CENTERS for MEDICARE & MEDICAID SERVICES
Enterprise Information Security Group
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Enterprise Information
Security Group

Risk Management, Oversight,
And Monitoring

Risk Management Handbook
Volume I
Chapter 1

Risk Management in the XLC

Final
Version 1.0
November 8, 2012

Document Number: CMS-CISO-2012-vI-ch1

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN CMS-CISO-2012-VI-CH1, *RISK MANAGEMENT IN THE XLC,* VERSION 1.0, DATED NOVEMBER 8, 2012

1. Baseline Version.

(This Page Intentionally Blank)

TABLE OF CONTENTS

1 INTRODUCTION....................1
1.1 Handbook Vocabulary.................... 3
1.2 CMS FISMA Control Tracking System (CFACTS).................... 5
2 RISK MANAGEMENT....................6
2.1 Risk Terminology.................... 6
2.2 Risk Context.................... 8
2.3 Risk Hierarchy.................... 9
3 RISK MANAGEMENT IS PART OF THE XLC....................11
4 THE XLC AS PART OF RISK MANAGEMENT....................15
4.1 Minimum Security Requirements.................... 16
4.2 Software Assurance: Build Security In.................... 17
5 NIST RMF STEPS....................18
5.1 Categorize Information System.................... 18
5.1.1 Security Categorization.................... 20
5.1.2 Information System Description.................... 21
5.1.3 Information System Registration.................... 24
5.2 Select Security Controls.................... 25
5.2.1 Common Control Identification.................... 27
5.2.2 Security Control Selection.................... 28
5.2.3 Monitoring Strategy.................... 28
5.2.4 Security Plan Approval.................... 29
5.3 Implement Security Controls.................... 29
5.3.1 Security Control Implementation.................... 32
5.3.2 Security Control Documentation.................... 32
5.4 Assess Security Controls.................... 32
5.4.1 Assessment Preparation.................... 35
5.4.2 Security Control Assessment.................... 35
5.4.3 Security Assessment Report.................... 36
5.4.4 Remediation Actions.................... 36
5.5 Authorize Information System.................... 37
5.5.1 Plan of Action and Milestones.................... 39
5.5.2 Security Authorization Package.................... 39
5.5.3 Risk Determination.................... 40
5.5.4 Risk Acceptance.................... 40

5.6 Monitor Security Controls 41
5.6.1 Information System and Environment Changes 43
5.6.2 Ongoing Security Control Assessments 43
5.6.3 Ongoing Remediation Actions 44
5.6.4 Key Updates 44
5.6.5 Security Status Reporting 45
5.6.6 Ongoing Risk Determination and Acceptance 45
5.6.7 Information System Removal and Decommissioning 46

6 PROCUREMENT 46

7 GOVERNANCE AND REVIEWS 48

7.1 Architecture Review 51

7.2 Investment Selection Review 51

7.3 Project Baseline Review 52

7.4 Requirements Analysis Review 54

7.5 Preliminary Design Review 54

7.6 Detailed Design Review 55

7.7 Environmental Readiness Reviews 56
7.7.1 Validation Readiness Review 56
7.7.2 Implementation Readiness Review 56
7.7.3 Production Readiness Review 57

7.8 Operational Readiness Review 57

7.9 Post Implementation Review 57

7.10 Annual Operational Analysis Review 58

7.11 Disposition Review 59

8 CROSSWALK BY XLC PHASES 59

8.1 Initiation, Concept, and Planning Phase 60
8.1.1 Initiation Segment 60
8.1.2 Concept Segment 60
8.1.3 Planning Segment 61

8.2 Requirements Analysis and Design Phase 62
8.2.1 Requirements Analysis Segment 62
8.2.2 Design Segment 63

8.3 Development and Test Phase 63
8.3.1 Development Segment 63
8.3.2 Test Segment 64

8.4 Implementation Phase 64

8.5 Operations & Maintenance Phase 65

9 GLOSSARY AND ACRONYMS 66

10 APPROVED 66

LIST OF TABLES

Table 1 Risk Definitions 7
Table 2 NIST RMF Steps and Tasks with associated XLC Phases 12
Table 3 Content of an Information System Description 21
Table 4 Implement Security Controls Step by XLC Phase Segment 30
Table 5 Security Gates 48
Table 6 XLC Phases and Associated NIST RMF Steps and Tasks 59

LIST OF FIGURES

Figure 1 The Risk Management Framework 2
Figure 2 Risk Management Hierarchy 10
Figure 3 NIST RMF Tasks within the XLC 14
Figure 4 Categorize Information System 19
Figure 5 Select Security Controls 26
Figure 6 Implement Security Controls 31
Figure 7 Assess Security Controls 34
Figure 8 Authorize Information System 38
Figure 9 Monitor Security Controls 42
Figure 10 Risk Management Security Gates 50

(This Page Intentionally Blank)

1 INTRODUCTION

The *Federal Information Security Management Act of 2002* (FISMA) was enacted as Title III of the *E-Government Act (Public Law 107-347) in December 2002*[1]. FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

FISMA reaffirmed the National Institute of Standards and Technology's (NIST) role in developing information security standards (Federal Information Processing Standards) and guidelines (Special Publications in the 800-series) for non-national security federal information systems and assigned NIST some specific responsibilities, including the development of:

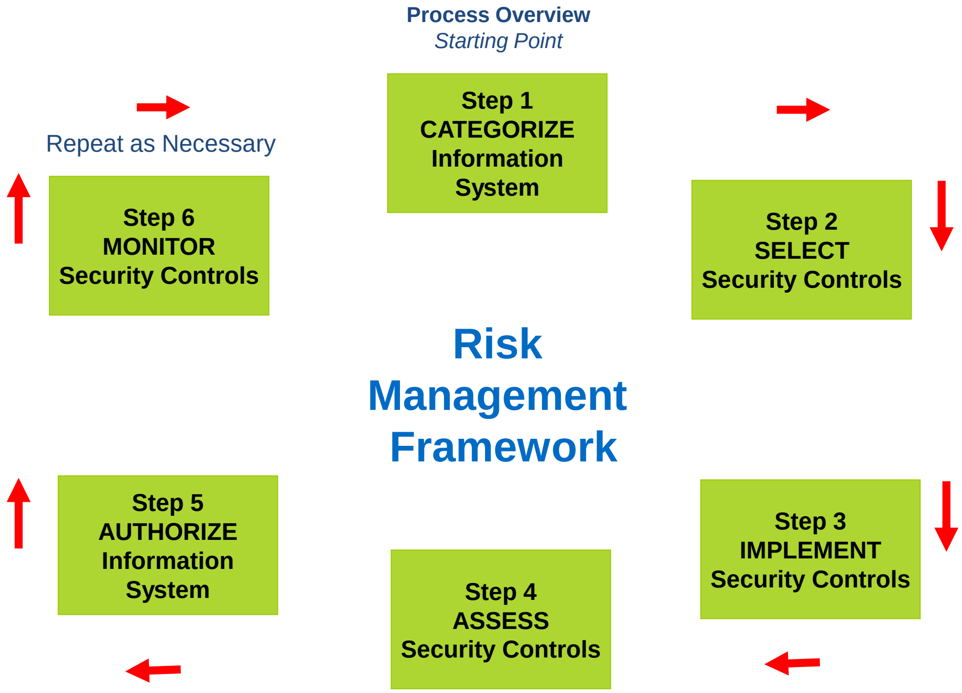
- Standards to be used by Federal agencies to categorize information and information systems based on the objective of providing appropriate levels of information security according to a range of risk levels.
- Guidelines recommending the types of information and information systems to be included in each category.
- Minimum information security requirements (management, operational, and technical security controls) for information and information systems in each category.

In February 2010, NIST published Special Publication (SP) 800-37 Revision 1; *Guide for Applying the Risk Management Framework to Federal Information Systems* subtitled *A Security Life Cycle Approach*[2] and hereafter referred to as "SP 800-37 R1." NIST views SP 800-37 R1 as part of a fundamental and transformational change in the approach to information security within the federal government. Specifically, security emphasis is shifting from a "proving compliance only" orientation to one where agency attention and effort focuses on the conduct of stated missions with appropriate security implementation (or security commensurate with risk). To facilitate this change in approach, NIST developed the Risk Management Framework, hereafter referred to as the "NIST RMF." Figure 1 shows the steps of the NIST RMF.

[1] Public Law 107-347, *E-Government Act (Public Law 107-347) in December 2002*, is available at http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf.

[2] SP 800-37 R1, *Guide for Applying the Risk Management Framework to Federal Information Systems* subtitled *A Security Life Cycle Approach*, is available at http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

Figure 1 The Risk Management Framework[3]



NIST states that the NIST RMF has the following characteristics:

- Promotes the concept of **near real-time** risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes.
- Encourages the use of automation to provide senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational information systems supporting their core missions and business functions.
- **Integrates information security into the enterprise architecture and system development life cycle**, which at Centers for Medicare and Medicaid Services (CMS) is the *eXpedited Life Cycle (XLC)*[4].
- Emphasizes the selection, implementation, assessment, and monitoring of security controls, and the authorization of information systems.
- Links risk management processes at the information system level to risk management processes at the organization level through a risk executive (function).
- Establishes responsibility and accountability for security controls deployed within organizational information systems and inherited by those systems (i.e., common controls[5]).

