidents to appropriate senior officials.
9. Maintenance	<ul style="list-style-type: none">Implementation of processes that provide timely maintenance on the organization's ICT systems.Availability of effective controls on the tools, techniques, mechanisms, and staff used to conduct ICT system maintenance.
10. Media protection	<ul style="list-style-type: none">Protection of system media provided.Limitation of access to information on system media, making it only available to authorized users.Sanitization or destruction of system media before disposal or release for reuse.
11. Physical and environmental protection	<ul style="list-style-type: none">Limitation of physical access to ICT systems, equipment, and the respective operating environments to authorized individuals.Protection of the physical facilities and support infrastructure for ICT systems.Availability of supporting utilities for ICT systems.Protection of systems from environmental hazards.Availability of appropriate environmental controls within facilities housing ICT systems.
12. Planning	<ul style="list-style-type: none">Development, documentation, scheduled update of security plans for an organization's ICT systems, containing the details of the security controls in place or planned for implementation into the ICT system in addition to applicable rules of behavior for individuals accessing the systems.

1. Access control	<ul style="list-style-type: none">• Assurance that managers and users of all of the organization's ICT systems are made aware of all security risks related to activities they perform on the systems, as well as any applicable laws, directives, policies, standards, instructions, regulations, or procedures related to the security of the systems.• Assurance that adequate training is provided in order to carry out assigned information security-related duties and responsibilities.
2. Awareness and training	<ul style="list-style-type: none">• Assurance that managers and users of the organization's ICT systems have awareness of the security risks associated with the activities that they perform, in addition to the applicable laws, policies, standards, regulations, or procedures related to the overall security of the systems.• Assurance that adequate training has been provided in order to carry out assigned security-related duties and responsibilities.
3. Audit and accountability	<ul style="list-style-type: none">• Creation, protection, and retention of all system audit records necessary to monitor, analyze, investigate, and report unlawful, unauthorized, or inappropriate system activity.• Assurance that the actions of system users can be traced so that each individual is held accountable for his or her own actions.
4. Certification, accreditation, and security assessment	<ul style="list-style-type: none">• Assessment of ICT security controls for the purpose of determination of effectiveness.• Development and implementation of action plans designed to correct identified deficiencies and reduce or eliminate vulnerabilities in ICT systems.• Authorization procedures related to the operation of ICT systems and any integrated systems.• Frequent monitoring of system security controls to ensure continued effectiveness of the controls.
5. Configuration management	<ul style="list-style-type: none">• Establishment and maintenance of baseline configurations and inventories of ICT systems (including hardware, software, firmware, and documentation) throughout the system life cycle.• Establishment and enforcement of security configuration settings for ICT products utilized by organizational systems.
6. Contingency planning	<ul style="list-style-type: none">• Establishment, maintenance, and effective implement planning for emergency response, backup operations, and post-disaster recovery for ICT systems aimed to ensure the availability of critical information resources and continuity of operations subjected to emergency situations.

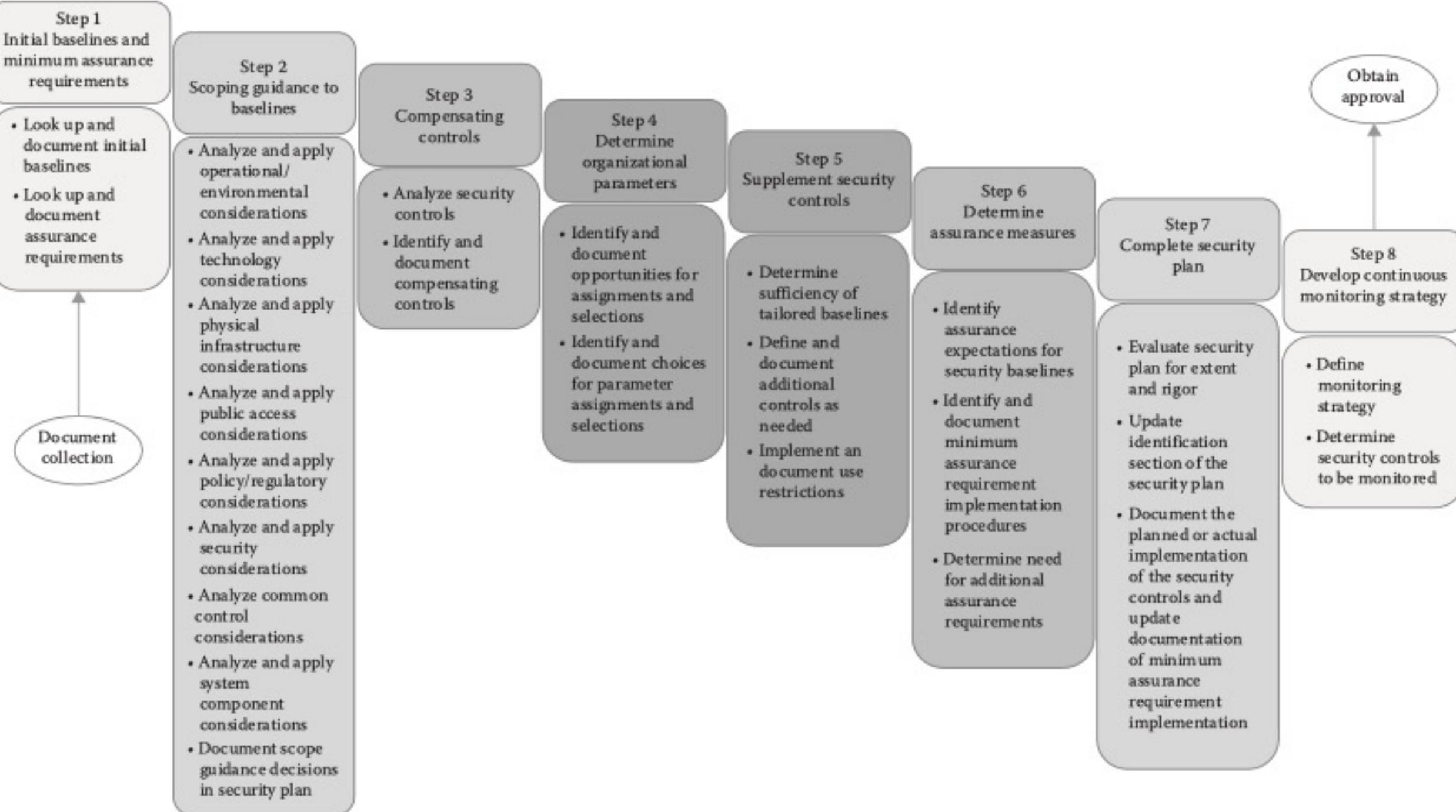
Section 4

Implementation of Step 2—Select Security Controls

Implementation of Step 2—Select Security Controls

- A control identification section
- A supplemental guidance section providing a detailed description of the control
- A control enhancements section providing the optional criteria that organizations can consider, for the control, in order to meet their individual needs
- A references section
- A priority and baseline allocation section matching each control to the established priorities and baselines





Document Collection and Relationship Building

- All organizational ICT systems
- A group of information systems at a specific site
- Common information systems, subsystems, or applications (i.e., common hardware, software, and/or firmware embedded within ICT components) installed at multiple operational sites



Section 4

Select Initial Security Control Baselines and Minimum Assurance Requirements

Select Initial Security Control Baselines

- One of the most difficult realities of the security control selection process is that organizations must find the most cost-effective and appropriate set of security controls to adequately mitigate risk but at the same time comply with security requirements.
- Upon completion of the *security categorization* step of the RMF, the system's impact level has been determined and documented in the security plan.
- The system's security impact level is what determines the initial security base-line.
- Some security controls do not make supplemental guidance or control enhancements indicative in any of the baselines.



Control number	Control name	Tailoring	Rationale
AC-1	Access control policy and procedure		
AC-2	Account management		
AC-3	Access enforcement		
AT-1	Security awareness and training		
AT-4	Security training records		
AU-1	Audit and accountability		
CM-1	Configuration management		
CP-1	Contingency planning		
IA-1	Identification and authentication		
IR-1	Incident response		
MA-1	System maintenance		
MP-1	Media protection		
PE-1	Physical and environmental protection		
SC-1	System and communications protection		
SI-1	System and information integrity		

Select Initial Security Control Baselines and Minimum Assurance Requirements

1. The inclusion of assurance requirements in procurements of ICT systems, or components and services that they contain
2. Establish and maintain system development processes that result in trustworthy ICT
3. Use information technology products within the SDLC processes that demonstrate appropriate security engineering techniques and provide an adequate level of assurance within the processes
4. Be conscious of security risks by deploying trustworthy ICT products within critical systems
5. Collect assurance evidence that justifies trustworthiness is maintained within the organization's ICT system



Section 4

Apply Scoping Guidance to Initial Baselines

Apply Scoping Guidance to Initial Baselines

- Determining the extent that a given security control applicable to a specific information technology is necessary for a specific ICT system
- Development of the specification of compensating security controls, if it becomes necessary to replace recommended security controls.
- Development of the specification of organization-defined parameter values, when required to implement specific security controls.



Apply Scoping Guidance to Initial Baselines

- The activity of applying scoping guidance entails the review of the ICT system to determine whether the use of common controls, physical infrastructure-related considerations, or technology-related considerations is needed.
- To adequately take into consideration the degree to which the operating environment affects the selection of controls .
- Many of the NIST SP 800-53 families have technology-specific controls hat may or may not have been included within the initial baseline for the ICT system under consideration
- In considering technology-specific controls, it is important to note that one control will not necessarily meet all of the security needs related to one type of technology.



Apply Scoping Guidance to Initial Baselines

- A decision must be made about whether or not the control applies to the ICT system
- In addition to considering the operating environment, organizations must also evaluate security implications to the location in which the system components are housed.
- An important decision to make is that a single organizational facility may not house just one ICT component or even one entire ICT system.
- Often, the common control selected to support a particular facet of an organization's physical infrastructure may not provide adequate security protection to the ICT system.



Apply Scoping Guidance to Initial Baselines

- Many ICT systems provide some form of public access.
- As the organization makes its selection of security controls, consideration must be made for the public access necessary of the ICT system and whether or not each baseline control meets the appropriate security needs.
- Security controls directly affected by laws, policies, standards, or regulation are only required if the implementation of those controls directly affects the enforcement of those laws
- Assuming adequate familiarity with all laws, policies, standards, and regulations, the organization must review each baselined control and determine whether the control does or does not apply to the ICT system.



Apply Scoping Guidance to Initial Baselines

NIST SP 800-53 stipulates that security controls that are determined to have an initial baseline that is too high can be downgraded.

- The downgrade provides consistency with the security category for the supported security objectives before moving to system's impact level.
- The downgrade is supported by an organizational assessment of risk.
- The downgrade does not negatively affect the level of protection for the information within the ICT system.



Section 4

Determine Need for Compensating Controls

Determine Need for Compensating Controls

- In making the decision about whether compensating controls are necessary, the organization should perform an analysis on each tailored and baselined security control to determine whether anything prevents it from being implemented due to technical or cost implications.
- Once the most appropriate compensating control has been selected, the baseline control table of the security plan should be updated to reflect that a compensating control was used, along with the rationale for the compensating control.



Determine Organizational Parameters

- The organization should take the time to review each security control to determine whether there is a need to make a parameter assignment within the security control.
- Most organizations have an information security program office or organization-level security team.
- The initial baseline table within the security plan must be updated to indicate that an assignment has been made and the specific details about the choice.



Section 4

Supplement Security Controls

Supplement Security Controls

- To thoroughly understand what supplemental controls are necessary, the organization must analyze the tailored security control baseline to determine whether the controls already selected meet the needs of the ICT system.
- The organization must be cautious not to implement information technology beyond its ability to adequately provide protection
- Once the supplemental security controls are identified, a notation is made in the baseline control table of the security plan.



Determine Assurance Measures for Minimum Assurance Requirements

- The NIST SP 800-53 guideline devotes an entire section to appropriately defining security assurance and trustworthiness from the perspective of security control specification, design, development, implementation, and maintenance.
- As we alluded to earlier in this section, the NIST minimum assurance recommendations are defined in SP 800-53, *Appendix E*.
- Likewise, the guideline recommends that for security controls in ICT systems categorized as moderate impact, the focus should be on actions that foster increased confidence in the correct implementation and operation of each control.



Determine Assurance Measures for Minimum Assurance Requirements

- It is clear that the responsibility of assurance requirements falls squarely on the shoulders of those individuals who perform the tasks
- As each control is designed and implemented, it should be reviewed to determine whether any additional enhancements or documentation is needed to satisfy assessment criteria.
- When documenting in the security plan how the assurance requirements are implemented in the ICT system.

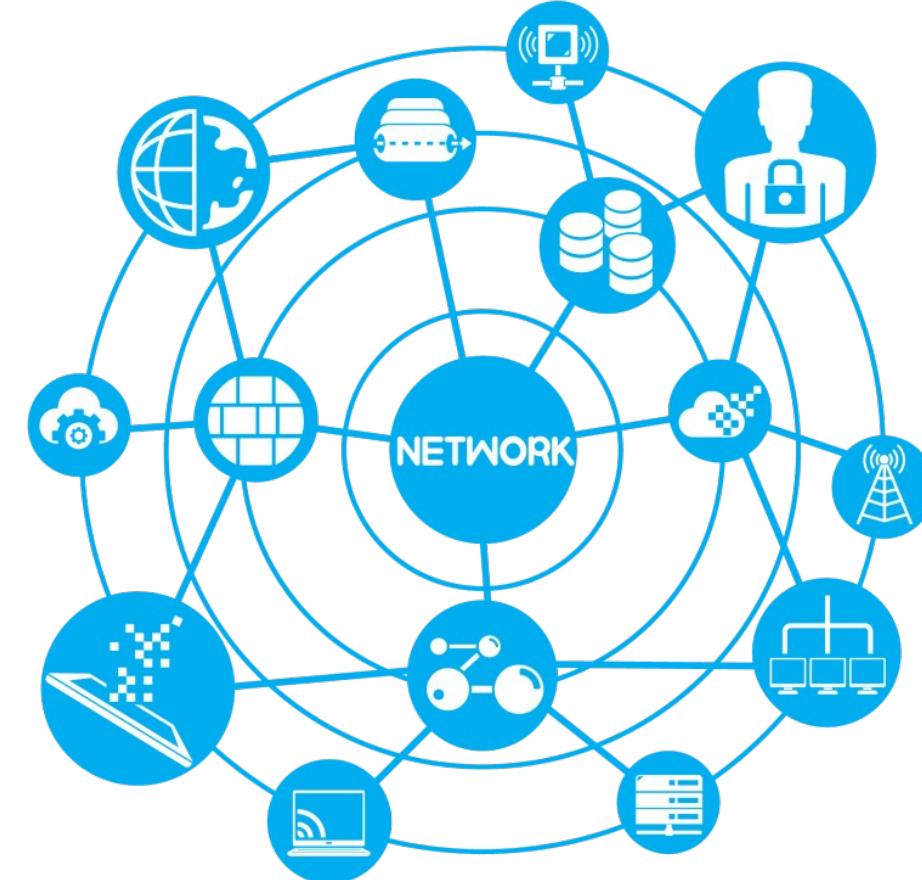


Section 4

Complete Security Plan

Complete Security Plan

- The organization documents the decisions made during the initial security control selection, tailoring, and supplementation processes in the security plan. Each decision must be supported with a convincing rationale that leads to the conclusion that those decisions directly support prescribed security objectives and requirements.
- While the table is an important resource within the plan, the details and definitions related to how each control is designed and implemented are much more extensive and must be present within the larger context of the plan.



Develop Continuous Monitoring Strategy

Upon successful Authorization, the process of continuous monitoring of implemented security controls begins.

- **Define** a continuous monitoring strategy
- **Establish** measures, metrics
- **Implement** a continuous monitoring program
- **Analyze** the data gathered and report findings
- **Respond** to assessment findings by making decisions
- **Review and update** the monitoring program



Approval of Security Plan and Continuous Monitoring Strategy

- It is the responsibility of the organization's authorizing official to determine whether the security plan is complete, consistent, and satisfies the stated security requirements for the ICT system.
- Relative to the approval of the security plan, the authorizing official determines, to the best of their ability and based on the availability of supporting documentation,
- If the security plan is reviewed and considered acceptable, the authorizing official acknowledges acceptance.
- As is the case in most ICT plans and specifications, the front matter of the security plan will provide a page with the names of reviewers and approvers of the document and a place for each to sign and date.



Section 4

Other Control Libraries

Other Control Libraries

- This Section has introduced the Select Security Controls step of the NIST RMF from the perspective of NIST SP 800-53, while using the control libraries of that guideline as a basis for our discussion.
- Aside from NIST SP 800-53 (which has already been discussed) other control libraries include the following.



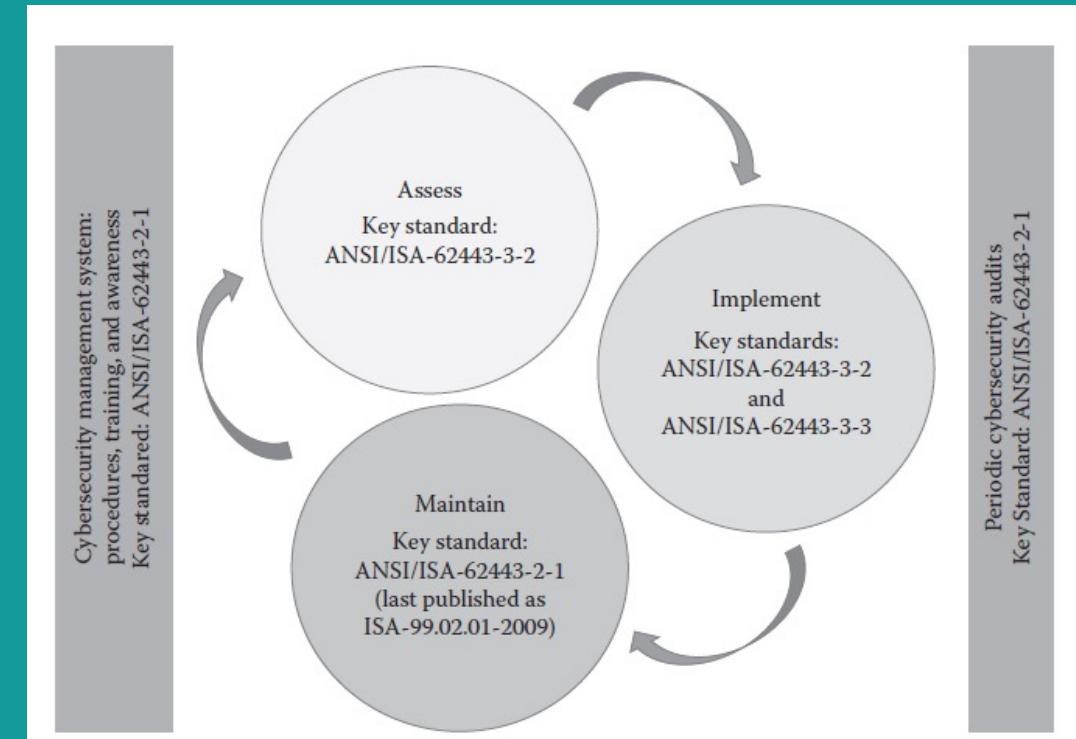
Control Objectives for Information and Related Technology (COBIT 5)

- COBIT 5 is a framework for developing, implementing, monitoring, and improving IT governance and management practices.
- The COBIT 5 framework is published by the IT Governance Institute and the Information Systems Audit and Control Association (ISACA).

-
- Principle 1:** Meeting stakeholder needs
 - Principle 2:** Covering the enterprise end-to-end
 - Principle 3:** Applying a single integrated framework
 - Principle 4:** Enabling a holistic approach
 - Principle 5:** Separating governance from management
-

CIS Critical Security Controls

- The Center for Internet Security (CIS) collaborated to create The Critical Security Controls for Effective Cyber Defense, Version 6.0. The 20 CSC are now governed by the Council on CyberSecurity, an independent, expert, not-for-profit organization with a global scope.



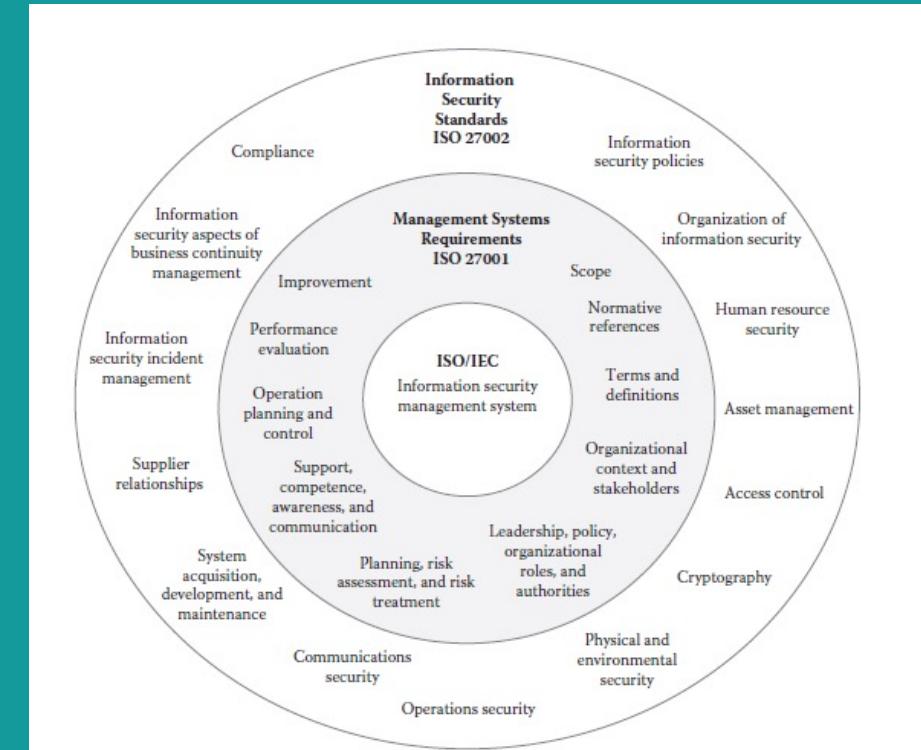
Industrial Automation and Control Systems Security Life Cycle

- The International Society of Automation is a nonprofit professional association that has developed a global standard called the Industrial Automation and Control Systems Security Life Cycle.

Critical Security Control	
1	Inventory of Authorized and Unauthorized Devices
2	Inventory of Authorized and Unauthorized Software
3	Secure Configurations for Hardware and Software
4	Continuous Vulnerability Assessment and Remediation
5	Malware Defenses
6	Application Software Security
7	Wireless Access Control
8	Data Recovery Capability
9	Security Skills Assessment and Appropriate Training to Fill Gaps
10	Secure Configurations for Network Devices
11	Limitation and Control of Network Ports, Protocols, and Services
12	Controlled Use of Administrative Privileges
13	Boundary Defense
14	Maintenance, Monitoring, and Analysis of Audit Logs
15	Controlled Access Based on the Need to Know
16	Account Monitoring and Control
17	Data Protection
18	Incident Response and Management
19	Secure Network Engineering
20	Penetration Tests and Red Team Exercises

ISO/IEC 27001

- The purpose of ISO/IEC 27001 is to help organizations to establish and maintain an ISMS. An ISMS is a set of interrelated elements that organizations use to manage and control information security risks and to protect and preserve the confidentiality, integrity, and availability of information.



Section Summary

- This Section introduced the selection of the security controls step of the NIST RMF.
- The activities and tasks in this step aim to identify the security controls needed to meet the ICT system's security requirements.
- It also has tasks associated with documenting those controls in the system security plan and development of a continuous monitoring strategy.

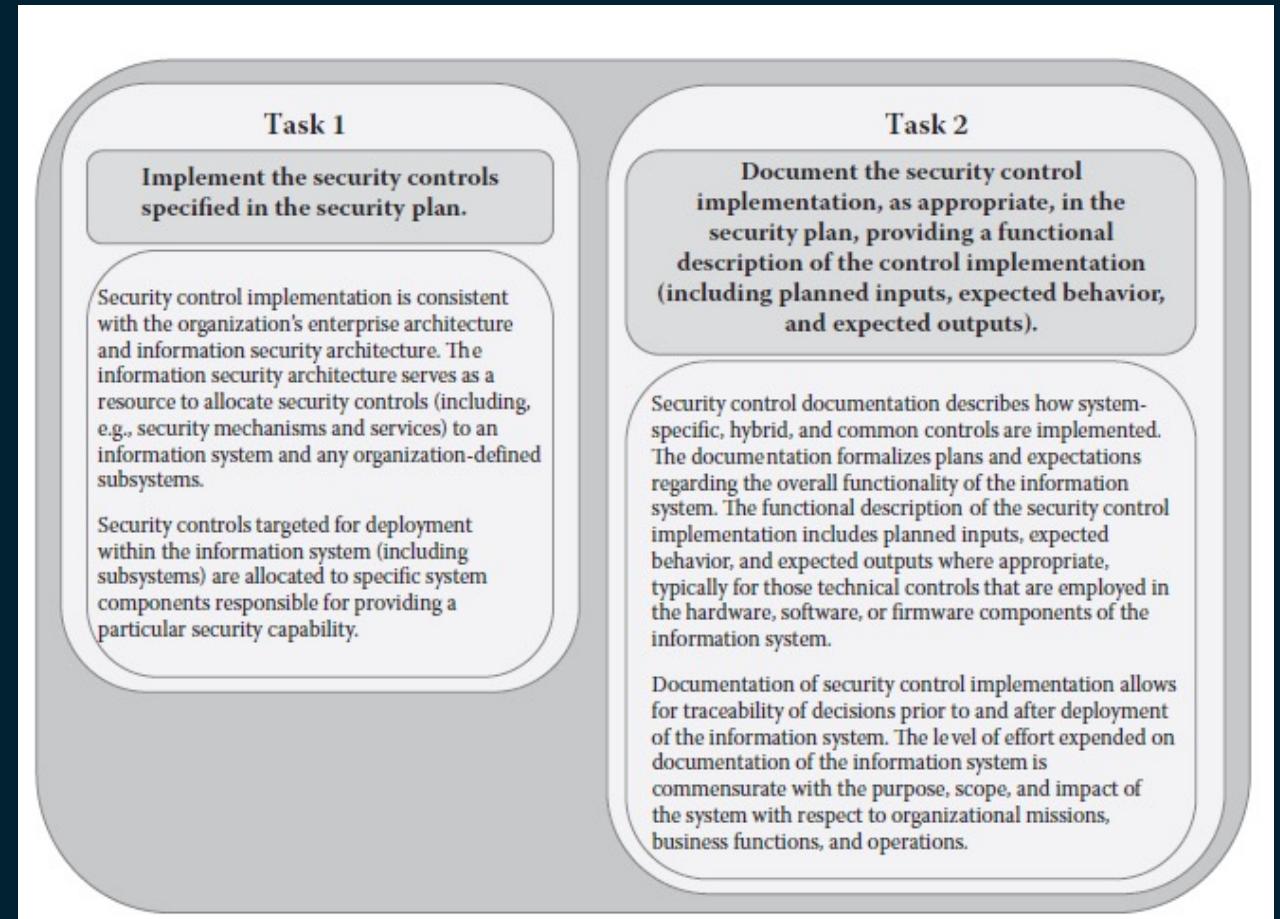


Section 5

Step 3—Implement Security Controls

Introduction

- Implementing security controls involves putting into action the choice that has been made for mitigating risk.
- There are four possible actions for mitigating risk: accept the risk, transfer the risk, limit the risk, or avoid the risk. From



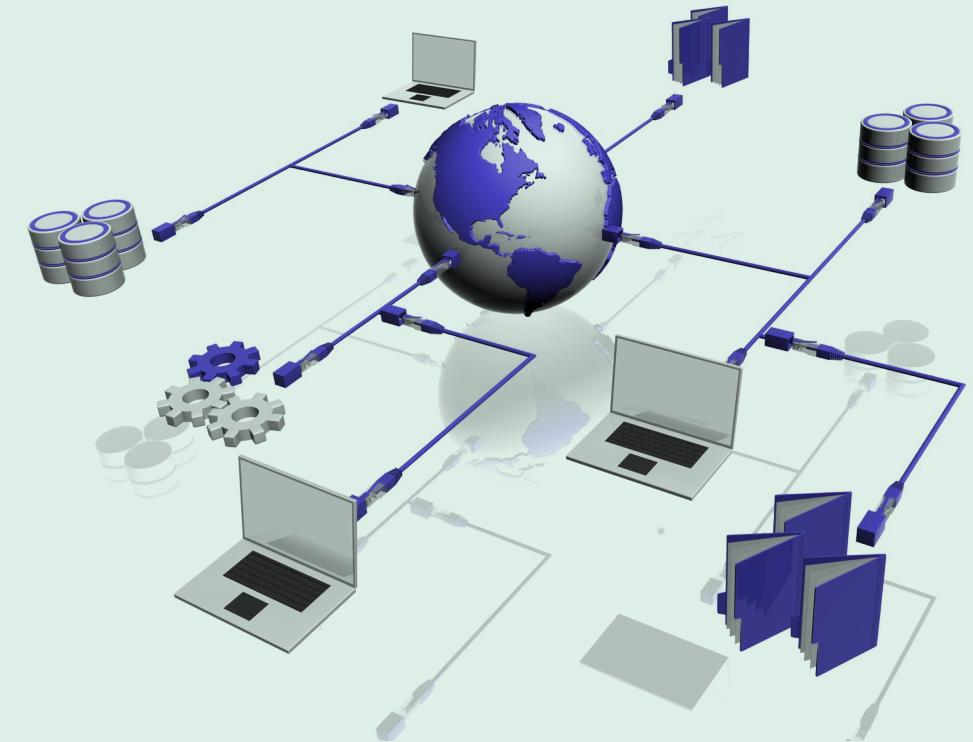


Section 5

Implementation of the Security Controls Specified by the Security Plan

Implementation of the Security Controls Specified by the Security Plan

- It is worthy of mention, up front, that this task of the implementation step of the RMF closely correlates with the supporting processes of the system development life cycle (SDLC), such as agreement, project, technical, software implementation, and software.
- That point, in and of itself, speaks volumes to the importance of the existence of a well-defined life cycle process that integrates with the steps of the RMF.



NIST SP 800 53A guidelines

- The NIST SP 800 53A guideline provides the specific requirements that are used to assess the security controls implemented in the information system. There may be confusion as to why an assessment guideline is being used in support of implementation. The clarification point is simple and rather realistic.



Assessment Objective: *Determine if the organization:*

CP-9(a)	CP-9(a)[1]	Defines a frequency, consistent with recovery time objectives and recovery point objectives as specified in the information system contingency plan, to conduct backups of user-level information contained in the information system.
	CP-9(a)[2]	Conducts backups of user-level information contained in the information system with the organization-defined frequency.
CP-9(b)	CP-9(b)[1]	Defines a frequency, consistent with recovery time objectives and recovery point objectives as specified in the information system contingency plan, to conduct backups of system-level information contained in the information system.
	CP-9(b)[2]	Conducts backups of system-level information contained in the information system with the organization-defined frequency.
CP-9(c)	CP-9(c)[1]	Defines a frequency, consistent with recovery time objectives and recovery point objectives as specified in the information system contingency plan, to conduct backups of information system documentation including security-related documentation.
	CP-9(c)[2]	Conducts backups of information system documentation, including security-related documentation, with the organization-defined frequency.
CP-9(d)	Protects the confidentiality, integrity, and availability of backup information at storage locations.	