[3] Figure adapted from NIST SP 800-37 R1, G*uide for Applying the Risk Management Framework to Federal Information Systems* subtitled *A Security Life Cycle Approach*, Figure 2-2 (p. 8).
[4] Information regarding the eXpedited Life Cycle (XLC) is available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/index.html.
[5] *Common Control* definition is in Section 1.1.

The *CMS Risk Management Handbook (RMH)* comprises three volumes. The first Volume is the reference source. It provides a detailed overview, guidance, background, and tasks for all parts of the NIST RMF. References to **Chapters** throughout the RMH indicate the related chapter of Volume I. Volume II of the RMH contains the procedures for risk management. This includes procedures for the *CMS FISMA Controls Tracking System (CFACTS)*. References to **Procedures** throughout the RMH indicate the related chapter of Volume II. Volume III of the RMH contains current CMS standards, requirements, directives, and practices. References to **Standards** throughout the RMH refer to the related chapter of Volume III.

1.1 HANDBOOK VOCABULARY

Words have different meanings, or shades of meaning, to individual readers or in varying contexts. There are many terms used throughout the material presented by the RMH that have specific meanings or intents. This section presents terms used frequently within the RMH to establish common understanding. When appropriate, definitions of localized terms within the RMH accompany the discussion of the specific subject.

All CMS information security terms, definitions, and acronyms are available in the RMH Volume I, Chapter 10, *CMS Risk Management Terms, Definitions, and Acronyms*, which is available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

Information System[6] means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

> Throughout the RMH, the unqualified use of the term "system" is synonymous with information system. Please note: system includes any form of information system (e.g., three-tier, mainframe, cloud-based services, General Support System[GSS], Major Application, and minor application) as the NIST RMF makes no distinction.

Two other terms relate to the definition of an information system. These are:

Information Resources[7] means information and related resources, such as personnel, equipment, funds, and information technology.

Information Technology[8] with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract

[6] 44 USC §3502. Note: Per FISMA (44 USC §3502 (a)), *"In General.--Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter"* (http://www.gpoaccess.gov/uscode/browse.html).
[7] 44 USC §3502. Note: Per FISMA (44 USC §3542 (a)), *"In General.--Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter"* (http://www.gpoaccess.gov/uscode/browse.html).
[8] 40 USC §11101. Note: Per FISMA (44 USC §3502 (b) (3)), *"The term 'information technology' has the meaning given that term in section 11101 of title 40"* (http://www.gpoaccess.gov/uscode/browse.html).

with the executive agency that requires the use of that equipment; or of that equipment to a significant extent in the performance of a service or the furnishing of a product.

- Information technology includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.
- Information technology does not include any equipment acquired by a federal contractor incidental to a federal contract.

Significant Change[9] means a change that is likely to affect the security state of an information system.[10]

IT Project[11] means a temporary planned endeavor funded by an approved information technology investment; thus achieving a specific goal and creating a unique product, service, or result. A project has a defined start and end with specific objectives that signify completion, when attained.

> Throughout the RMH, unqualified use of the term project is synonymous with IT project. A project comprises the activities performed to create a new system (or components thereof) or modify an existing system (or its components).

Security implementations consist of requirements and controls.

Security Requirements[12] means requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

Security Controls[13] means the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Within the RMH, security requirements denote specific protections necessary for information and information systems. Requirements are specified in the *CMS Minimum Security*

[9] NIST SP 800-37 R1 p. F-7.

[10] Examples of significant changes to an information system may include, but are not limited to: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform; (iv) modifications to cryptographic modules or services; or (v) modifications to security controls. Examples of significant changes to the environment of operation may include, but are not limited to: (i) moving to a new facility; (ii) adding new core missions or business functions; (iii) acquiring specific and credible threat information that the organization is a target of a threat source; or (iv) establishing new/modified laws, directives, policies, or regulations.

[11] U.S. Department of Health and Human Services *Glossary of Key Enterprise Terms*, located at http://www.hhs.gov/ocio/about/terms/index.html#ITPROJ.

[12] FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006, available at http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

[13] FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, available at http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

Requirements (CMSR)[14] in appendices A, B, and C of the *CMS Acceptable Risk Safeguards (ARS)*[15].

The RMH uses security controls to denote the mechanisms employed to implement each required protection. Control implementations consist of automated processes, manual procedures, or a combination of both. Regardless of implementation, controls fall into one of three types based on the scope of the control and the control's ability to meet the full intent of the requirement. NIST SP 800-37 R1 defines these types of controls and related vocabulary.

Common Control means a security control inherited by one or more organizational information systems.

System-Specific Security Control means a security control that is not designated as a common security control or the portion of a hybrid control that is to be implemented within an information system.

> The RMH uses *system-specific control* and *system-specific portion of a hybrid control* to refer to particular instances of a *system-specific security control*.

Hybrid Security Control means a security control that is implemented in an information system as part common control and part system-specific control.

> The RMH term *hybrid control* is synonymous.

Common Control Provider means an organizational entity responsible for the planning, development, implementation, assessment, authorization, and maintenance of some common controls (i.e., security controls inherited by other information systems.) There can be many Common Control Providers.

1.2 CMS FISMA CONTROL TRACKING SYSTEM (CFACTS)

CFACTS[16] is the data repository in use by CMS to store, manage, and report information relating to the risk and security status of all CMS systems to support FISMA requirements. CFACTS serves as the single data entry point for data relating to the information security status of CMS systems. From this single repository of data, CFACTS satisfies multiple reporting requirements. Thus, each business owner, Common Control Provider, system developer/maintainer, and Information System Security Officer (ISSO) can focus more time on the system and its controls, instead of cutting-and-pasting from document to document.

A significant feature of CFACTS is the ability to build information for required security artifacts incrementally, concurrent to the development of information. At the beginning of a new project, there is little detail about the final system, but there is a high-level overview of the system's

[14] The *CMS Minimum Security Requirements (CMSR)* is documented in appendices A through C, of the *CMS Acceptable Risk Safeguards (ARS)* and is available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

[15] The *CMS Acceptable Risk Safeguards (ARS) is* located at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

[16] CFACTS is accessible on CMSnet at https://cfacts.cms.cmsnet. (CFACTS is not available through the Internet.)

objectives and attributes. The high-level view can be input to CFACTS during the earliest phase of the project. Because CFACTS contains all ARS requirements and the current security status of all systems, CFACTS can help the project team determine required and possibly inheritable security controls.

More details can be input into CFACTS supplementing high-level information, as they become available during the project. This helps ensure consistency with basic objectives and fundamental requirements and provides a method to track the status of security requirements and controls throughout the XLC.

RMH Volume II contains all procedures, including those for CFACTS.

2 RISK MANAGEMENT

Risk and its management are broad, multifaceted subjects. Risk is context dependent (relative) and can vary over time. Risks exist at all levels of the organization and can have long-range and short-range implications. There are many types of risk. A few examples are:

- Economic and financial risks can be measured quantitatively (in dollars) and relate to the ongoing viability of the organization as measured by its balance sheet.
- Safety risks use qualitative scales (e.g., Low-Medium-High, Green-Yellow-Red) and relate to the injury that can happen to people.
- Mission/business process risks can have many measurement scales and relate to the success of a specific mission or business process and its operations. These could be quantitative or qualitative.
- Information system security risks usually use a qualitative measurement scale, typically High, Medium, Low, or occasionally Non-existent. These risks relate to the confidentiality, integrity, and availability of the information and the information system.

Risks of one type can also represent risks of other types. For example, a lack of data integrity (information system security risk) in a hospital’s recovery room patient monitoring system could cause injury to the patient (safety risk), send staff to the wrong patient (mission/business process risk), and subject the hospital to a lawsuit (financial risk).

2.1 RISK TERMINOLOGY

As with any specialized area, the subject of risk has its own vocabulary. Many different definitions of risk related terms are context dependent. Understanding risk vocabulary facilitates a better understanding of risks, the impacts on CMS business and missions, and possible strategies to address those risks.

NIST SP 800-39, *Managing Information System Risk: Organization, Mission, and Information System View*[17], defines key terms related to risk and risk management. Table 1 contains this document's definitions of some common risk terms.

Table 1 Risk Definitions

Term	Definition
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Information System-Related Security Risks	Those risks that arise through the loss of confidentiality, integrity, or availability of information or information systems and consider impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the Nation.
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.
Risk Executive (function)	An individual or group within an organization that helps to ensure that: (i) security risk-related considerations for individual information systems, to include the authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and (ii) managing risk from individual information systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success.
Risk Management	The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.
Risk Mitigation	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/ countermeasures recommended from the risk management process.
Risk Monitoring	Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions.
Risk Response	Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.
Risk Response Measure	A specific action taken to respond to an identified risk.

[17] NIST SP 800-39, *Managing Information System Risk: Organization, Mission, and Information System View* is available at http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

2.2 RISK CONTEXT

As previously mentioned, risk is context dependent (relative) and can vary over time. For example, a physical structure will decay over time if not maintained. Eventually the structure will crumble and fall, a direct outcome of lack of maintenance. What risk is associated with this event? This depends on the context of the physical structure. The risk associated with the inevitable decay relates to and varies with the context of those affected by the collapse of the structure. For example:

- **If the structure is an old house**, which is long abandoned, empty, and in a remote area there may be little or no risk of any kind. At worst, the landowner might have to clean up the mess after the building crumbles.
- **If the structure is a segment of an oil pipeline across uninhabited desert**, economic impact will result to oil companies. The magnitude of the economic risk is still context dependent. For a large oil company the economic impact would potentially be low, due to its size and access to multiple sources of supply. However, the failure might be a medium economic risk for most medium sized oil companies and a high economic risk for a small one.
- **If the structure is a bridge on a heavily traveled highway**, which decays through lack of maintenance, people may lose their lives when it collapses. Putting this in context, this is a high safety risk to people crossing the bridge. To the government entity responsible for maintaining the bridge it is a high political risk, an economic risk whose severity may be dependent upon the resources of the government entity, and a high legal risk. Depending on the laws of the jurisdiction, the legal risk might have civil and criminal aspects. The contracting company that originally built the bridge may have no risk, if there were no defects in construction and the company was not responsible for maintenance.

Risk management strives to minimize or constrain risks to acceptable levels. Different solutions and mitigation techniques are appropriate in different contexts. Some appropriate techniques from the prior example of the decaying physical structure that has not yet collapsed could be:

- The landowner of the property on which the old house resides could decide to either dismantle the house or take no action. These risk response measures are examples of an avoidance risk response and an acceptance risk response, respectively.
- The oil company may decide to place cut-off valves in the pipeline to limit spillage and facilitate replacement of pipe sections, increase the frequency of monitoring and inspections, or purchase extra insurance to reduce the economic burden to rebuild a pipeline segment that breaks. These risk response measures are examples of a mitigation risk response, a mitigation risk response achieved through heightened monitoring, and a transfer risk response that transfers the risk (cost of repairing the pipeline) to another entity, respectively. Please note: The oil company may also decide to do several of these.
- The case of the bridge on a heavily traveled highway is more complicated. There is no reasonable expectation that people driving over the bridge on the highway are aware of its disrepair, so they will not perceive the risk until the bridge collapses. However, the government entity that is responsible for maintaining the bridge has no reason to be unaware of the bridge’s condition. It must act to manage the risk. The government entity might

decide to close the bridge permanently. Alternatively, it might decide to detour traffic to an alternate route or limit traffic significantly while performing maintenance or building a new bridge. The risk response measure of closing the bridge permanently is an example of an avoidance risk response, while the other measures are examples of a mitigation risk response.

At CMS, as in all organizations, the appropriate officials must be informed of and address all risks to the systems that fall within their purview.

- Business Owners and Common Control Providers must know the information security/ assurance risks, as they are in a position to budget for and take action to minimize and constrain those risks for their information, systems, and controls, as required by FISMA.
- Because risk has many contexts, the CMS Chief Information Officer (CIO) and CMS Chief Information Security Officer (CISO) must know the information security/assurance risks of all systems to ensure adequate protection for the CMS enterprise and all of its information and information systems.

2.3 RISK HIERARCHY

The NIST RMF[18] links risk management processes at the information system level to risk management processes at the mission/business process and organizational (enterprise) level. This linkage promotes a more enterprise-centric view of risk. This facilitates understanding of the risk from the organizational context and enables more realistic gauging of its magnitude.

In the traditional approach, risk evaluations were measured on a system-centric basis (i.e., *"What is the risk to the given system?"*). This (former) view can lead to:

- System-level risk-acceptance without due diligence in the evaluation of the enterprise risk (i.e., *"What's the risk to the enterprise?"*) that may be introduced if a system-level risk is tolerated.
- System-level risks designated higher than they actually are to the enterprise.

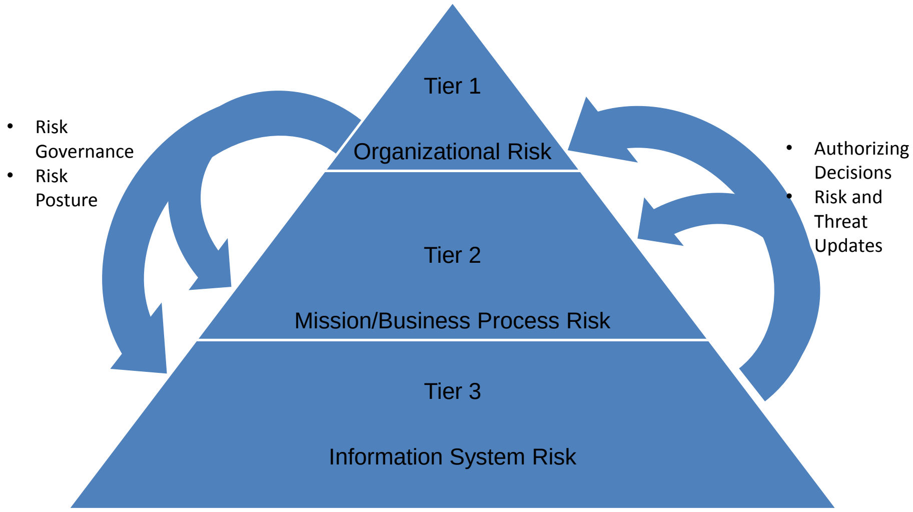
Clearly, neither of these possibilities is desirable. The first leaves the organization exposed when an un-mitigated system risk has significant impact in the context of the enterprise. The second can divert organizational resources (e.g., time, personnel, and funding) away from significant organizational risk issues to address risks of lesser impact to the enterprise.

The NIST SP 800-39, *Managing Information System Risk: Organization, Mission, and Information System View*[19], addresses risk management in three risk tiers: 1) organizational, 2) mission/business process, and 3) information system. Figure 2 illustrates the three tiers of the risk management hierarchy.

[18] NIST SP 800-37 R1 - http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

[19] NIST SP 800-39, *Managing Information System Risk: Organization, Mission, and Information System View*, is available at http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

Figure 2 Risk Management Hierarchy



Tier 1 addresses enterprise-wide aspects of risk management including the development of a comprehensive governance structure and an enterprise-wide risk management strategy. Tier 2 addresses mission and business process aspects of risk management using the risk decisions made at the Tier 1 level as guidance. Tier 3 addresses information system aspects of risk management including the selection of safeguards and deployment of controls (common, hybrid, and system-specific) for and within the system, guided by Tiers 1 and 2.

These tiers interoperate seamlessly. Organization-wide risk posture includes awareness, tolerances, and risk governance (e.g., traceability and transparency of risk decisions) all flowing downward from Tier 1 to Tiers 2 and 3. Conversely, situational awareness and feedback for improvement flow upward from Tier 3 to Tier 2 and Tier 1. Effective Inter-Tier and Intra-Tier communications are essential.

Risks determined in one system may affect the risk exposure of its related mission/business processes and the CMS enterprise. **Please note: vulnerabilities uncovered in one system can pose threats to other systems.** For example, SQL injection vulnerabilities may expose multiple databases to malicious attacks, whether or not those databases belong to the system containing the vulnerability.

Understanding where risks fall within the risk management hierarchy is essential for effective employment of the three-tiered risk approach. Many risks are not at the information system tier. For example, Project Risk, a type of risk that occurs at the mission/business process tier, is a component of project management. Project risk deals with events that can happen that affect the project cost, resources, schedule, process, and success. Whether the project is building a bridge or creating (modifying) an information system, project risk is part of the project management process. At CMS, project risk management processes, procedures, and artifacts for information systems projects are part of the XLC[20].

The NIST RMF addresses information system risk. NIST SP 800-39 is concerned with the process of managing risk within the enterprise based on the three-tiered risk approach. The RMH combines these subjects to provide an enterprise wide risk management structure that addresses information system-related security risk.

3 RISK MANAGEMENT IS PART OF THE XLC

A key component of effective risk management is integration with the CMS XLC. The NIST RMF consists of six steps, each containing several tasks. Each task has distinct objectives and activities. The structure and order of tasks builds upon the results of prior tasks. Performing NIST RMF tasks at the appropriate time as part of the designated XLC phase(s) assists project planning, security control selection and implementation, and cost control.

Note: the XLC is artifact-focused. This means the existence of certain artifacts (documents) implies completion of underlying XLC processes and activities. The XLC is a flexible methodology, allowing projects to customize the deliverables schedule based on the complexity of the project. There is no need to create unnecessary deliverables and some deliverables may be consolidated into fewer documents. **However, Federal law mandates Information Security and Privacy processes, artifacts, reviews, and tests to ensure the implementation and effectiveness of controls that meet mandated requirements.** Furthermore, security requirements in the current *CMS Acceptable Risk Safeguards* cannot be waived or ignored. Therefore, the Project Process Agreement (PPA) and contracts must contain them.

Conversely, the NIST RMF is task-based and all tasks are required. The NIST RMF focuses on risk management steps by defining specific tasks to perform and the sequence of those tasks. Together, the XLC and NIST RMF provide a method that projects use to meet business goals at acceptable risk levels.

Prior to publication of SP 800-37 R1, many security implementations were after-the-fact components, added to systems to make them compliant with law and regulations. In effect, developing the system’s business functionality was often divorced from implementing security requirements. This resulted in dedicating substantial efforts and resources to prove compliance, but not necessarily addressing the main purpose of containing risk to an acceptable level. When integrated with the XLC as required by SP 800-37 R1, the NIST RMF helps project stakeholders and participants focus on the risk levels inherent in a system throughout the project and life of the system.