Potential Assessment Methods and Objects:

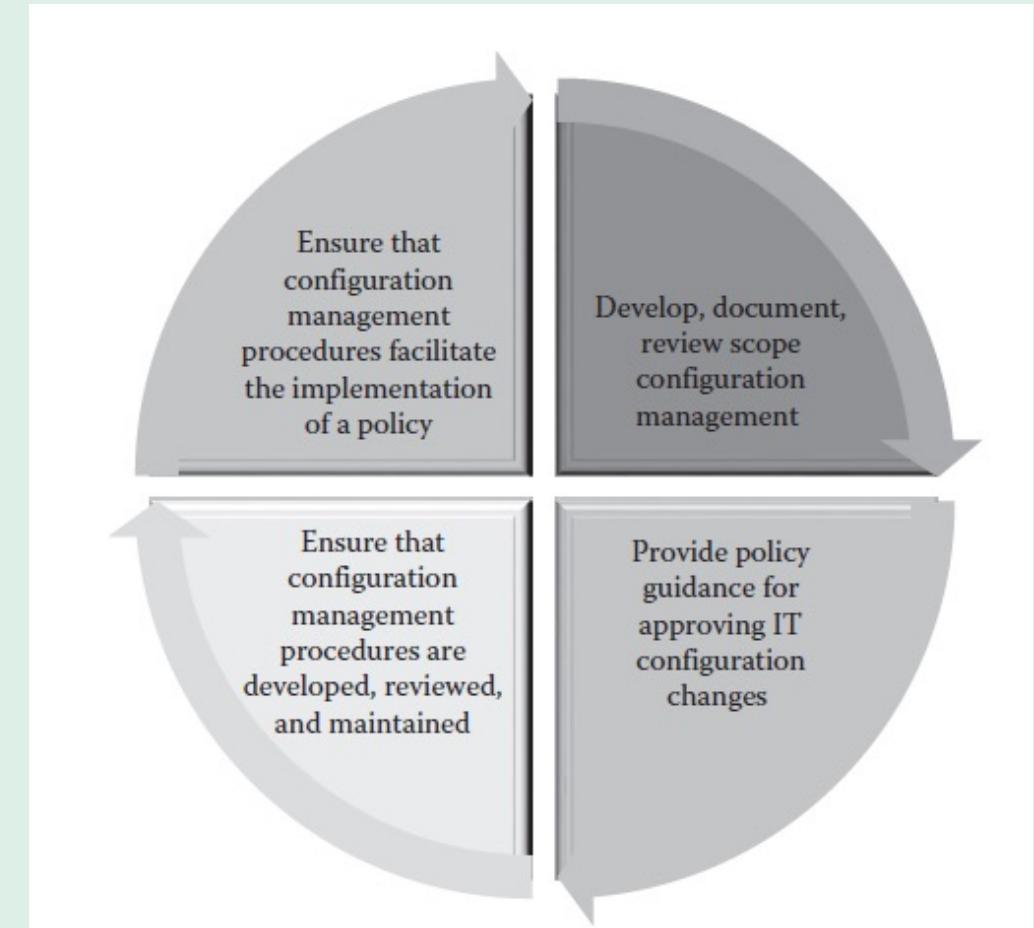
Examine: [SELECT FROM: Contingency planning policy; procedures addressing information system backup; contingency plan; backup storage location(s); information system backup logs or records; other relevant documents or records].

Interview: [SELECT FROM: Organizational personnel with information system backup responsibilities; organizational personnel with information security responsibilities].

Test: [SELECT FROM: Organizational processes for conducting information system backups; automated mechanisms supporting and/or implementing information system backups].

Control provider(s) responsibilities

- Develop, document, and review/update a CM control policy of greater scope to support all affiliated organizations, and define the frequency for reviews and updates.
- Provide policy and guidance for centralizing, managing, and approving IT configuration changes across all affiliated organizations.
- Ensure that system-specific CM procedures are developed, reviewed/updated, and maintained for the systems in accordance with requirements.
- Ensure that system-specific CM procedures facilitate the implementation of the CM policy.



Control provider(s) responsibilities

- It is not uncommon in any facet of the ICT industry for technologies and software currently existing in systems to be reused.
- Prior to implementation, the technology components must be evaluated to ensure that what is being integrated into an ICT system is compliant with specific security standards.



Control provider(s) responsibilities

What many ICT managers fail to realize is that there is a significant amount of coordination that must be ensured in order to just correlate the inheritance of controls from a common control provider:

- The control must have been approved for inheritance by both parties.
- The control's lifetime, its approval status, and approval expiration must be determined.
- The implementing organization then must determine how the common control will be documented in the system's security plan (through reference to the provider's body of evidence or by documenting the control completely)



Section 5

A System Perspective to Implementation

A System Perspective to Implementation

- To better understand the activities of security control implementation from a system perspective.
- In most cases, implementation involves the requirement of constructing external and internal interfaces.
- During the development phase, the developer also produces a technical design for the database and updates the user documentation as necessary.
- Once the technical design is confirmed to be correct, it is turned over to the internal staff or outside contractors that do the actual construction.
- Upon completion of the activities of the security control selection step, the security plan will provide criteria relative to what controls, common controls, hybrid controls, and control enhancements are required for implementation within the ICT system.



A System Perspective to Implementation

- One of the key tasks in implementing security controls within ICT systems is the design of the security architecture.
- The main objective of security architecture is to specify which security controls apply to the various components of the ICT system and clearly establish the context by which common or hybrid controls are allocated.
- It is common practice for the organization to allocate security controls to an ICT system consistent with the organization's enterprise architecture relative to its security architecture.



A System Perspective to Implementation

- With a greater insight and appreciation for enterprise architecture, we now turn our attention to security architecture.
- As a security architecture evolves over time, organizations should identify and implement common security controls supporting multiple ICT systems as much as possible.
- The security controls are implemented through a life cycle process called security engineering.
- The advantage of applying security engineering principles to control implementation is that they provide a plethora of general guidance



Section 5

A Management Perspective to Implementation

A Management Perspective to Implementation

- In considering the scope from which management should be understood with respect to security control implementation, the discussion can lead in two directions.
- Because the NIST RMF is intended to be generic, this model essentially serves as a template rather than the actual implementation of practical controls.
- The creation of a functioning, real-world control system requires the performance of an individually planned and intentionally executed risk management process within the specific setting where the controls will be operated.



Implementation via Security Life Cycle Management

- For the purposes of security assurance, security life cycle management is practiced when each of the minimally required management controls within the domains seen in Figure is in place and capable of being improved

Security Control Class	Security Control Family	Identifier
1	Technical	Access control
2	Operational	Awareness and training
3	Technical	Audit and accountability
4	Management	Certification, accreditation, and security assessments
5	Operational	Configuration management
6	Operational	Contingency planning
7	Technical	Identification and authentication
8	Operational	Incident response
9	Operational	Maintenance
10	Operational	Media protection
11	Operational	Physical and environmental protection
12	Management	Planning
13	Operational	Personnel security
14	Management	Risk assessment
15	Management	System and services acquisition
16	Technical	System and communications protection
17	Operational	System and information integrity

Implementation via Security Life Cycle Management

- In order to ensure proper integration, security life cycle management has to create and then coordinate a top-level process that combines and subsequently manages all of the underlying life cycle management functions that are required to support the security requirements of the organization.
- In much the same way that tailoring is performed, according to the RMF, to establish required security controls
- It is important to ensure the continuing day-to-day effectiveness of activities that comprise that process.
- Persistent observation and quantitative assessment of performance are critical to security life cycle management.
- There are always costs and risks associated with large security development projects.



Section 5

Establishing Effective Security Implementation through Infrastructure Management

Establishing Effective Security Implementation through Infrastructure Management

sources can be tapped to assist in developing a detailed infrastructure specification:

- Current standard operating procedures within the organization
- Current or commonly recognized methods
- Other assigned responsibilities from the organization that might not be covered by the preceding two items
- Any contract stipulations



Establishing Effective Security Implementation through Infrastructure Management

- An important assumption that we are making is that every organization will establish a formal infrastructure appropriately tailored to its needs.
- The next step is to formally define ETX specifications for each task to fit within the adopted framework.
- The overall execution of the implementation process must be uniform, yet because every component in the project is unique, it must be tailored specifically.
- Partly because of its monumental and somewhat indistinct scope, the infrastructure management of security implementation is one of the simplest to execute.



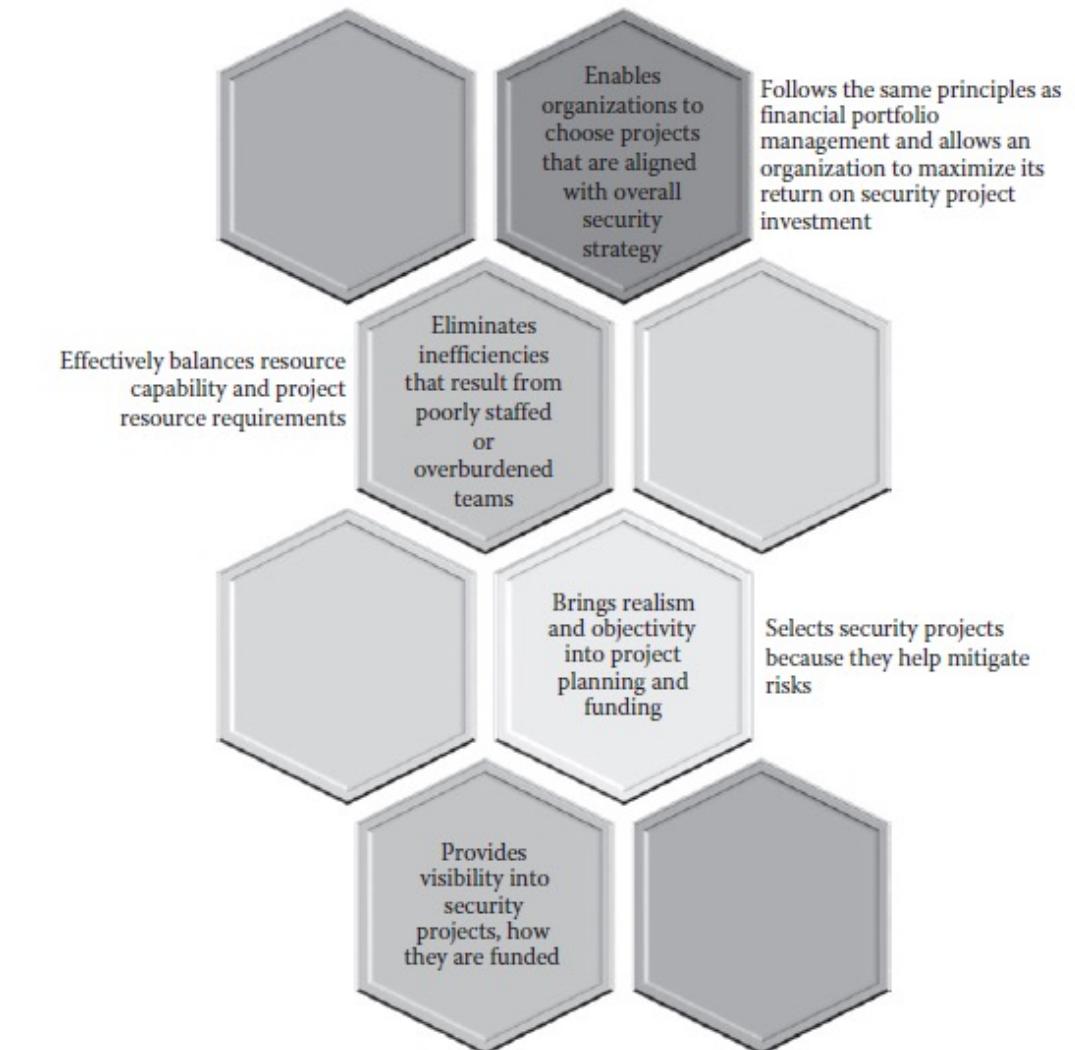
Section 5

Security Implementation Projects and Organization Portfolios

Finding the Fit: Security Implementation Projects and Organization Portfolios

Project portfolio management (PPM) is often not understood or embraced in large organizations and sometimes is managed haphazardly. Many definitions of PPM have emerged over the years. Sometimes, it is easier to describe something by explaining what it is not. PPM is neither just enterprise-wide project management nor simply the management of projects and metrics generation across various programs and projects.

- No organization consciously funds a project that it knows will fail, but changes in security requirements, business functions, economics, or market conditions can render some projects nonviable.



Security Implementation Project Management

- Project management for security engineering projects involves defining and deployment of a fully integrated set of security implementation life cycle activities.
- Project definition and subsequent coordination also ensure the efficient utilization of resources.
- The project management plan is the essential first condition for ensuring best practice at the project level.
- The project's manager is also responsible for actually writing the plan and then maintaining it, once it has been approved.
- Thus, the goal of the plan is to ensure that the intended business and technical work will progress down a logical timeline to a final product, which satisfies the security needs of the organization, its supply chain, and its customers.



Three big-picture questions

- What is the precise mission of the team?
- What are the specific organizational competencies required to achieve that mission?
- Are those competencies available for this particular project?

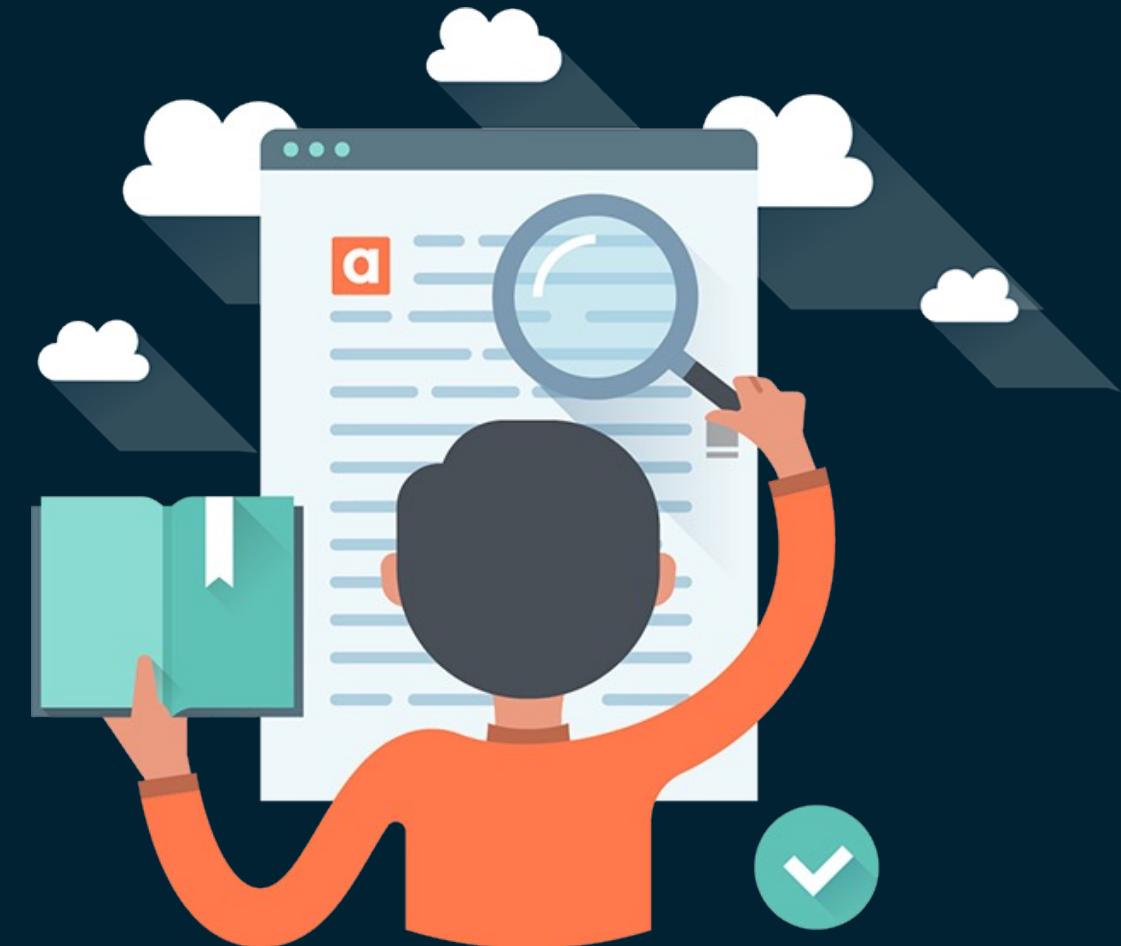


Section 5

Document the Security Control Implementation in the Security Plan

Document the Security Control Implementation in the Security Plan

- The NIST RMF takes the support of documentation a step further than simply describing the activities performed to implement each security control.
- The NIST RMF takes the support of documentation a step further than simply describing the activities performed to implement each security control.
- Through documentation, the organization is able to effectively create a balance between the level of effort and the impact that implementing each control
- It is important to note that the documentation created during this task becomes part of the authorization package



Document the Security Control Implementation in the Security Plan

- In addition to the authorization package requiring all of the life cycle documentation and control implementation and documentation traceability validation, it also requires an updated security plan.
- The advantage of this method of documentation is that it ensures security control assessors are able to expeditiously identify the location of the method employed to implement a given security control.