The planning segment of the *Initiation, Concept, and Planning Phase* of the XLC is a pivotal point for projects. Planned project costs and resources become final at this point. The work done before this segment defines the high-level functional and security requirements of the system. This includes a business process description and both functional and non-functional

[20] The CMS XLC artifacts are available on the XLC Artifacts and Templates web page, at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/Artifacts.html.

(e.g., security and privacy) requirements for the system. During this segment, the evaluation of various alternatives for the proposed system against all requirements enables development of project cost and time estimates, including those that are security related. The estimates include both project and ongoing system cost. The design, development (or acquisition), testing, implementation, and operation of the system happen after the *Initiation, Concept, and Planning Phase*.

NIST RMF tasks are mapped to the XLC to support projects.[21] All tasks that develop information needed to define and cost security requirements for the system occur before completion of the *Initiation, Concept, and Planning Phase* of the project, while tasks that develop, test, implement, and operate the security controls of the system follow this phase. Table 2 shows NIST RMF steps, tasks, and the XLC phases when performed. Figure 3 graphically relates these NIST RMF tasks to the XLC.

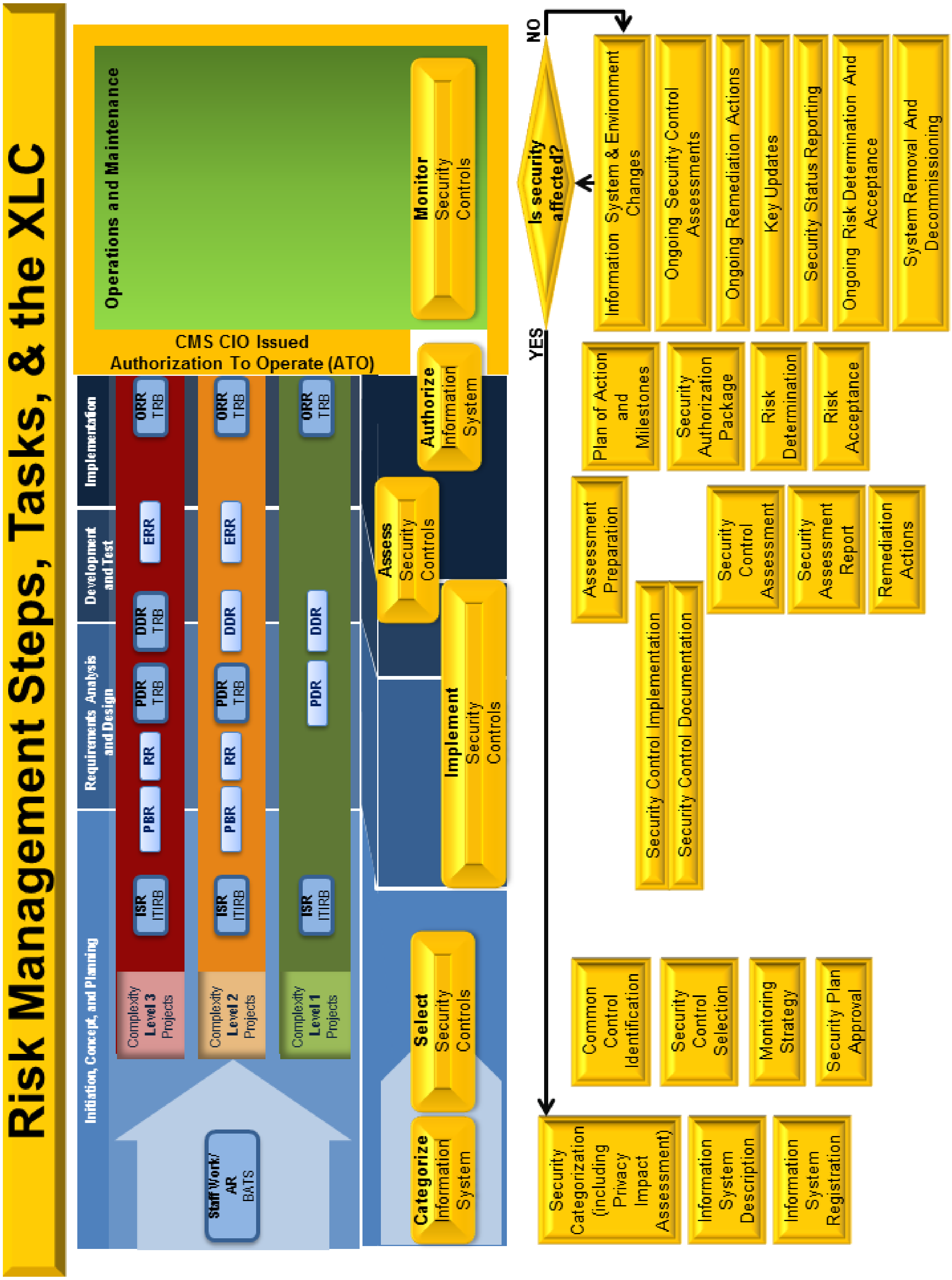
Table 2 NIST RMF Steps and Tasks with associated XLC Phases

NIST RMF Step	NIST RMF Task	XLC Phase(s)
Categorize Information System	Security Categorization	Initiation, Concept, and Planning
	Information System Description	Initiation, Concept, and Planning
	Information System Registration	Initiation, Concept, and Planning
Select Security Controls	Common Control Identification	Initiation, Concept, and Planning
	Security Control Selection	Initiation, Concept, and Planning
	Monitoring Strategy	Initiation, Concept, and Planning
	Security Plan Approval	Initiation, Concept, and Planning
Implement Security Controls	Security Control Implementation	Requirements Analysis and Design through Development and Test (includes Acquisition)
	Security Control Documentation	Requirements Analysis and Design through Development and Test (includes Acquisition)
Assess Security Controls	Assessment Preparation	Development and Test
	Security Control Assessment	Implementation
	Security Assessment Report	Implementation
	Remediation Actions	Implementation
Authorize Information System	Plan Of Action And Milestones	Implementation
	Security Authorization Package	Implementation
	Risk Determination	Implementation
	Risk Acceptance	Implementation
Monitor Security Controls	Information System And Environment Changes	Operations and Maintenance
	Ongoing Security Control Assessments	Operations and Maintenance

[21] The mapping matches NIST RMF tasks to XLC phases. When phases have a broad span (such as in the case of the Initiation, Concept, and Planning Phase) and the mapping requires greater specificity a reference to a segment of the phase (such as the concept segment) provides the granularity.

NIST RMF Step	NIST RMF Task	XLC Phase(s)
	Ongoing Remediation Actions	Operations and Maintenance
	Key Updates	Operations and Maintenance
	Security Status Reporting	Operations and Maintenance
	Ongoing Risk Determination And Acceptance	Operations and Maintenance
	Information System Removal And Decommissioning	Operations and Maintenance

Figure 3 NIST RMF Tasks within the XLC


Risk Management Steps, Tasks, & the XLC
Initiation, Concept, and Planning
Requirements Analysis and Design
Development and Test
Implementation
Operations and Maintenance
Staff Work/ AR BATS
Complexity Level 3 Projects
Complexity Level 2 Projects
Complexity Level 1 Projects
ISR ITIRB
PBR
RR
PDR TRB
DDR TRB
ERR
ORR TRB
ISR ITIRB
PBR
RR
PDR TRB
DDR
ERR
ORR TRB
ISR ITIRB
PDR
DDR
ORR TRB
CMS CIO Issued Authorization To Operate (ATO)
Categorize Information System
Select Security Controls
Implement Security Controls
Assess Security Controls
Authorize Information System
Monitor Security Controls
Security Categorization (including Privacy Impact Assessment)
Information System Description
Information System Registration
Common Control Identification
Security Control Selection
Monitoring Strategy
Security Plan Approval
Security Control Implementation
Security Control Documentation
Assessment Preparation
Security Control Assessment
Security Assessment Report
Remediation Actions
Plan of Action and Milestones
Security Authorization Package
Risk Determination
Risk Acceptance
Is security affected?
YES
NO
Information System & Environment Changes
Ongoing Security Control Assessments
Ongoing Remediation Actions
Key Updates
Security Status Reporting
Ongoing Risk Determination And Acceptance
System Removal And Decommissioning

4 THE XLC AS PART OF RISK MANAGEMENT

The XLC Detailed Description states:

> *The XLC model provides a streamlined approach to project oversight and execution. It is the next generation of project life cycle processes with a flexible approach to project execution and governance where the level of governance is directly associated with the complexity of the project. This model promotes agility, effective review of projects, and determines appropriate oversight early in the process – increasing predictability and efficiency.*[22]

The XLC includes risk management activities. For example, XLC deliverables may contain sections addressing project risk, plans to address project contingencies, business and system risks, security and functional requirements, designs for such requirements, and tests to validate the system works as required.

The *CMS Policy for Information Technology (IT) Investment Management & Governance*[23] requires that risk be managed, stating:

> *All CMS IT investments/projects must demonstrate that costs for appropriate IT privacy and security controls, security test and evaluation, and system certification and accreditation are explicitly incorporated into the life cycle planning of all systems. Cost-effective security of CMS information systems must be an integral component of business operations.*
>
> *CMS IT investments/projects selected for funding in any fiscal year and/or included in the CMS IT Investment Portfolio shall: …*
>
> - *Have well documented business process models, business requirements, risk assessment, data and security analysis, and business and technical alternatives identified.*
> - *Provide a comprehensive risk mitigation and life cycle management plan.*
> - *Ensure security of data and systems and compliance with applicable laws, regulations, policies, and guidance.*
>
> *All IT investments in the CMS IT Investment Portfolio shall be consistently controlled (monitored and managed) to maximize value, mitigate risks, ensure successful results, and to take corrective action when necessary.*

Managing risk must be done for both the system and the project that creates/changes the system. Federally mandated security requirements impose specific criteria for information systems and information system projects.[24] These criteria are the same for all project complexity levels, but

[22] CMS Expedited Life Cycle Process: Detailed Description, Version 2.7, May 3, 2012 p. 3. The document is available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/Downloads/XLC-DDD.pdf.

[23] Policy is available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/SystemLifecycleFramework/downloads/InvestmentMgmtPolicy.pdf.

[24] The NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, provides the government-wide requirements. These are refined into the CMS context by the ARS, including all appendices, available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

do vary based on the security category of the new or modified information system. Although these are not new requirements, SP 800–37 R1 places emphasis on performing tasks to meet these requirements as part of the project within the XLC, not separately. The concept that security is an add-on to a system has proven costly and ineffective, often resulting in significant security weaknesses and higher costs to mitigate these weaknesses.

A good number of these weaknesses are within the software or architecture that systems use, meaning many corrections may require overhauls of that specific software or architecture. Other initiatives are underway to improve the quality of software development, whether custom-developed, government off-the-shelf (GOTS), commercial off-the-shelf (COTS), or proprietary. *Build Security In*[25] is a Software Assurance[26] strategic initiative of the National Cyber Security Division (NCSD) of the U.S. Department of Homeland Security (DHS). It recognizes that software, lacking assurances to be secure, will have exploitable flaws. Enterprises, both government and business, are increasingly dependent on software to function and are at risk to flaws and weaknesses in the software they develop and acquire.

4.1 MINIMUM SECURITY REQUIREMENTS

The ARS defines the security protection requirements for information systems. These requirements include minimum safeguards that pertain to operational aspects of the system as well as the earlier (pre-operational) phases of the XLC.

For operational systems, controls for each security requirement that are appropriate for the system's security category[27] must be operational and functioning as designed. Systems that are in non-operations phases of the XLC (e.g., development, acquisition, or in the process of modification) must have their inherited security controls operational in the targeted operations environment and their system-specific controls (including the system-specific portions of hybrid controls) in the process of development and implementation.

***CMS Minimum Security Requirements* exist for projects, also**. Controls that must be in place and operating for projects during earlier XLC phases (and the CMSR reference ID) include, but are not limited to the following:

- Security Impact Analysis (CM-4)
- Allocation of Resources (SA-2)

[25] *Build Security In* is a collaborative Public/Private effort to build security into software in every phase of its development. It provides practices, tools, guidelines, rules, principles, and other resources that software developers, architects, and security practitioners can use at https://buildsecurityin.us-cert.gov/bsi/home.html.

[26] The United States Computer Emergency Readiness Team (US-CERT) *IT Security EBK: A Competency and Functional Framework* defines Software Assurance (SwA) as the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its lifecycle, and that the software functions in the intended manner. See http://www.us-cert.gov/ITSecurityEBK/.

[27] Security Category: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals. Source - FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, which is located at http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

- Lifecycle Support (SA-3)
- Acquisitions (SA-4)
- Information System Documentation (SA-5)
- Security Engineering Principles (SA-8)
- External Information System Services (SA-9)
- Developer Configuration Management (SA-10)
- Developer Security Testing (SA-11)
- Supply Chain Protection (SA-12)

An explanation of each requirement is available in the CMSR[28].

4.2 SOFTWARE ASSURANCE: BUILD SECURITY IN

The approach to securing a system after completion has proven to be inefficient and costly, yielding mixed results. Hence, the revised approach of the NIST RMF places equal emphasis on the selection and implementation of controls with the verification that the security controls are compliant. This means the controls will evolve during the project just as functional aspects of the system evolve. Sections 5 and 8 further describe this evolutionary process.

Virtually all information systems are dependent on software. Another key aspect of building in security relies on assuring that software does not contain inherent flaws that will introduce additional risk to the organization. A mature software assurance process typically requires years of coordinated effort across many IT disciplines and is beyond the scope of the RMH.

However, many systems (both new and existing) have significant software flaws, the most prevalent being injection attacks and memory management (buffer and stack) attacks. Prevention of these flaws occurs only during the code development (or re-development) process. This means the software development team must be aware of the risks in order to provide appropriate protective measures. Many developers employ a technique called "use cases" to define how the system should perform. A similar technique, "misuse cases," defines how it should not perform. Using misuse cases (a.k.a. abuse cases) achieves awareness by defining attack vectors for developers and testers, who can then ensure that the code does not have flaws that enable the attacks. The advantage of using these cases is that they are testable by the development team. **Agile development note:** please substitute *user story* for *use case* and *EVIL user story* for *misuse case*.

CMSR CM-4(1) states:

> *The organization analyzes new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.*

[28] The *CMS Minimum Security Requirements (CMSR's)* are documented in appendices A through C, of the *CMS Acceptable Risk Safeguards (ARS)* and are available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

Documented results of software misuse case tests serve as a base level of software assurance and can aid in proving compliance with CMSR CM-4(1) and SA-8. This applies to both developed and acquired software. At a minimum, misuse cases are to include all forms of injection attacks and all forms of buffer and stack mismanagement attacks.

5 NIST RMF STEPS

This section introduces the NIST RMF steps and their tasks, relates them to the XLC from the NIST RMF perspective, and addresses the impact that not completing a given task within the assigned XLC phase can have on a project.

5.1 CATEGORIZE INFORMATION SYSTEM

NIST SP 800-37 R1 states:

> *The security categorization process influences the level of effort expended when implementing the NIST RMF tasks. Information systems supporting the most critical and/or sensitive operations and assets within the organization, as indicated by the security categorization, demand the greatest level of attention and effort to ensure that appropriate information security and risk mitigation are achieved.*[29]

The *Categorize Information System* step consists of the following tasks:

- Security Categorization (including *Privacy Impact Assessment* [PIA] initiation)
- Information System Description
- Information System Registration

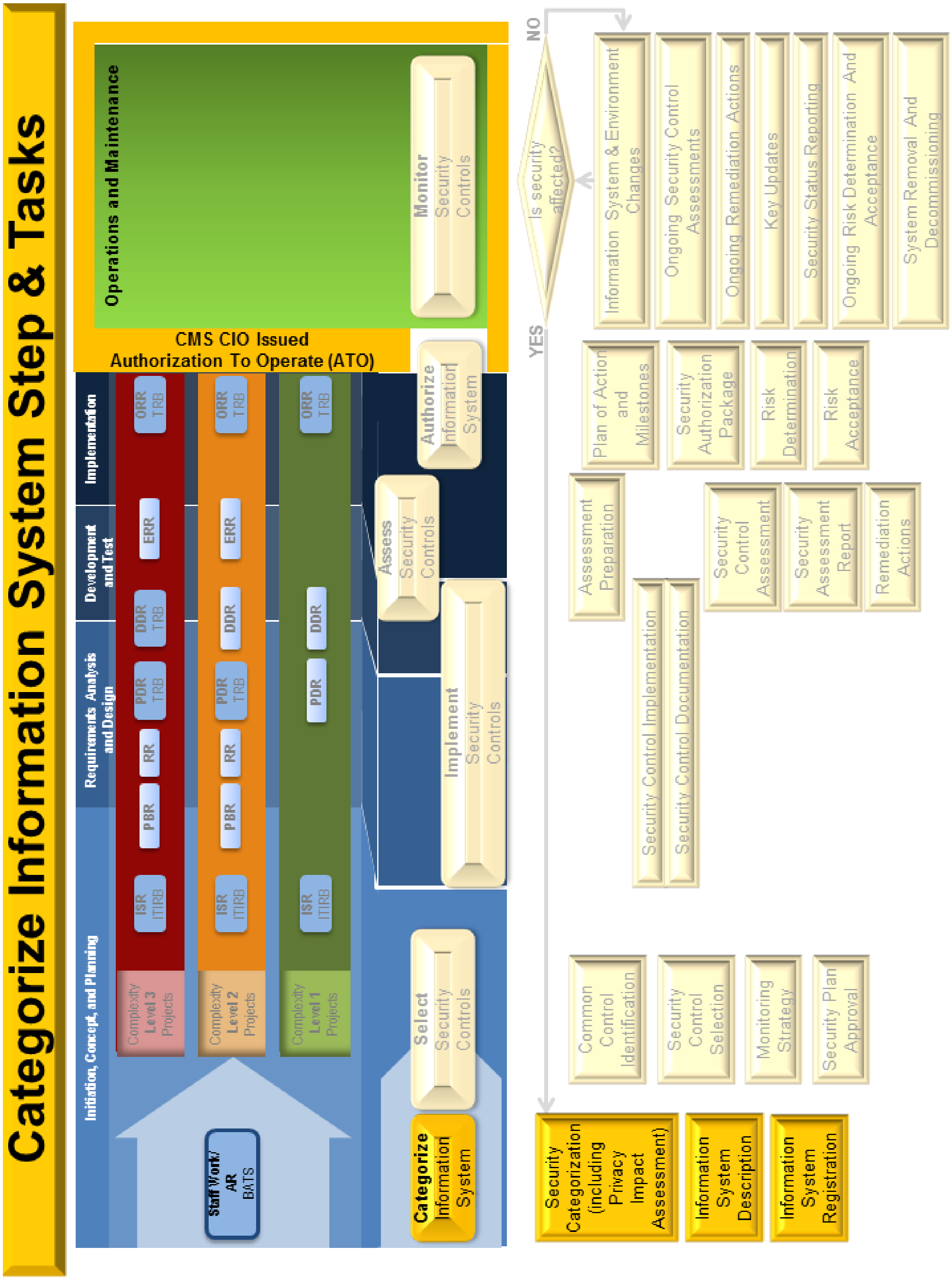
RMH Volume I, Chapter 2 contains in-depth coverage of considerations and activities for these tasks.