Section Summary

- This Section presented the practice of logic that should be performed, from a system and managerial perspective, by organizations that have a vested incentive to properly implementing cybersecurity controls.



Section 6

Step 4—Assess Security Controls

Understanding Security Control Assessment

- The security control assessment process aims to gather and evaluate security control information and evidence produced by the ICT risk management program, common control providers, and individuals responsible for developing and deploying the ICT system.
- The security assessment process and the security control assessors/ auditors who execute it typically have no prior responsibility in the development or enhancement of any of the security controls.



NIST SP 800-53A
Revision 4
*Security and Privacy
Controls in Federal
Information Systems
and Organizations*

NIST SP 800-115
*Technical Guide to
Information Security
Testing and
Assessment*

NIST SP 800-37 Revision 1
*Guide for Applying the
Risk Management
Framework*

NIST Risk Management Framework (NIST RMF)

Information produced through the control assessment process can be used

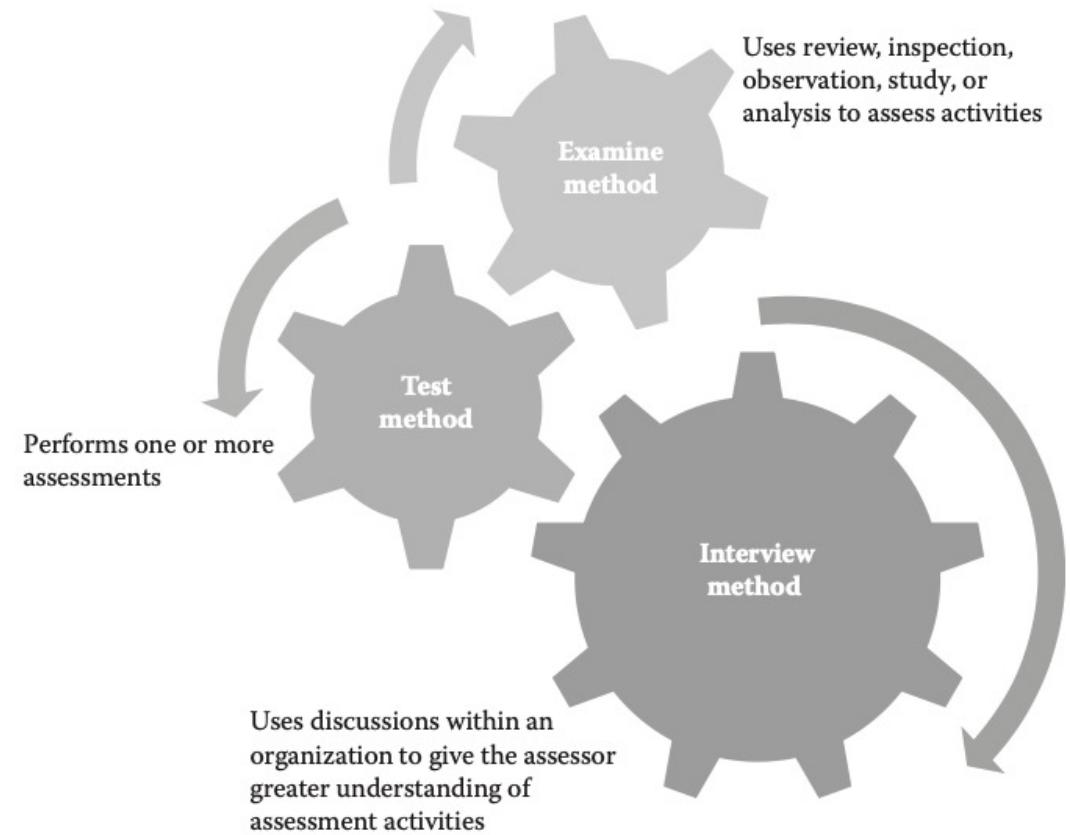
- Identify problems that may have occurred in the organization's implementation of RMF
- Identify the security or privacy issues in the ICT system and its operating environment
- Prioritize risk mitigation decisions and activities
- Verify and validate that the identified security or privacy issues in the ICT system operating environment are adequately corrected
- Implement mechanisms for support monitoring, and information security and privacy awareness
- Make security authorization, privacy authorization, and ongoing authorization decisions
- Make data-driven budgetary decisions directly impacting the capital investment process

Section 6

Components of Security Control Assessment

Components of Security Control Assessment

- The examine method uses review, inspection, observation, studying, or analyzing assessment specifications and activities.
- The interview method uses discussions among individuals or groups within an organization to give the assessor greater understanding, obtain clarification on observations that may have been performed, or gather evidence of implemented security controls.
- The test method performs one or more assessments.



Components of Security Control Assessment

- The assessment team normally works closely with the organizational management, internal audit team, and other members of the security team during the security control assessment planning process to choose the appropriate methods and objects for each control and to determine the applicable scope of each assessment method.
- NIST SP 800 series of guidelines is quickly becoming the de facto standard for security control formulation



Section 6

Control Assessment and the SDLC

Control Assessment and the SDLC

Some of the benefits of integrating security assessments into the SDLC include:

- Early identification and mitigation of security vulnerabilities, thus reducing the cost of implementing security controls
- Proactive action taken to reduce engineering challenges caused by mandatory security controls
- Awareness of the availability of shared security services and ability to reuse security strategies and tools, thus reducing development costs
- Capability of informed and timely decision-making through the capacities present of a risk management process
- Streamlined documentation of the security decisions that directly affect the development process and the security considerations made during those processes
- Greater flexibility in capabilities provided by systems interoperability and integration

Control Assessment and the SDLC

- To assure continuous security control effectiveness, security assessments are also conducted during the operations and maintenance phases of the life cycle
- The vital point to remember about this discussion is that the organization must continuously assess all implemented security controls on an ongoing basis in accordance with its information security continuous monitoring plan.



Section 6

Ensuring Adequate Control Implementation

Ensuring Adequate Control Implementation

- Compile evidence from pertinent activities within the SDLC that the controls prescribed for the ICT system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements of the system and the organization.
- Present the resulting evidence in a way that allows decision-makers to use it effectively in making the risk-based decisions about the operation or use of the system.



Ensuring Adequate Control Implementation

- Over the past decade, organizations are increasingly becoming “data-driven.”
- The assessment evidence needed to make such decisions can be obtained from a variety of sources such as the availability of the ICT component and system assessments.
- Conversely, the system assessments provide a larger scope of evidence of effectiveness.



Section 6

Assessment Plan Development, Review, and Approval

Assessment Plan Development, Review, and Approval

- Defined organizational requirements that affect the compliance of assessments
- Defined roles and responsibilities of the individuals approving and executing the assessments
- Strategies for adherence to established methodology
- Established assessment frequency requirements
- A list of documentation requirements (such as assessment plans and assessment results) and a procedure for storage and retrieval

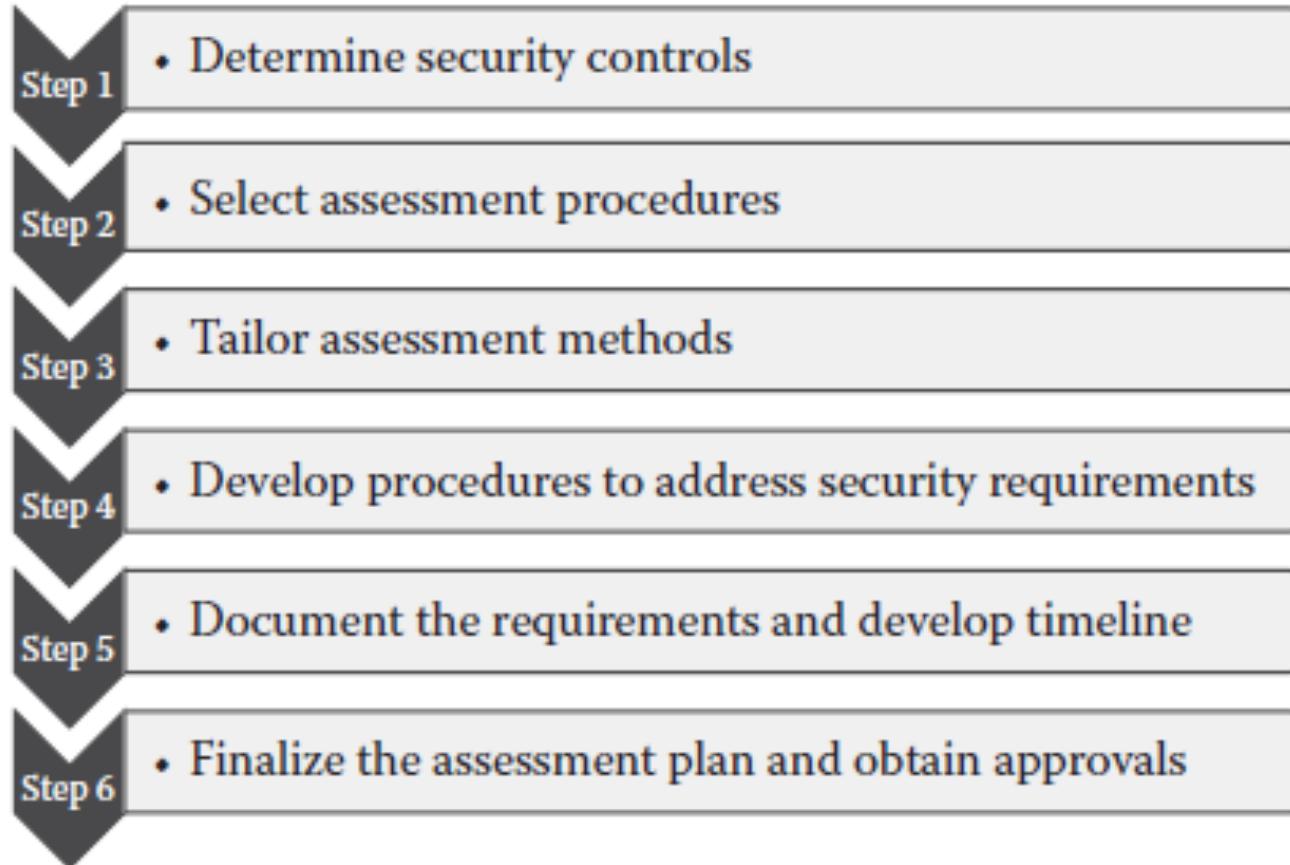


NIST recommends that the following three factors

- The system security categorization
- The set of security controls selected for the system that fall within the scope of the assessment
- The level of assurance the organization needs to satisfy to determine the effectiveness of implemented security controls



complete and comprehensive NIST compliant document

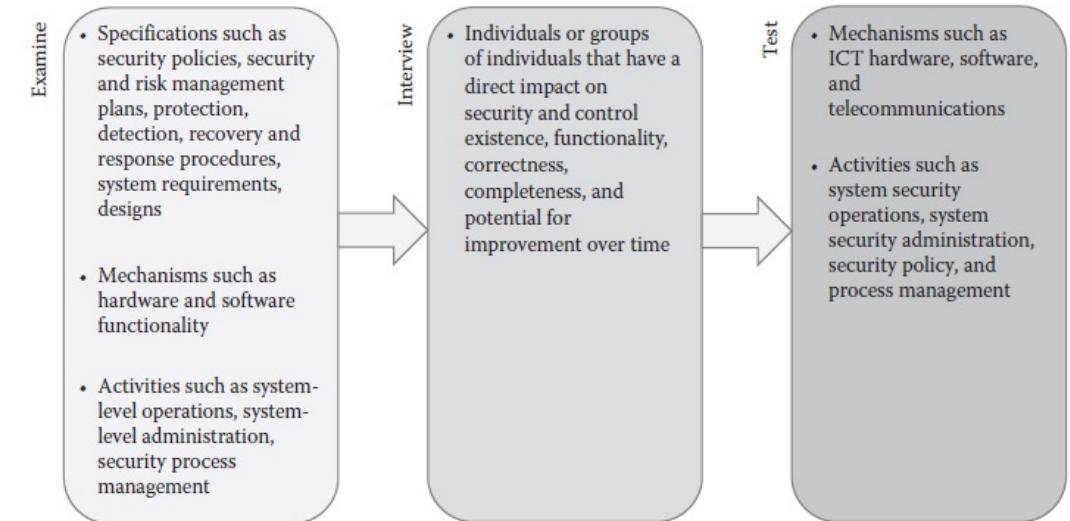


Section 6

Security Control Assessment Procedures and Methodologies

Security Control Assessment Procedures and Methodologies

- The recommendation set forth by the NIST RMF is that organizations utilize the most effective approach for the set of security controls they have implemented and the security priorities the organization has established.
- Such a methodology should contain the following phases at a minimum:
 - **Planning**
 - **Execution**
 - **Postexecution**



Assess Controls in Accordance with Assessment Plan

- The second task of Step 4 of the NIST RMF stipulates that once the assessment plan has progressed through the appropriate approval process, management oversight must ensure that security control assessment proceeds according to the schedule and approach specified in the plan.
- Evidence obtained through performing activities of the SDLC justifying that the controls implemented in the ICT system have been done so correctly, are operating as intended, and are producing the desired outcome based on established security and privacy requirements
- Presenting the evidence in a way that assists decision-makers in making risk-based decisions effectively



Level	Depth	Coverage
Basic	<ul style="list-style-type: none"> • High-level reviews, observations, or inspections of the assessment objects, discussions with ICT professionals, or tests on the basis of no previous knowledge of internal control implementation details. • Conducted using limited evidence, generalized questions, or functional control specifications. • Results are basic assessments providing a high level of understanding of the security control necessary for determining whether the control is implemented and error free. 	Uses a sample set of assessment objects that provide just enough coverage necessary for determining whether the security control is implemented and error free.
Focused	<ul style="list-style-type: none"> • Greater depth of analysis is performed on each assessment object. • Conducted using a substantial amount of evidence, detailed questions, or high-level design and process descriptions for controls. • Provide a level of understanding for determining whether the control is implemented and error free, and the assurance that the control is implemented correctly and operating according to specification. 	Uses a sample set of assessment objects and other pertinent assessment objects considered important to achieving the assessment objective to provide a higher level of coverage necessary for determining whether the security control is implemented and error free and there exists assurance that the control is implemented correctly and operating according to specification.
Comprehensive	<ul style="list-style-type: none"> • Activities that can range from basic or focused levels to a very detailed depth of analysis of the assessment object. • Conducted using an extensive amount of evidence, in-depth interview questions, or detailed technical control specifications. • Provide a level of understanding of the security control necessary for determining whether the control is implemented and error free, and the assurance that the control is implemented correctly and operating as intended on an ongoing and consistent basis. • There is evidence that supports continuous improvement in the effectiveness of the control. 	Uses a large sample set of assessment objects and other pertinent assessment objects considered to be important to achieving the assessment objective to provide the greatest level possible of coverage necessary for determining whether the security control is implemented and error free, and there exists assurance that the control is implemented correctly and operating according to specification, and that there is support for continuous improvement in the effectiveness of the control.

Assess Controls in Accordance with Assessment Plan

- Assessment objectives for each control are achieved by performing the defined assessment methods on individual assessment objects and then documenting the evidence.
- In most cases, the finding of *other than satisfied* indicates weaknesses or deficiencies in a control's implementation.
- Regardless of the procedure, it is important that security control assessment findings be objective, evidence-based indications of the way the organization has implemented each security control.



Section 6

Prepare the Security Assessment Report

Prepare the Security Assessment Report

- The third task of the security control assessment step is a draft security assessment report.
- Once prepared, the organizational management together with the ICT system users and common control providers review the security assessment reports, privacy assessment reports, and updated risk assessment to determine the next steps required in response to the identified weaknesses and deficiencies.



NIST SP 800-53A stipulates the following content be included within the report

Specifically, NIST SP 800-53A stipulates the following content be included within the report:

- The information system name
- The impact level assigned to the system
- Results of previous assessments or other related documentation
- The identifier of each control or control enhancement assessed
- The assessment methods and objects used and level of depth and coverage for each control or enhancement
- A summary of assessment findings
- Assessor comments or recommendations



SC-6	Resource objective		
	Assessment objective <i>Determine if:</i>		
	SC-6[1]	<i>The organization defines resources to be allocated to protect the availability of resources (S)</i>	
	SC-6[2]	<i>The organization defines security safeguards to be employed to protect the availability of resources (S)</i>	
	SC-6[3]	<i>The information system protects the availability of resources by allocating organization-defined resources by one or more of the following: (O)</i>	
	SC-6[3][a]	<i>Priority</i>	
	SC-6[3][b]	<i>Quota</i>	
	SC-6[3][c]	<i>Organization-defined safeguards</i>	
	Comments and recommendations:		
	SC-6[3] was marked as other than satisfied because the assessors could not find any evidence, within any ICT specifications or plans that the organization allocates resources based on one of the three defined criteria as indicated in SC-6[3][a],[b], or [c].		

Section 6

Initial Remedy Actions of Assessment Findings

Initial Remedy Actions of Assessment Findings

- The finalized security assessment report provides awareness about specific weaknesses and deficiencies in the security controls within an organization or through their control provider that were not resolved during system development.
- The advantage of a system audit is that it includes details of technical verification of the changes that have been implemented on the system
- The process of security control reassessment is intended to determine the extent to which the remediated controls have been implemented correctly,



Initial Remedy Actions of Assessment Findings

- In a postmortem of the remediation process, some organizations and control providers choose to prepare an addendum to the security assessment report in response to the initial findings of the assessors.
- We must emphasize that the addendum to the security assessment report does not change any of the findings documented within it, and is not intended to be influential in any manner.

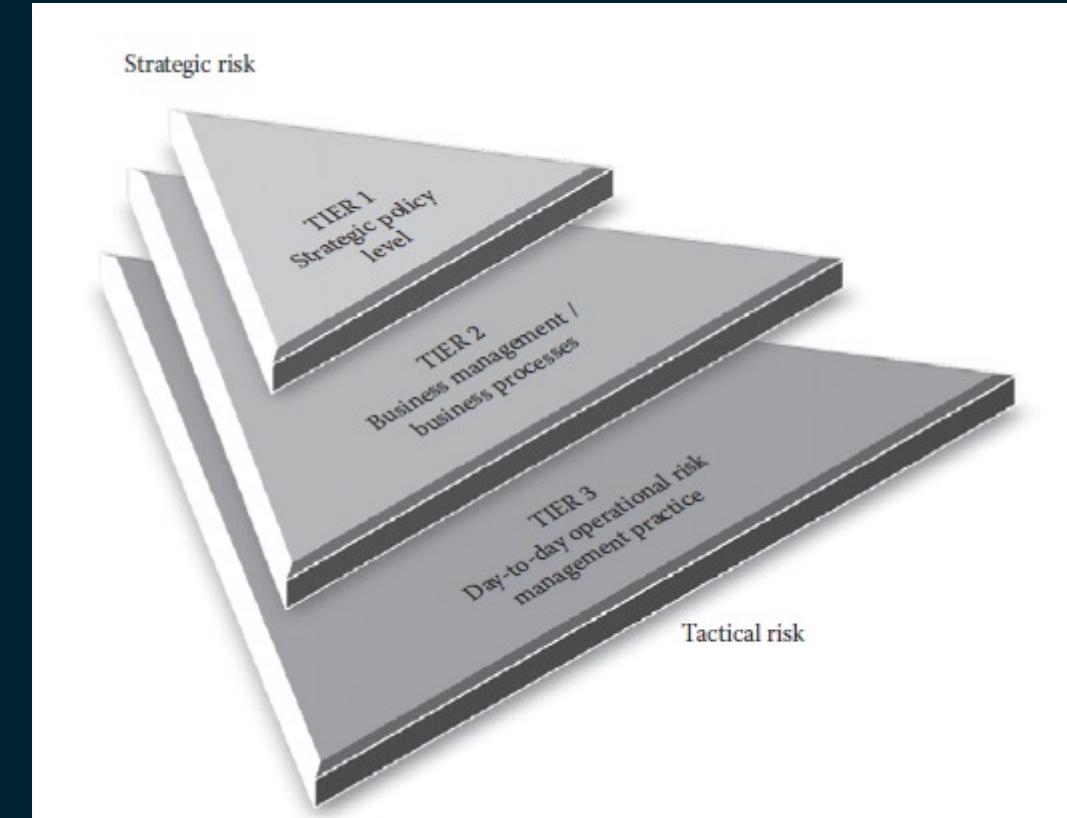


Section 7

Step 5—Authorize: Preparing the Information System for Use

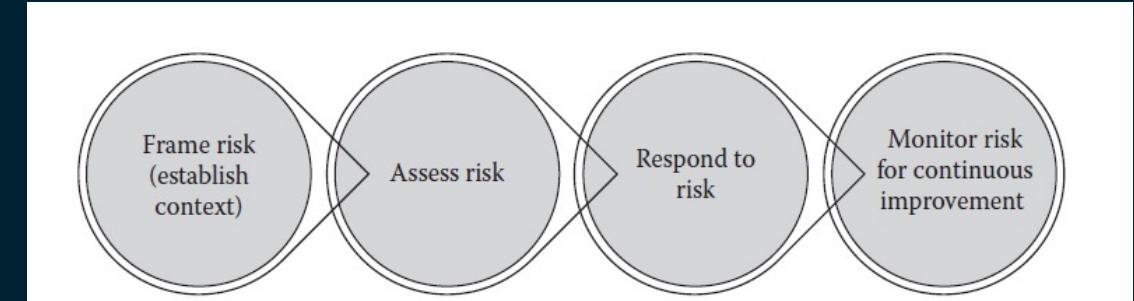
Authorizing the Formal Risk Response

- This Section describes the fundamental concepts associated with Authorize Information System, Step 5 of the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) (NIST, 2014).
- The Authorization phase includes the documentation of the acceptance of a formally sanctioned, organization-wide, and systematic approach to the risk management needs of a given situation.



NIST SP 800-39

- According to NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, risk management is a comprehensive process that requires organizations to systematically (NIST, 2011)
- Frame risk (i.e., establish the context for risk-based decisions)
- Assess risk
- Respond to risk once determined
- Monitor risk on an ongoing basis for continuous organizational improvement



Section 7

Elements of Risk Management

Elements of Risk Management

- The aim of this step is to make clear and transparent any and all forms of risk or threat across the organization.
- Establishing a realistic and credible risk frame requires the organization to lay out all of its underlying assumptions about the current threat environment.
- More importantly, the organizational risk tolerance, or appetite, has to be made clear up front. This includes the levels of risk, types of risk that must be addressed, as well as the acceptable degree of risk uncertainty.



Elements of Risk Management

- The second component of risk management is risk assessment.
- It is necessary for the organization to adopt and document an unambiguous set of standard methods and tools that will be employed in the risk assessment/management process for that given situation.
- The third component of general risk management involves the development of the organizational response to risk.
- The actual execution of this stage of the process depends on the organization's ability to acceptably choose between the classic types of risk responses that might be implemented for a given situation.



Section 7

Certification and Accreditation

Certification and Accreditation

- Authorization typically involves the concepts and general practices of the formal C&A process.
- ***Certification and Accreditation*** describes a well-defined and systematic procedure for evaluating, describing, testing, and authorizing systems
- ***Accreditation*** is a formal and well-defined organizational process for performing certification.



The Accreditation and Certification Process

- **The accreditation process** ensures that the testing and audit practices of the certifying body are sufficient to distinguish conformance with a given standard, or regulation, as well as to certify that the audited parties behave ethically and employ appropriate control assurance.
- **The certification process** itself is meant to evaluate, test, and audit security control behaviors in order to confirm that those behaviors meet predetermined criteria.



Section 7

Application of the RMF

Application of the RMF

It is commonly recognized that risk management is a holistic activity that must be fully integrated into every aspect of the organization in order to be effective.

- Ensure that senior leaders/executives recognize the importance of managing information security risk.
- Ensure that the organization's risk management process is being effectively conducted.
- Foster an organizational climate where information security risk is considered.
- Help individuals with responsibilities for information system implementation.



Four key factors

- The effective organization-wide management of risk to information systems requires the following four key factors (NIST, 2011):
- Assignment of risk management responsibilities to senior leaders/executives
- Ongoing recognition and understanding by senior leaders/executives of the information security risks to organizational operations and assets arising from the operation and use of information systems
- Establishing the organizational tolerance for risk and communicating the risk tolerance throughout the organization
- Accountability by senior leaders/executives for their risk management decisions and for the implementation of effective, organization-wide risk management programs



Three Tires for Risk Management

- *Tier One* approaches the management of risk from a *strategic* perspective.
- *Tier Two* addresses risk from a mission and business process perspective.
- *Tier Three* addresses risk from an *operational* perspective.



Section 7

Security Authorizations/Approvals to Operate

Security Authorizations/Approvals to Operate

- Formal authorization of federal systems is required by the E-Government Act of 2002. Specifically, these authorizations are mandated by Title III of that Act: FISMA.
- Because of their importance, these authorizations are always granted by a senior organizational official.
- The security authorization process involves comprehensive testing and evaluation of all of the designated security controls within an information system.
- Every system that falls under the purview of FISMA must have an *Authority to Operate* granted before it becomes operational.



Security Authorizations/Approvals to Operate

- The assessment results and the authorization decision are all captured in an *Accreditation Decision Letter* that is typically issued prior to system launch.
- In general, the process for conducting a reauthorization is the same, which is used to conduct the initial security authorization.
- The interest from the standpoint of this book is that the security authorization process is the current end result of the implementation of the NIST RMF.



Section 7

Certification of the Correctness of Security Controls

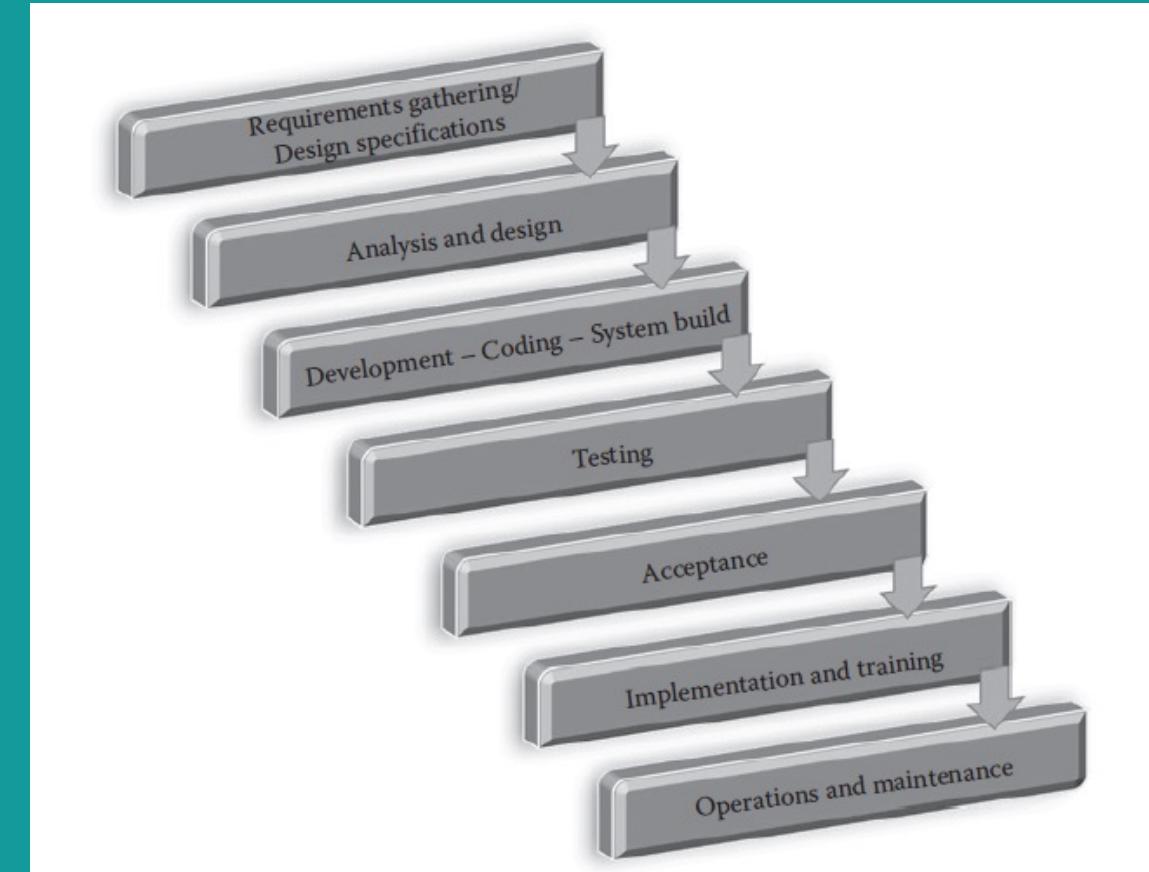
Certification of the Correctness of Security Controls

- Within the federal government, all unclassified systems including general support systems and major governmental applications fall under FISMA. Therefore, they must be assessed and authorized in accordance with a well-defined and commonly accepted process sanctioned by the government.
- NIST DP 800-37 defines three types of controls that might be potentially certified as effective.
- **system-specific controls**
- **common controls.**
- **hybrid controls**



Risk Management and Enterprise Architecture

- Risk management is substantively enabled through the design and implementation of an organization-wide enterprise architectural process.
- This process designs and implements the tangible proof that the various strategies the organization has adopted to facilitate its day-to-day operation are in place and functioning properly
- A top-down conceptual approach to coherent design is capable of ensuring a tightly integrated operational risk management process for the organization



Section 7

Particular Role of Requirements

Particular Role of Requirements

- General requirements definition is a critical part of any system development process as it defines the shape of the system and all subsequent activity devolves from that understanding.
- Security requirements are a critical element within that phase, since they are derived as part of the overall definition of the functional and nonfunctional requirements set for the information system.
- In essence, security requirements are a subset of the general functional and nonfunctional requirements.



Drawing Hard Perimeters

- With regard to risk management and enterprise architecture in general, the term system boundary, or perimeter, is synonymous with the authorization boundary, for example, the precise limits of the system that is being certified.
- Because that definition is conceptual in nature, the organization has significant flexibility in determining what constitutes an information system and its associated boundary.
- The need to draw a precise and unambiguously understood boundary around the system elements that will be assured.