The *Categorize Information System* step begins during the initiation segment of the project and concludes during the concept segment of the *Initiation, Concept, and Planning Phase* of the project.

Figure 4 portrays the tasks of the *Categorize Information System* step as they occur within the XLC.

[29] NIST SP 800–37 R1: page 19.

Figure 4 Categorize Information System


Categorize Information System Step & Tasks
Operations and Maintenance
Monitor Security Controls
CMS CIO Issued Authorization To Operate (ATO)
Initiation, Concept, and Planning
Requirements Analysis and Design
Development and Test
Implementation
Staff Work/ AR BATS
Complexity Level 3 Projects
ISR ITIRB
PBR
RR
PDR TRB
DDR TRB
ERR
ORR TRB
Complexity Level 2 Projects
ISR ITIRB
PBR
RR
PDR TRB
DDR
ERR
ORR TRB
Complexity Level 1 Projects
ISR ITIRB
PDR
DDR
ORR TRB
Categorize Information System
Select Security Controls
Implement Security Controls
Assess Security Controls
Authorize Information System
Is security affected?
NO
YES
Security Categorization (including Privacy Impact Assessment)
Information System Description
Information System Registration
Common Control Identification
Security Control Selection
Monitoring Strategy
Security Plan Approval
Security Control Implementation
Security Control Documentation
Assessment Preparation
Security Control Assessment
Security Assessment Report
Remediation Actions
Plan of Action and Milestones
Security Authorization Package
Risk Determination
Risk Acceptance
Information System & Environment Changes
Ongoing Security Control Assessments
Ongoing Remediation Actions
Key Updates
Security Status Reporting
Ongoing Risk Determination And Acceptance
System Removal And Decommissioning

5.1.1 SECURITY CATEGORIZATION

Federal Information Processing Standard (FIPS) 199[30], *Standards for Security Categorization of Federal Information and Information Systems*, is the basis for the *Security Categorization* task. RMH Volume II Procedure 2.3, *Categorizing an Information System*[31] procedure implements the CMS specific process for FIPS 199 and establishes the security category of the (proposed) system. The PIA process should begin within this task as processing of, or access to, privacy information is relevant to the determination of the security category.

This task occurs during the initiation segment of the *Initiation, Concept, and Planning Phase* of the project and must conclude before the project can proceed beyond the Architecture Review.

The Business Owner is responsible for the *Security Categorization* task. The ISSO provides support.

Determining security categorization during the initiation segment of the *Initiation, Concept, and Planning Phase* of the XLC may sound premature because very little is known about the final system at initiation time. However, the sole determining factor of security categorization is the types of information the system processes, stores, accesses, transmits, or conveys between other points. It does not matter whether the information is structured data or unstructured data. The storage location of the information does not matter, either. These important technical considerations are addressed in later phases of the XLC. Therefore, performing the NIST RMF *Security Categorization* task during the initiation segment is realistic.

Even in the most stringent of development efforts, system functional requirements[32] may frequently change during the course of the project. Please understand that these changes can affect security requirements. When functional requirements change, business owners and system developers/maintainers must re-evaluate the security categorization and non-functional requirements[33] (including security requirements). This ensures that evolving business requirements do not alter the base assumptions on data categorization.

[30] FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems*, is available at http://csrc.nist.gov/publications/PubsFIPS.html.

[31] RMH Volume II Procedure 2-3 *Categorizing an Information System* is available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

[32] DHHS *Enterprise Performance Life Cycle Glossary*, located at http://www.hhs.gov/ocio/eplc/eplc_glossary.html, defines Functional Requirements as "Functional requirements specify Business Product features and what the Business Product must do. They are directly derived from the objectives defined in the Project Management Plan. A functional requirement is a tangible service, or function, that the Business Product must provide and is a non-technical requirement."

[33] DHHS *Enterprise Performance Life Cycle Glossary*, located at http://www.hhs.gov/ocio/eplc/eplc_glossary.html, defines Non-functional Requirements as "Non-functional requirements specify the criteria that are used to judge the operation of a Business Product, rather than specific behaviors (in contrast to functional requirements, which describe behavior or functions). Typical non-functional requirements are reliability, scalability, accessibility, performance, availability, and cost. Other terms for non-functional requirements are "constraints", "quality attributes", and "quality of service requirements". Non-functional requirements also specify the laws, regulations, and standards with which the Business Product must comply." Information system security, information security, records retention, and system continuity/recovery requirements are non-functional requirements of a system.

Non-functional requirements may change during the course of the life cycle, too. Projects lasting several years should expect some changes due to revisions in federal security requirements[34]. Such revisions are less likely to change the security categorization, but the revised federal requirements as stated in the current CMS ARS will be the standard used when assessing the security controls of the system.

Failure to address the *Security Categorization* task on a timely basis can affect the timing of future tasks and could result in both project delays and the costly implementation of controls that may otherwise not be required. Experience has shown that projects that fail to identify non-functional security requirements at the earliest possible XLC phase suffer the most costly setbacks in later phases as they attempt to reposition and redesign to meet omitted security control requirements.

5.1.2 INFORMATION SYSTEM DESCRIPTION

In the *Information System Description* task, focus shifts from the information that the system processes to the business and business processes that the system supports. Business risk analysis occurs. High-level record keeping and system availability requirements are determined. Documentation of the information system description in CFACTS begins. The CFACTS process for documenting the information system description proceeds in a way that allows the description to start with information at high level and later, in subsequent tasks, continue adding more detail as that knowledge becomes available. Table 3 contains a list of the content of the information system description and the XLC Phases when development of the content occurs.

Table 3 Content of an Information System Description

Relevant Information	XLC Phase
Full descriptive name of the information system including associated acronym	Initiation, Concept, & Planning
Unique information system identifier (typically a number or code)	Initiation, Concept, & Planning
Information system owner and authorizing official including contact information	Initiation, Concept, & Planning
Parent or governing organization that manages, owns, and/or controls the information system	Initiation, Concept, & Planning
Location of the information system and environment in which the system operates	Initiation, Concept, & Planning
Version or release number of the information system	Initiation, Concept, & Planning
Purpose, functions, and capabilities of the information system and missions/business processes supported	Initiation, Concept, & Planning – Requirements Analysis & Design
How the information system integrates into the enterprise architecture and information security architecture	Requirements Analysis & Design

[34] In August 2009, NIST published SP 800-53, Revision 3: *Recommended Security Controls for Federal Information Systems and Organizations*. NIST has scheduled Revision 4 for publication in July 2012. Usual time between revisions is in the two to three year range.

Relevant Information	XLC Phase
Status of the information system with respect to acquisition and/ or system development life cycle	All
Results of the security categorization process for the information and information system	Initiation, Concept, & Planning
Types of information processed, stored, and transmitted by the information system	Initiation, Concept, & Planning
Boundary of the information system for risk management and security authorization purposes	Initiation, Concept, & Planning
Applicable laws, directives, policies, regulations, or standards affecting the security of the information system	Initiation, Concept, & Planning
Architectural description of the information system including network topology	Requirements Analysis & Design
Hardware and firmware devices included within the information system	Requirements Analysis & Design
System and applications software resident on the information system	Requirements Analysis & Design
Hardware, software, and system interfaces (internal and external)	Initiation, Concept, & Planning – Requirements Analysis & Design
Subsystems (static and dynamic) associated with the information system	Initiation, Concept, & Planning – Requirements Analysis & Design
Information flows and paths (including inputs and outputs) within the information system	Requirements Analysis & Design
Cross domain devices/requirements	Requirements Analysis & Design
Network connection rules for communicating with external information systems	Requirements Analysis & Design
Interconnected information systems and identifiers for those systems	Development & Test
Encryption techniques used for information processing, transmission, and storage	Requirements Analysis & Design
Cryptographic key management information (public key infrastructures, certificate authorities, etc.)	Requirements Analysis & Design
Information system users (including organizational affiliations, access rights, privileges, citizenship, if applicable)	Initiation, Concept, & Planning Refined in Requirements Analysis & Design
Ownership/operation of information system (e.g., government-owned, government-operated; government-owned, contractor-operated; contractor-owned, contractor-operated; nonfederal [state and local governments, grantees])	Initiation, Concept, & Planning
Security authorization date and authorization termination date	Implementation
Incident response points of contact	Development & Test
System availability requirements (MTD, RTO, RPO)	Initiation, Concept, & Planning – Requirements Analysis
Planning for security in the SDLC	Initiation, Concept, & Planning – Development & Test
E-authentication level	Initiation, Concept, & Planning

Relevant Information	XLC Phase
Assignment of security responsibility	Initiation, Concept, & Planning
Business risk assessment and risk management	Initiation, Concept, & Planning
Interconnection Security Agreements (ISA) or Memorandum of Understanding (MOU) for interconnections between systems owned by different organizations.	Any, but before the connection is established.
Other information as required by the organization	T.B.D.