Section 7

Preparing the Action Plan

Preparing the Action Plan

- The authorize phase of the NIST RMF is where the authorizing officer makes a decision whether or not to authorize the system for operation.
- The security assessment report contains the findings from the testing

Specifically, the plan of action and milestones identifies :

- The tasks to be accomplished with a recommendation for completion either before or after information system implementation
- The resources required to accomplish the tasks
- Any milestones in meeting the tasks
- The scheduled completion dates for the milestones



Preparing the Action Plan

The strategy must be able to ensure that organizational plans of action and milestones are directly referenced to the earlier findings of the NIST RMF process, and it must specifically align with:

- The security categorization of the information system (NIST RMF Step 1)
- The specific weaknesses or deficiencies in the security controls (NIST RMF Step 2)
- The organization's proposed approach to mitigate the identified weaknesses or deficiencies in the security controls (NIST RMF Step 3)
- The direct or indirect effect that the weakness or deficiency might have on the overall risk exposure of the organization (NIST RMF Step 4)

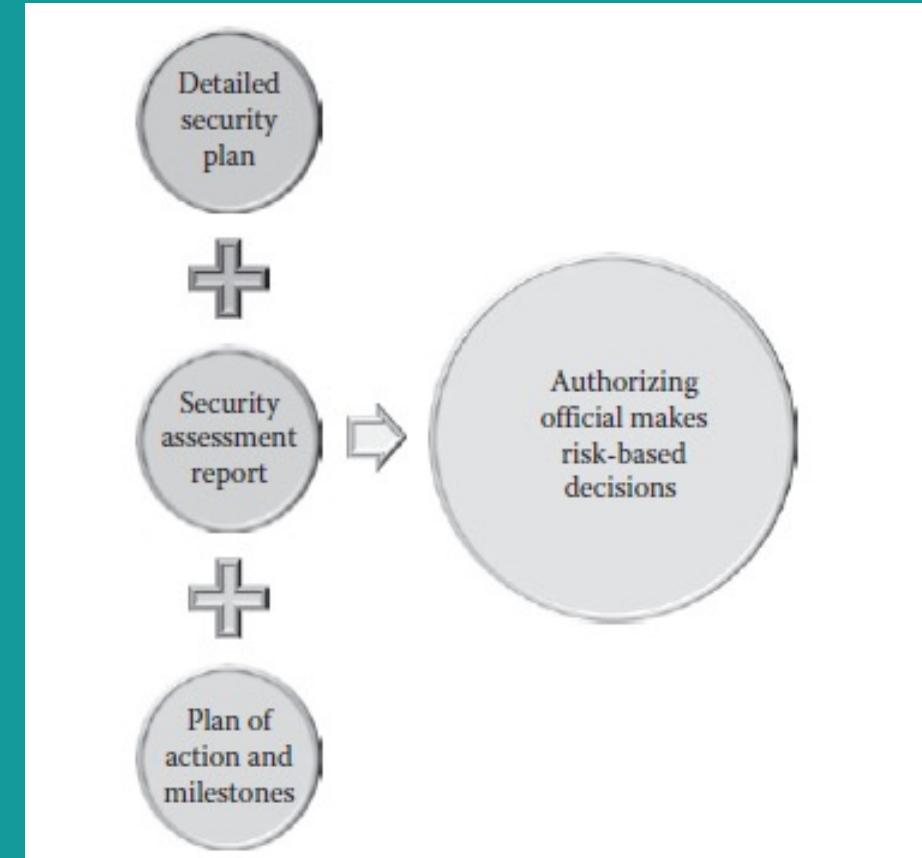


Section 7

Preparing the Security Authorization Package

Preparing the Security Authorization Package

- The final step before an information system is placed into day-to-day operation is the acceptance of risk by the authorizing official. This is called an authorization.
- The security authorization package contains: (1) a detailed security plan, (2) the security assessment report, and (3) the plan of action and milestones for addressing any identified weaknesses, or deficiencies.
- The organization ensures that the information needed for authorizing officials to make risk-based decisions about system correctness and functionality is always available.



Standard Risk Determination

→ In the end, every decision to authorize has to be made in light of the level of risk that is represented by a given state or condition of the system.

The general purpose of this step is to

- Review and/or update the individual plan of action and milestone elements to ensure everything has been included, analyzed, planned, and prioritized
- Perform the final review of the plan of action and milestone report itself



Standard Risk Determination

The objective of the documentation process is to:

- Assess the completeness of the information provided by the security assessment against organizational quality standards
- Improve the informational and educational feedback process to assist units across the organization in developing a more consistent and repeatable security assessment process
- Complete a review of a security assessment package for a particular information system or major application before it has been signed by the authorizing official
- Provide feedback to help refine the general authorization process
- Identify trends across units to help determine the root causes of deficiencies



Standard Risk Determination

To perform this task, the authorizing agent will:

- Use the officially sanctioned documentation to review the accreditation package
- Use the ATO letter to review the granting of the ATO
- Update the project accreditation, if this is a renewal



Authorization decision document

- The authorization decision
- The terms and conditions for the authorization
- The authorization termination date
- Whether the system is authorized to operate or not authorized to operate
- Any specific limitations or restrictions on the operation of the information system or inherited controls



Section Summary

- This Section describes the fundamental concepts associated with the authorization phase of the NIST RMF. The authorization documents the acceptance of a formally sanctioned, organization-wide, and systematic approach to the risk management needs of a given situation.
- The risk management is intended to leverage trust and confidence for any given system across the entire spectrum of the organizational culture. The risk management strategy is meant to underwrite an acceptable level of trust in the correctness of the organization's overall functioning



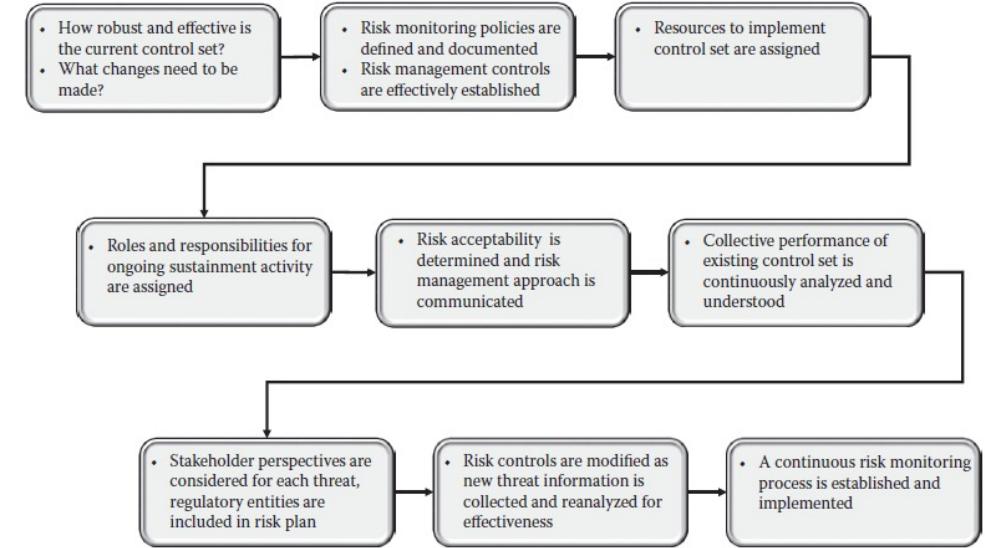


Section 8

Step 6—Monitor Security State

Sustaining the Organization's Risk Management Response

- The approval to operate documents an independent authorization decision on the part of an approval authority and is a form of contract between the approval authority and the stakeholders of the target system.
- **The authorization decision document contains the following information [National Institute of Standards and Technology (NIST), 2011]:**
 1. The authorization decision
 2. The terms and conditions for the authorization
 3. The authorization termination date
 4. Whether the system is or is not authorized to operate
 5. Any specific limitations or restrictions on the operation of the information system or inherited controls



Sustaining the Organization's Risk Management Response

- The initial system authorization is based on evidence that is gathered at the time of the initial controls assessment; however, as was stated previously, systems and environments change over time.
- The risk management process embodies the organization's commitment to identify and mitigate any relevant threats and vulnerabilities.
- Because it is a formal process, all of the operational steps of the risk management process have to be planned.



Sustaining the Organization's Risk Management Response

- Once the analysis operation is established, the formal responses in which the organization will utilize to mitigate all priority risks have to be maintained.
- The overall purpose of the risk-monitoring function is to establish and maintain a continuously appropriate set of risk controls.





Section 8

Sustaining Effective Risk Monitoring

Overview of the Process: Sustaining Effective Risk Monitoring

- Because there can be an infinite number of risks in the threat environment, the means for sustaining the risk management process over time has to be well-defined and yet flexible.
- The risk control set that is established through the NIST Risk Management Framework (RMF) process and authorized in the prior step is a formally executed organizational process, especially where certification is involved.
- Consequently, the control-monitoring process also needs to be properly resourced and specific roles and responsibilities for the ongoing sustainment activity have to be assigned.



Ongoing risk monitoring

- Because resourcing is always a factor, the maximum degree of acceptable risk must be made explicit with the organization.
- Risk acceptance decisions establish the link between the risk management approach of the organization and the contextual threat environment.



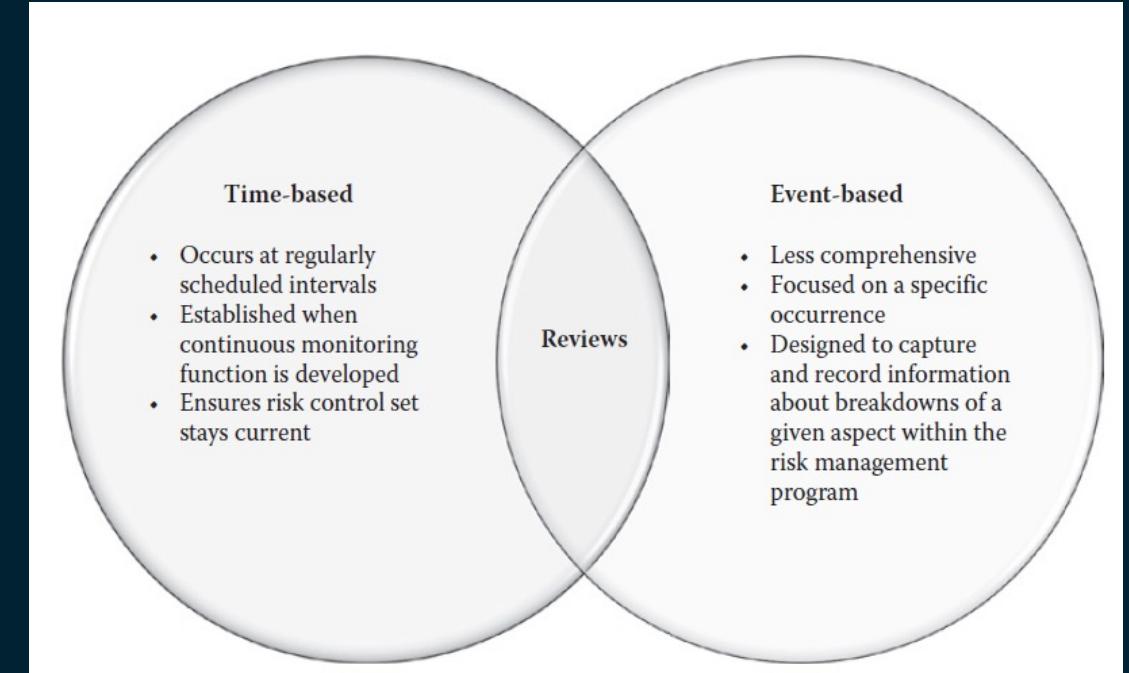


Section 8

Structuring the Risk-Monitoring Process

Structuring the Risk-Monitoring Process

- Information about control performance needs to be gathered throughout the life cycle of any risk management control set.
- A standard evaluation of the overall risk-monitoring process can generate useful lessons learned for improvement purposes.
- The risk-monitoring process assessment process is normally not continuous.
- Two types of reviews are commonly used to do this, a *time-based review* and an *event-based review*.



Structuring the Risk-Monitoring Process

- Two types of reviews are commonly used to do this, a *time-based review* and an *event-based review*.
- An *event-based* review is less comprehensive, but much more focused on a particular occurrence within the operational risk management process.
- The objective of both of these types of reviews is to ensure that the risk management control set stays aligned with its initial purposes.





Section 8

Sustaining an Ongoing Control-Monitoring Process

Sustaining an Ongoing Control-Monitoring Process

- The ongoing control-monitoring process implies the establishment of a fully planned and integrated set of activities.
- Control system assessments and the subsequent coordination of outcomes ensure efficient utilization of the organization's resources.
- The management stakeholders are also the people who are responsible for actually overseeing the day-to-day control-monitoring process and then making the appropriate decisions to maintain authorized compliance.



Sustaining an Ongoing Control-Monitoring Process

- The plan specifies the major assessment and response elements for the authorization period as well as itemizing the general set of resources that will be available to support the ongoing control performance assessment process.
- The ongoing control system assessment plan is the essential first condition for ensuring continued authorization of the system.
- Once the routine continuous assessment process is established, each of the component elements of that process are evaluated for correctness and then adjusted as necessary over time.





Section 8

Establishing a Continuous Control Assessment Process

Establishing a Continuous Control Assessment Process

- The control performance assessment process that underlies continuous monitoring is normally done by a designated assessment team.
- The first logical step in the process is to establish the scope of the general monitoring activity.
- A successful control assessment process usually monitors a diverse range of controls, ranging from electronic through human behavior and to physical security mechanisms.



Implementing a Practical Control System Monitoring Process

- Just as with any other large-scale organization, the control system monitoring process is established by a strategic planning effort.
- The overall goal of the strategic planning is to develop an effective and realistic way forward for the overall monitoring process.
- One challenge with the ongoing control performance assessment process is that it involves evaluating technology.





Section 8

Conducting Continuous Monitoring

Conducting Continuous Monitoring

- Once the scope of the assessment has been defined and all of the resources that are necessary to execute it have been put in place, the actual scheduling of the requisite activities and tasks takes place.
- The day-to-day continuous monitoring process is designed to understand and document the status of the control set that has been established by the NIST RMF process.
- Once all of the prep work is done, the individuals who have been assigned accountability for the execution of each task can now perform the actual work.



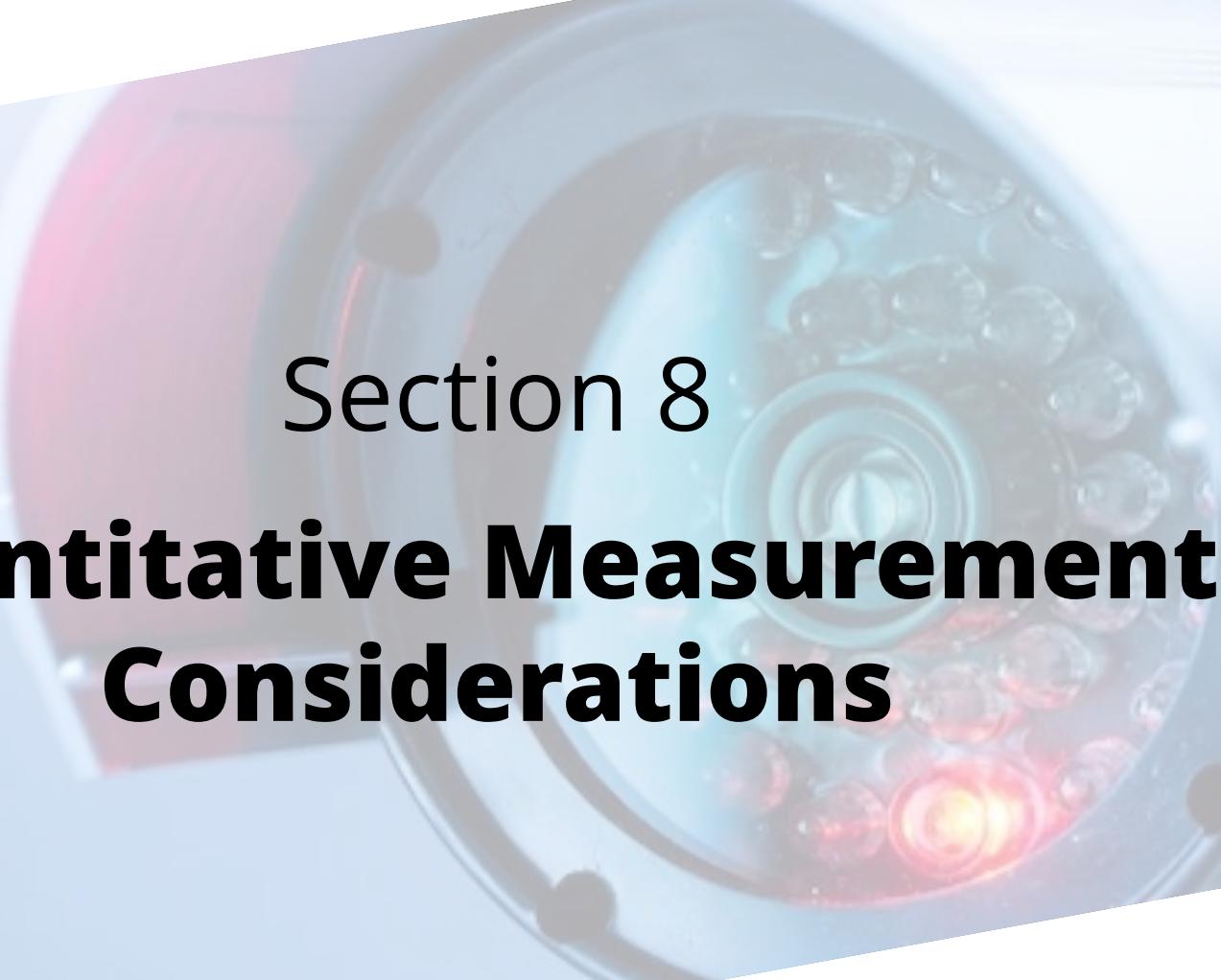
https://www.unsplash.com

© 2022 MartinY. All rights reserved.