The Business Owner is responsible for the *Information System Description* task. The ISSO provides support. Other groups may collaborate with the Business Owner to provide specialized subject matter expertise.

The CMS business owner examines the mission/business process and establishes its sensitivity to disruption during the initiation and concept segments of the *Initiation, Concept, and Planning Phase* of the project. The key value[35] established by this examination is:

- **Maximum Tolerable Downtime (MTD)**. The MTD represents the amount of disruption that the mission/business process can withstand without causing significant harm to the organization's mission, measured in time. This is the time span from the occurrence of a disruptive event until the business is back to normal day-to-day operations, on a current basis. This is a mission/business process requirement and is independent of the information system. Determining MTD is important because it defines the worst-case availability requirement for any system supporting this specific mission/business process.

Failure to define MTD leaves developers, designers, contractors, and contingency planners with imprecise direction regarding (1) the resiliency requirements for the IT infrastructure and the system, (2) selection of an appropriate recovery method, and (3) the depth of detail that will be required when developing recovery procedures, including their scope and content. When established, the MTD sets the baseline for the availability requirements of the mission/business process for *Contingency Plan (CP), Continuity of Operations (COOP), Business Continuity Planning (BCP), and Disaster Recovery (DR)* purposes. The *Office of Public Engagement/ Emergency Preparedness and Response Operations* (EPRO) can provide consultation on COOP planning, processes, and policy directives to business owners who need assistance.

Based on the MTD, CP requirements may rise above the level established based on the information types alone.

The MTD will be used in later phases of the project to specify equipment and capabilities and determine key system contingency planning parameters including:

- **Recovery Time Objective (RTO)**. The RTO is the overall length of time an information system's components can be out of service before negatively affecting the organization's mission or mission/business processes. In order to avoid harming the organization's mission the RTO is always less than the MTD. Determining the information system resource RTO is important for selecting technologies that are best suited for meeting the MTD. When it is not

[35] NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems, is available at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf.

feasible to meet the RTO **immediately**, and the MTD is inflexible, a Plan of Action and Milestone should be initiated to document the situation and plan for its mitigation.

- **Recovery Point Objective (RPO)**. The RPO is the point in time to which data must be recovered after an outage. This point in time is prior to a disruption or system outage and is the most recent time to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage. Unlike RTO, RPO is not directly considered as part of MTD. Rather, it is a factor of how much data loss the mission/business process can tolerate during the recovery process. However, after system recovery the RPO becomes a determining factor of work that must be caught up — typically through manual processes (see Work Recovery Time below) — in order to bring the system and its data current, after which normal day-to-day operations resume.
- **Work Recovery Time (WRT)**. The WRT is the time it takes to get critical business functions back up and running normally after the systems (hardware, software, and configuration) are restored to the RPO. This includes the manual processes necessary to verify that the system was restored to the RPO, completion of all necessary processes to address the remaining lost or out-of-synch data, and the orderly processing of all transactions and business processes from the time of the disruption until the current date and time.

In addition, business owners analyze other risks to the mission/business process and document them in the business risk assessment during the initiation and concept segments of the *Initiation, Concept, and Planning Phase*. Some examples of other business risks include fraud, privacy, customer relations, regulatory, safety, quality of service, and recordkeeping concerns.

Performing the *Information System Description* task occurs within the initiation and concept segments of the *Initiation, Concept, and Planning Phase* of the XLC, although more detail supplements the description of the information system in the form of incremental additions to CFACTS during later XLC phases, as described in Table 3. This task is dependent upon the security category, established during the *Security Categorization* task.

Failure to address the *Information System Description* task on a timely basis can introduce significant errors in determining both the functional and non-functional system requirements. This can result in:

- The system not performing its intended function.
- Inadequate security for the system.
- An increase in risk to the business.
- Project cost and time overruns.

5.1.3 INFORMATION SYSTEM REGISTRATION

The task of *Information System Registration* occurs during the initiation and concept segments of the *Initiation, Concept, and Planning Phase* of the XLC. It is imperative to register a system name and acronym to activate the system in CFACTS. Once activated, CFACTS facilitates incremental entry of data relating to security and risk management as such information evolves during the project.

The Business Owner is responsible for the *Information System Registration* task. The ISSO provides support. Enterprise Architecture is the official registration group.

Failure to perform the *Information System Registration* task on a timely basis means the CFACTS tool will be unavailable for use. CFACTS remains unavailable until registration is complete. This delays the start of, and increases the time to perform, the NIST RMF *Security Control Selection* step. In turn, these delays cascade, potentially exposing the project to needless increases in levels of security control expenditures, which arise from unidentified common controls.

5.2 SELECT SECURITY CONTROLS

The NIST RMF *Select Security Controls* step will establish the security control requirements and continuous monitoring strategy for the system, factoring in any need to supplement controls based on business needs (CP, COOP, and DR requirements). Its tasks require the CFACTS tool, which became available upon system registration.

The *Select Security Controls* step consists of four (4) tasks:

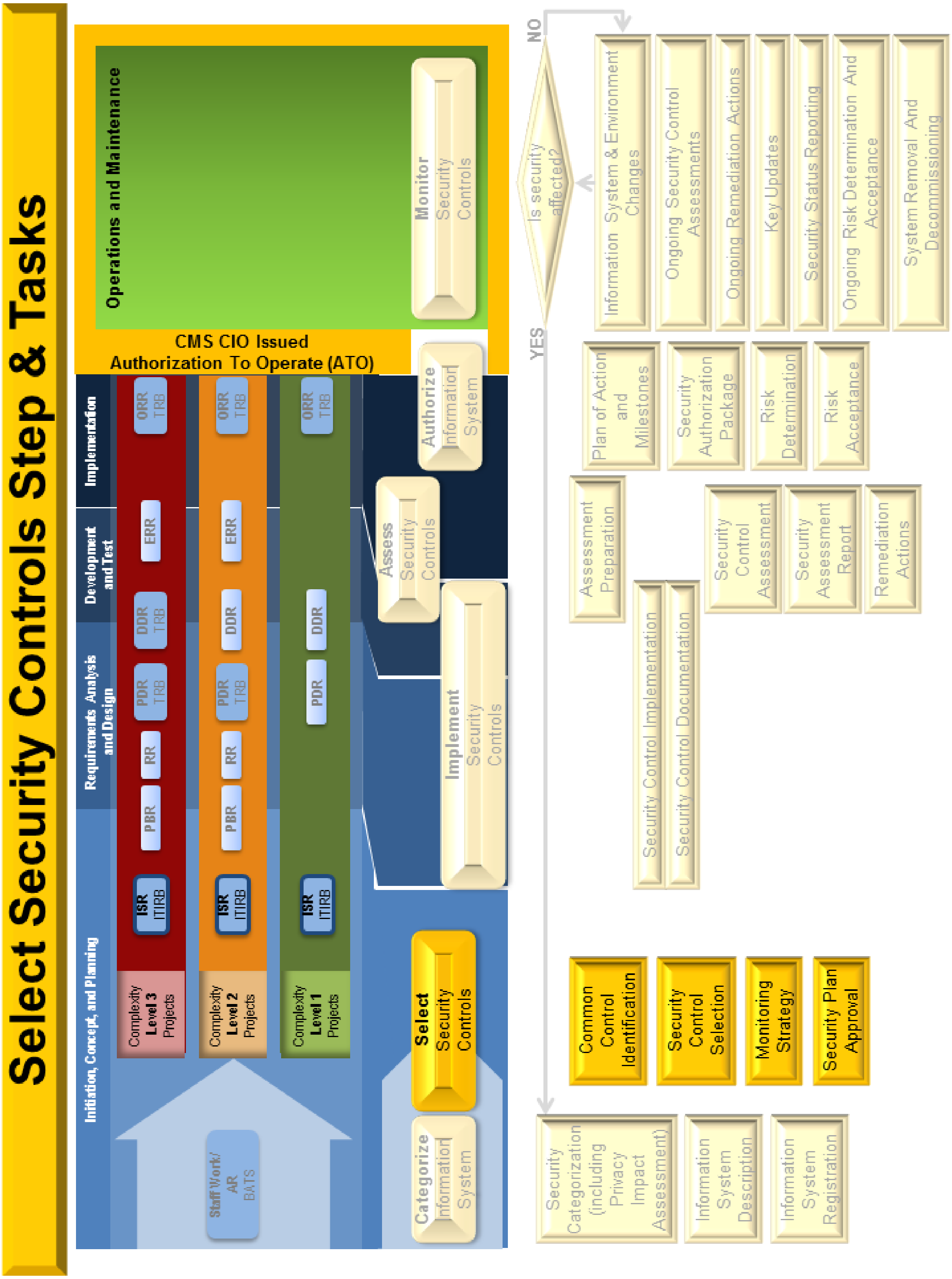
- *Common Control Identification*
- *Security Control Selection*
- *Monitoring Strategy*
- *Security Plan Approval*

Chapter 3 of the RMH Volume I contains in-depth coverage of considerations and activities for these tasks.