Conducting Continuous Monitoring

- The day-to-day continuous monitoring process is designed to understand and document the status of the control set that has been established by the NIST RMF process.
- Quantitative measurement is an important element of the management of information technology work but it is particularly important when it comes to the management of IT risk.
- Specifically, standard quantitative measures are required to enable benchmarking.





Section 8

Quantitative Measurement Considerations

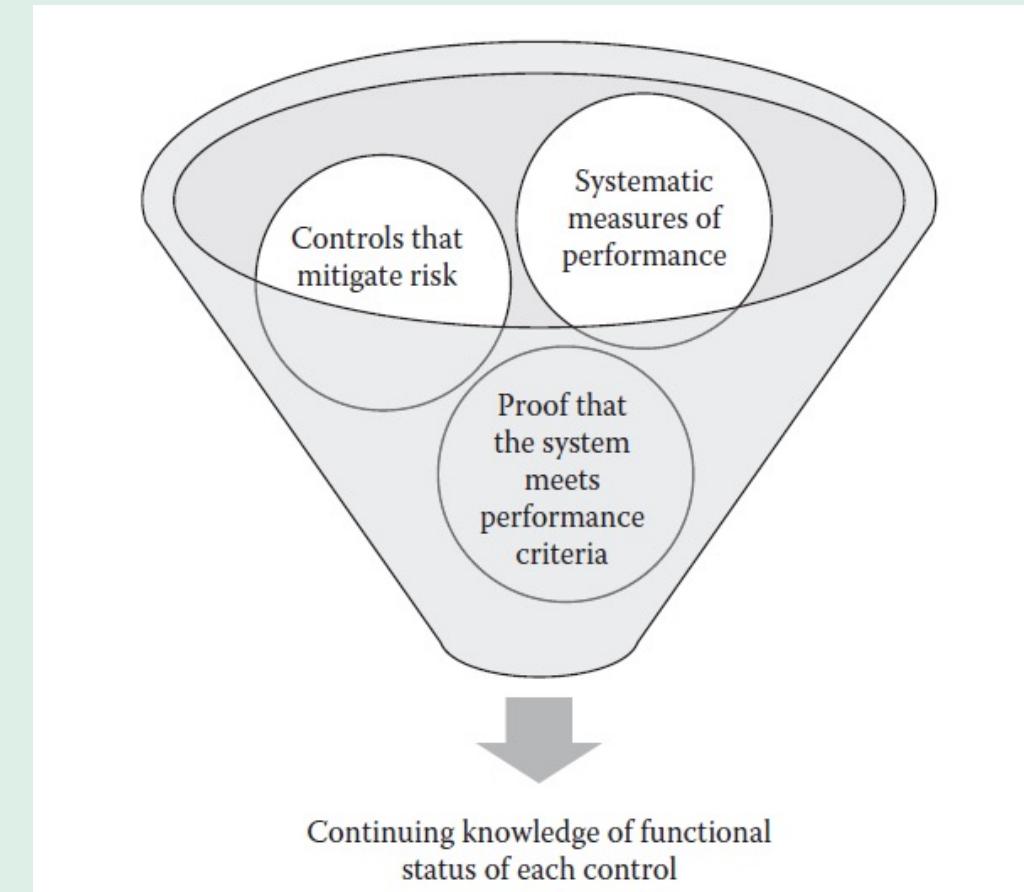
Practical Considerations

- Overall, the aim of the continuous control oversight process is to ensure that the compliance objectives necessary to maintain an approval to operate are successfully achieved and properly documented.
- Naturally, the sustainment of the correctness of the organization's formally established risk controls that have been put in place to provide the basis for the granting of an authorization to operate the system is a primary goal of the continuous monitoring process.



Quantitative Measurement Considerations

- The need to maintain a full, complete, and continuous understanding of the overall risk mitigation status of the organization's security controls is an essential part of good risk management practice
- The aim is to ensure that the day-to-day risk management operation satisfies all criteria for approved operation as well as documenting the fact that the system meets regulatory requirements



Foreseen and unforeseen decision-making

- The only difference between foreseen and unforeseen decision-making is whether there is already a policy or direction in place to guide subsequent actions. The actual policies and procedures to guide decision-making during the operational risk management sustainment phase are planned in advance and are meant to address situations that are known to happen.



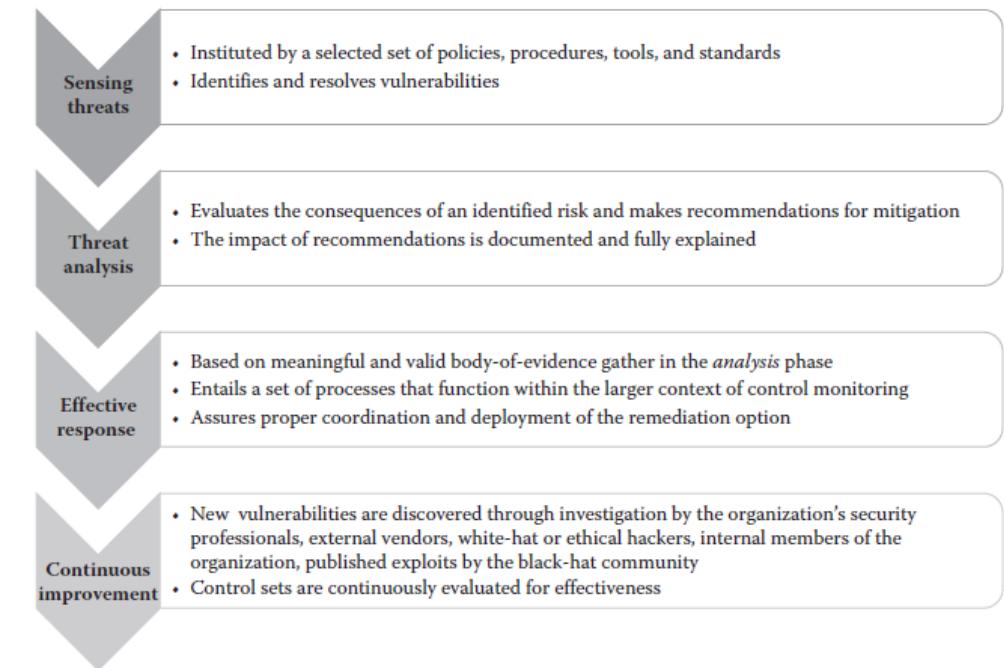


Section 8

Keeping the Control Set Correct over Time

Keeping the Control Set Correct over Time

- In essence, the NIST RMF model creates and recommends the implementation of a properly validated set of correct security controls.
- These controls are specifically aimed at addressing risk within a given organization. In this final stage of the NIST RMF framework, the aim is to ensure the effectiveness of the control set over time.
- Operational monitoring to **sense threats** is instituted by a selected set of policies, procedures, tools, and standards and are deployed to monitor, test, and review the control set or system.



Keeping the Control Set Correct over Time (Cont.)

- *Threat analysis*
- *Correct response*
- *Response management*

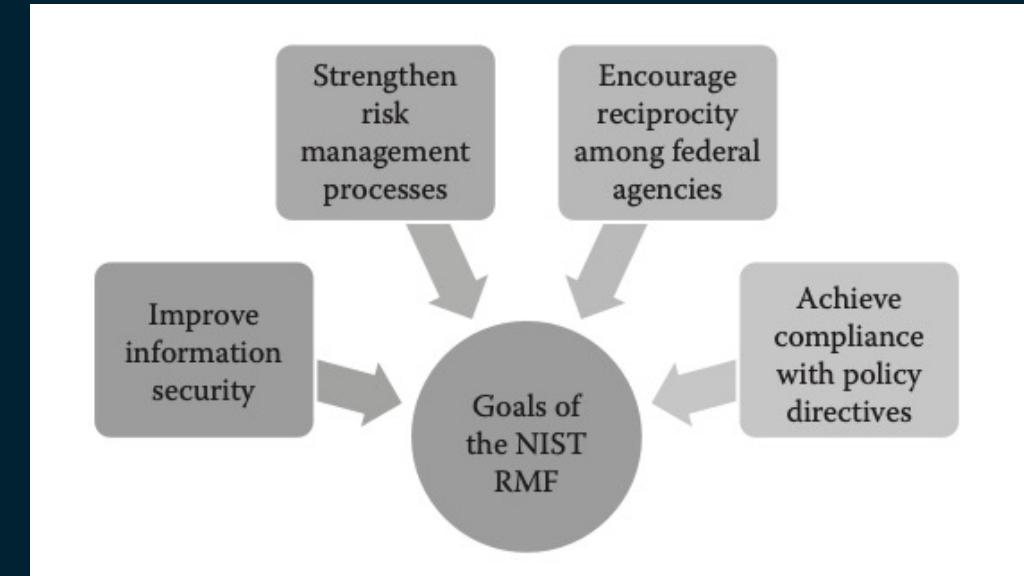


Section 9

Practical Applications of the NIST Risk Management Framework

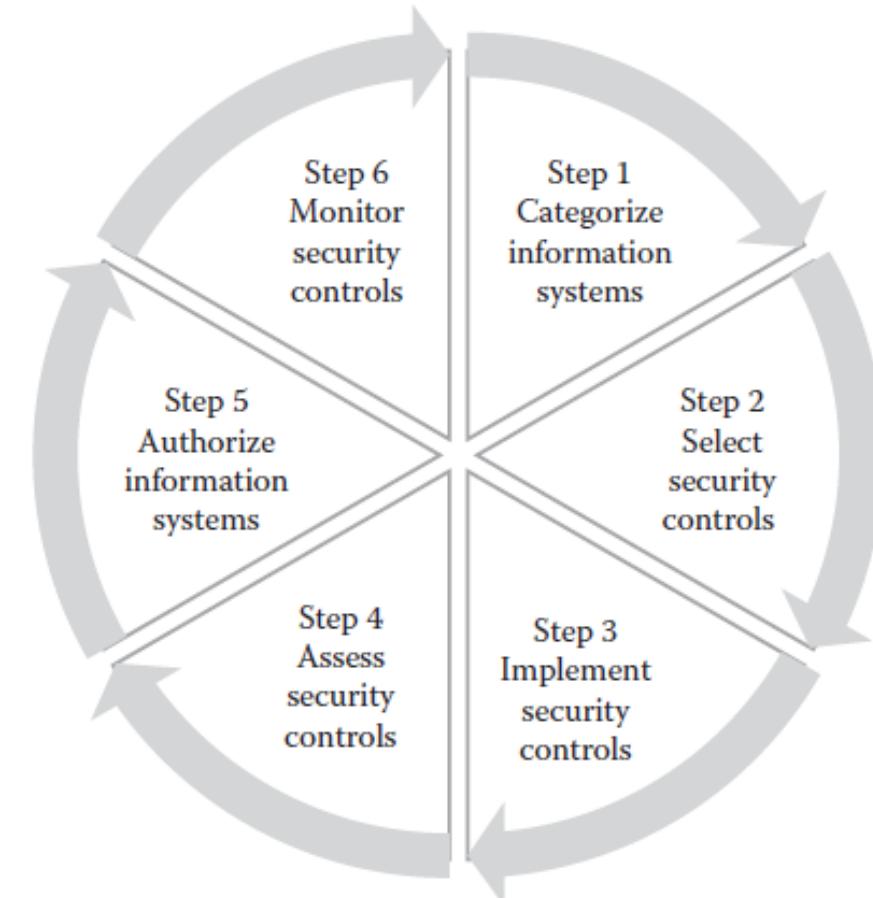
Applying the NIST RMF

- The NIST RMF was developed by the NIST as a specific way to ensure standard compliance with various federal information assurance certification programs.
- The specified goals of the NIST RMF
 - 1. To improve information security
 - 2. To strengthen risk management processes
 - 3. To encourage reciprocity among federal agencies
 - 4. Through implementation of the RMF, achieve compliance with policy directives.



RMF Application

- The DoD and other federal agencies require all information technology systems, including medical devices, to comply with a large number of well-defined information assurance requirements.
- It involves six life cycle stages
 1. Categorization of information systems (ISs)
 2. Selection of security controls
 3. Implementation of security controls
 4. Assessment of security controls
 5. Authorization of ISs
 6. Monitoring of security controls



Section 9

Certification and Accreditation in the Federal Space

Certification and Accreditation in the Federal Space

- Since it began in 1997, the formal C&A process for the ISs that operate within the federal government has been evolving through several incarnations.
- The government-wide effort to develop a new, universal, commonly understood, and accepted process for risk management produced the NIST RMF.
- Essentially, the NIST RMF is intended to be the fundamental methodology that will be used to establish and document the compliance of all federal systems with relevant regulatory requirements.



In the Beginning: The Clinger-Cohen Act (1996)

- There are a number of mandated accreditations required in the federal space. Most of these stem from the **Clinger-Cohen Act (CCA)**, enacted by Congress in February 1996 to reform and improve the way federal agencies acquired and managed their information technology assets.
- Most importantly, the CCA centralized the overall mandate for federal information technology management oversight with the Director of the OMB



Section 9

The E-Government Act

The E-Government Act of 2002: FISMA

- The central legislative piece in any discussion about the RMF is FISMA (2002). As we mentioned earlier, FISMA was enacted 6 years after the Clinger-Cohen Act as Title III of the E-Government Act of 2002 and it was FISMA that formally established the importance of cybersecurity as a national security priority for the United States.
- It is probably oversimplistic to call FISMA the Federal Cybersecurity Act, but in effect that is exactly what it is.
- FISMA assigns NIST the responsibility for developing standards, guidelines, and associated methods and techniques to guide that effort



The 17 areas

- A set of security controls establishes a level of “security due diligence” for the federal agency and its contractors

Security Control Class	Security Control Family	Identifier
1 Technical	Access control	AC
2 Operational	Awareness and training	AT
3 Technical	Audit and accountability	AU
4 Management	Certification, accreditation, and security assessments	CA
5 Operational	Configuration management	CM
6 Operational	Contingency planning	CP
7 Technical	Identification and authentication	IA
8 Operational	Incident response	IR
9 Operational	Maintenance	MA
10 Operational	Media protection	MP
11 Operational	Physical and environmental protection	PE
12 Management	Planning	PL
13 Operational	Personnel security	PS
14 Management	Risk assessment	RA
15 Management	System and services acquisition	SA
16 Technical	System and communications protection	SC
17 Operational	System and information integrity	SI

Section 9

Implementing Information Security Controls and Evaluating the Control Set



RMF

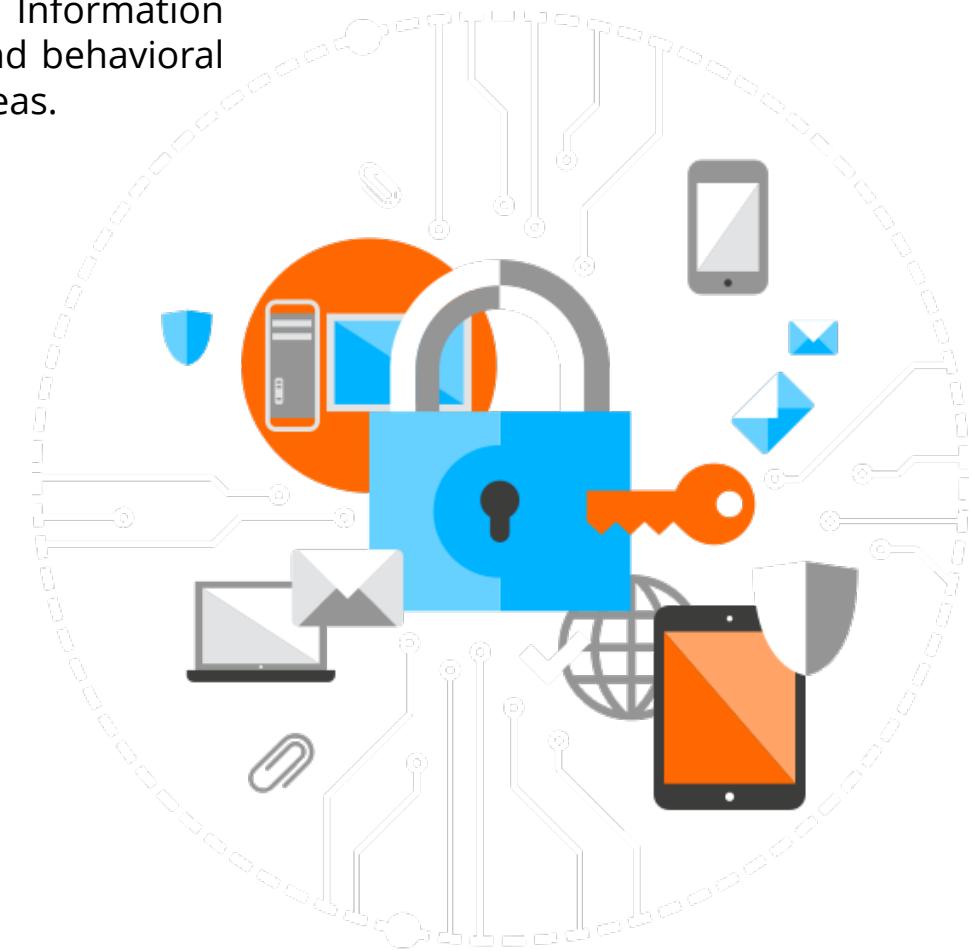
JUST

Implementing Information Security Controls—NIST 800-53

→ NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, is intended to supply the specific process and behavioral specifications for the controls that implement each of these 17 general areas.

→ NIST SP 800-53 subdivides security controls into

- Common
- Custom
- Hybrid



Evaluating the Control Set

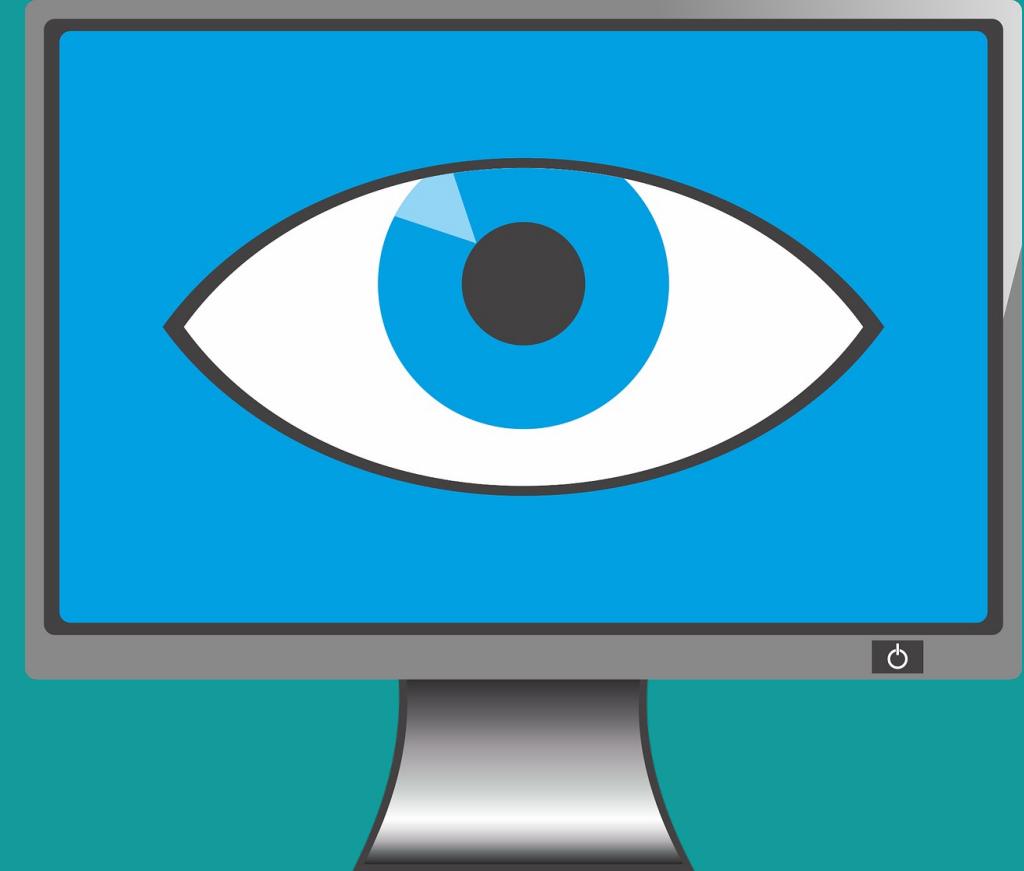
- It is one thing to specify controls and it is another to exemplify those controls in an effective practical process. As a result, NIST produced a companion work to NIST SP 800-53, called NIST SP 800-53A, ***Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans.***
- NIST SP 800-53A specifies a set of procedures that can be used to conduct a practical assessment of the specific security controls that have been implemented for a given IS



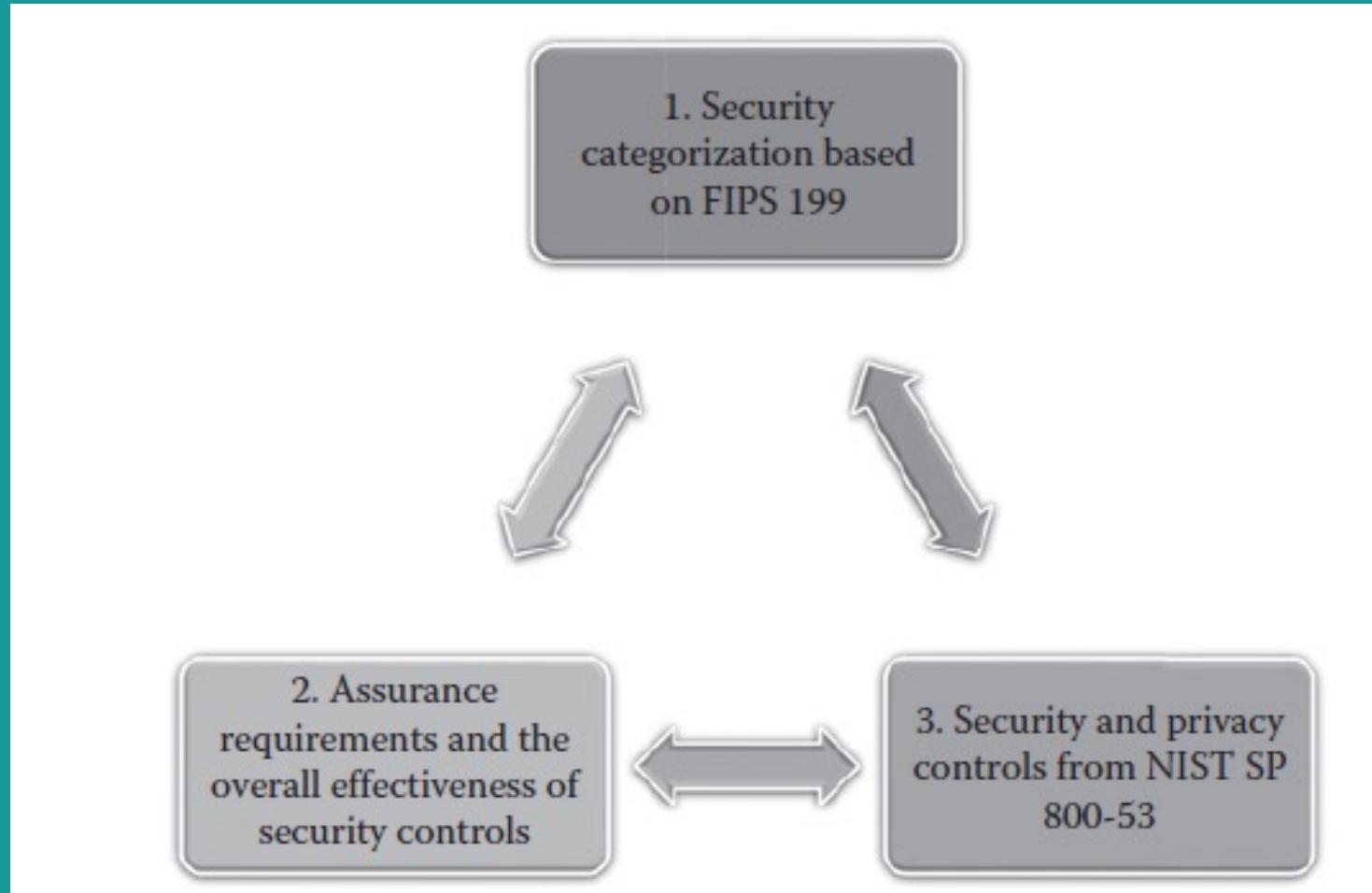
NIST SP 800- 53A (NIST, 2014) facilitate the assessment of security and privacy controls

→ The intention is to provide decision-makers with the following:

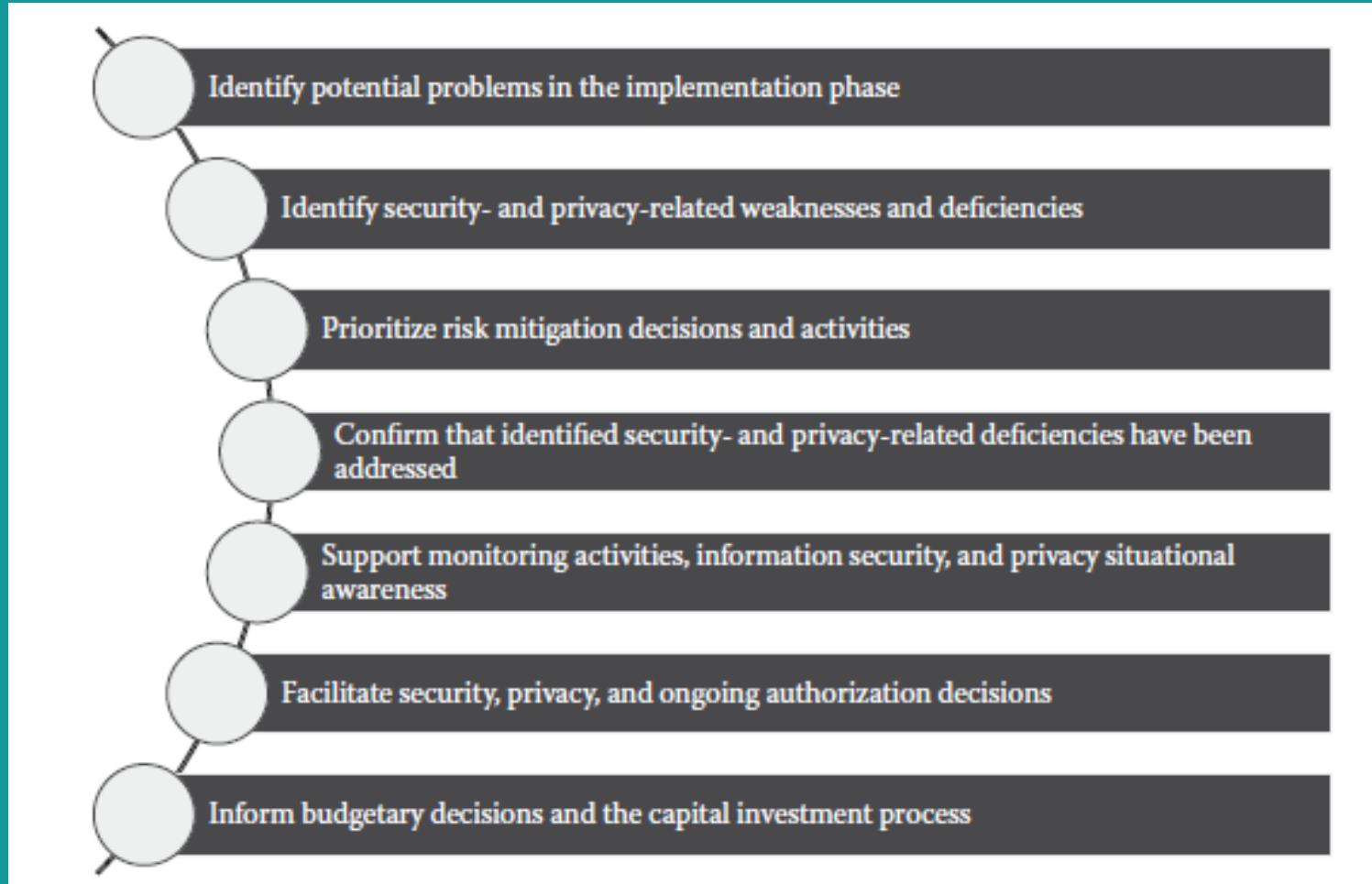
1. Evidence about the effectiveness of implemented controls
2. An indication of the quality of the risk management processes employed within the organization
3. Information about the strengths and weaknesses of the IS, which are supporting organizational missions and business functions in a global environment of sophisticated and changing threats



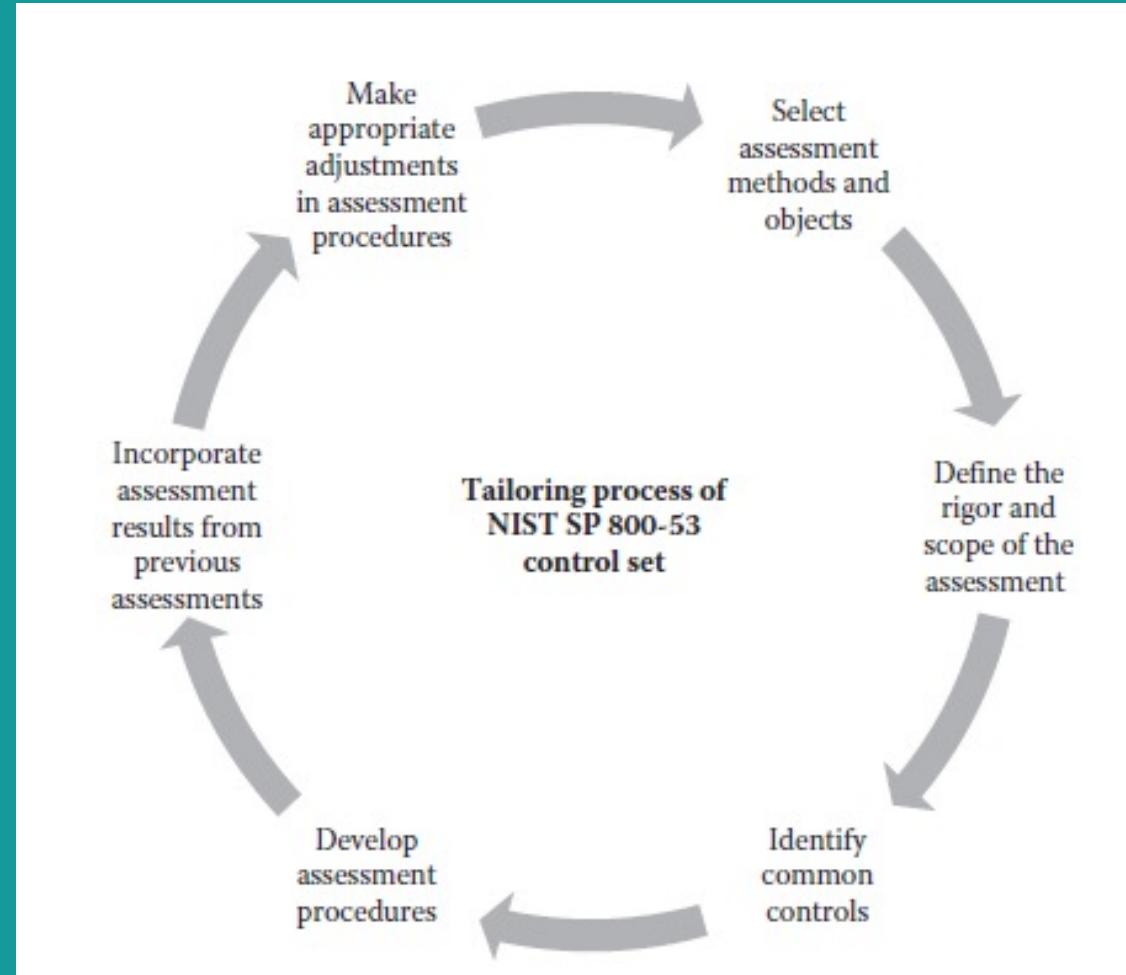
Three common factors in effective assessment and examination



Control assessment information.



Tailoring process of the NIST SP 800-53 control set.



Section Summary

- The DoD and other federal agencies require all information technology systems, including medical devices, to comply with a large number of well-defined information assurance requirements. Thus, in effect, the RMF specifies a standardized process for performing the traditional C&A functions.