This step occurs during the Concept and Planning segments of the *Initiation, Concept, and Planning Phase* of the XLC.

Figure 5 portrays the tasks of the *Select Security Controls* step as they occur within the XLC.

Figure 5 Select Security Controls


Select Security Controls Step & Tasks
Initiation, Concept, and Planning
Requirements Analysis and Design
Development and Test
Implementation
Operations and Maintenance
CMS CIO Issued Authorization To Operate (ATO)
Staff Work/ AR BATS
Complexity Level 3 Projects
ISR ITIRB
PBR
RR
PDR TRB
DDR TRB
ERR
ORR TRB
Complexity Level 2 Projects
ISR ITIRB
PBR
RR
PDR TRB
DDR
ERR
ORR TRB
Complexity Level 1 Projects
ISR ITIRB
PDR
DDR
ORR TRB
Categorize Information System
Select Security Controls
Implement Security Controls
Assess Security Controls
Authorize Information System
Monitor Security Controls
Security Categorization (including Privacy Impact Assessment)
Information System Description
Information System Registration
Common Control Identification
Security Control Selection
Monitoring Strategy
Security Plan Approval
Security Control Implementation
Security Control Documentation
Assessment Preparation
Security Control Assessment
Security Assessment Report
Remediation Actions
Plan of Action and Milestones
Security Authorization Package
Risk Determination
Risk Acceptance
YES
Is security affected?
NO
Information System & Environment Changes
Ongoing Security Control Assessments
Ongoing Remediation Actions
Key Updates
Security Status Reporting
Ongoing Risk Determination And Acceptance
System Removal And Decommissioning

5.2.1 COMMON CONTROL IDENTIFICATION

Common controls are inheritable controls that are in place, operational, and verified for the environment within which the proposed system will reside. For example, many of the physical and environmental security control requirements for systems that are verified to be wholly within the defined host data center may be fully inheritable from the organization responsible for securing the data center. A hosted system need not create redundant controls for such requirements as Fire Protection and Backup Power, when the host environment control is sufficient (i.e., "inherited"). However, a *fully*-inheritable control, by definition, cannot be influenced by an individual (inheriting) system. If an inheriting system is capable of influencing the *effectiveness* of an inheritable control, then that control cannot be considered *fully* inherited; but is instead considered to be only *partially* inherited, because other system-specific elements of the control must be implemented to ensure proper operation of the inherited control. These *partially*-inheritable controls are called *Hybrid* controls.

A hybrid control has two portions: the inherited part of the control (common control), and the other system-specific part of the control. The system-specific portion is that part of the requirement each system must address, individually. The common and system-specific portions collectively satisfy the security requirement. **Note: If an inherited control requires any management or configuration at the system-specific level to implement, then that control is *Hybrid*.**

For example, ARS AC-2 (Account Management) requires management of information system accounts. If the system will reside wholly within an Enterprise Data Center (EDC), existing account management procedures meet many portions of the control requirement. These are inheritable. However, some portions, such as identifying authorized users of the information system and specifying access privileges, are system-specific. The business owner, or a properly designated individual, must provide and update user information to the EDC for each system. This is the system-specific portion of this hybrid control.

Please note: the common controls that are available for inheritance can be different under various project solution scenarios. The same system deployed at different locations, with different system boundaries, or using different architectures can have different inheritable controls and, consequently, a different number of system-specific controls to address and implement as part of the project.

The *Common Control Identification* task takes place wholly within the concept segment of the *Initiation, Concept, and Planning Phase* of the XLC. Each system alternative has its own set of identified common controls. This task is fully dependent on completion of all tasks of the *Categorize Information System* step (Section 5.1), as previously described.

The Business Owner is responsible for this task, in collaboration with Common Control Providers and the CMS Chief Technology Officer. The ISSO, Technical Review Board (TRB), and the Enterprise Information Security Group (EISG) provide support.

Failure to complete the *Common Control Identification* task on a timely basis has negative project cost and schedule implications. Lacking identified common controls, the project must implement all security requirements as system-specific controls. This can lead to duplication of controls that already exist.

5.2.2 SECURITY CONTROL SELECTION

The Security Control Selection task defines system-specific security requirements the project implements to protect the confidentiality, integrity, and availability of information and the system. Some of the controls developed to meet these requirements become part of the system and its related procedures, protecting the system's operation. Others govern the execution of the project, protecting the system's development and implementation. A few controls do both.

Any controls not identified in the common control selection are system-specific. In addition, all hybrid controls will have some portion of the requirement for which the system is responsible; therefore, the project must develop this system-specific portion of the control. All controls identified in the *Security Control Selection* task, as well as information developed in prior tasks (e.g., availability requirements MTD, RTO, RPO, and WRT), define the security non-functional system requirements for the system.

In addition, project documents[36] including, but not limited to, the *Project Charter*, the *Project Management Plan*, and the *Project Process Agreement* must reflect those security requirements relating to system acquisition. Furthermore, controls implementing the system acquisition requirements must be in place and effective throughout the project.

As previously stated, both government and business are increasingly dependent on software to function and are at risk to flaws and weaknesses in the software they develop and acquire. Proactively addressing security defects through software assurance measures is effective in reducing risk and minimizing development and maintenance rework costs.[37] CMS requires proof of misuse case testing for software, whether developed and acquired, as a base level of software assurance. Identification of misuse cases takes place in conjunction with the *Security Control Selection* task. Misuse cases addressing all forms of injection attacks and all forms of buffer and stack mismanagement attacks comprise the base level software assurance requirements for projects.

Performing the *Security Control Selection* task follows the *Common Control Identification* task within the concept segment of the *Initiation, Concept, and Planning Phase* of the XLC.

The Business Owner is responsible for this task. The ISSO provides support and the EISG and CTO provide guidance.

Failure to perform Security Control Selection on a timely basis results in incomplete security requirements that, in turn, affect project cost, timing, and contracting.

5.2.3 MONITORING STRATEGY

The Monitoring Strategy task identifies how the business owner proposes to monitor appropriate controls throughout the project and on an ongoing basis during the *Operations and Maintenance*

[36] All project documentation templates are in the *XLC Artifacts & Templates* webpage at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/Artifacts.html.

[37] NIST SP 800-55 Revision 1, *Performance Measurement Guide for Information Security*, which is available at http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf.

(O&M) Phase of the XLC after system implementation. The controls monitored during the project need not be identical to those monitored during the *O&M Phase*. For example, the expectation for software assurance monitoring is during the project, but not following implementation as long as there is no software development activity. A combination of automated and manual processes is permissible to ensure the adequacy of system-specific controls (or portions) both during the project and during the *O&M Phase*.

The *Monitoring Strategy* task takes place within the planning segment of the *Initiation, Concept, and Planning Phase* of the XLC and completes prior to *Security Plan Approval*. The *Monitoring Strategy* task is dependent on completion of *Security Control Selection*.

The Business Owner (or Common Control Provider for common controls) is responsible for this task. The ISSO provides support and the EISG and CTO provide guidance.

Failure to perform the *Monitoring Strategy* task on a timely basis will result in an incomplete System Security Plan (SSP). CMS will not approve incomplete SSPs, which may cause potential delays in the project.

5.2.4 SECURITY PLAN APPROVAL

The *Security Plan Approval* task is a major checkpoint to ensure that all of the preceding tasks have been completed and included within CFACTS. CFACTS will produce an initial SSP, including an initial Risk Assessment (RA) that contains mission/business process risks and the monitoring strategy, for review and approval by the Technical Review Board (TRB). At this time, the document will contain a basic system description at a high level, identification of the business risks, and identification of all common, hybrid, and system-specific controls. The system-specific controls and the system-specific portion of hybrid controls will receive a ‘planned’ designation, as they are not yet operational. Project requirements, plans, and schedules include all such control requirements.

Approval of the security plan occurs during the planning segment of the *Initiation, Concept, and Planning Phase* and is dependent on completion of all prior risk management tasks.

The Business Owner (or Common Control Provider for common controls) is responsible for initiating this task and the TRB is responsible for review and approval/disapproval actions. The ISSO provides support and the EISG and CTO provide guidance.

Failure to obtain SSP approval indicates the project requirements and plan for requirement implementation are incomplete. Project delay results, as the SSP must be complete and receive formal approval prior to the next phase of the XLC.

5.3 IMPLEMENT SECURITY CONTROLS

The *Implement Security Controls* step spans two (2) XLC phases: the *Requirements Analysis and Design* phase and the *Development and Test* phase. This step consists of two (2) tasks:

- *Security Control Implementation*
- *Security Control Documentation*

Chapter 4 of the RMH Volume I contains in-depth coverage of considerations and activities for these tasks. Unlike other steps of the NIST RMF, the tasks associated with the Implement Security Controls step occur in parallel within each segment of these XLC phases, but serially across segments. Software assurance activities occur during these phases and segments in the same fashion. Table 4 provides a brief description of the activities done for these NIST RMF and software assurance tasks in each segment of the two (2) XLC phases.

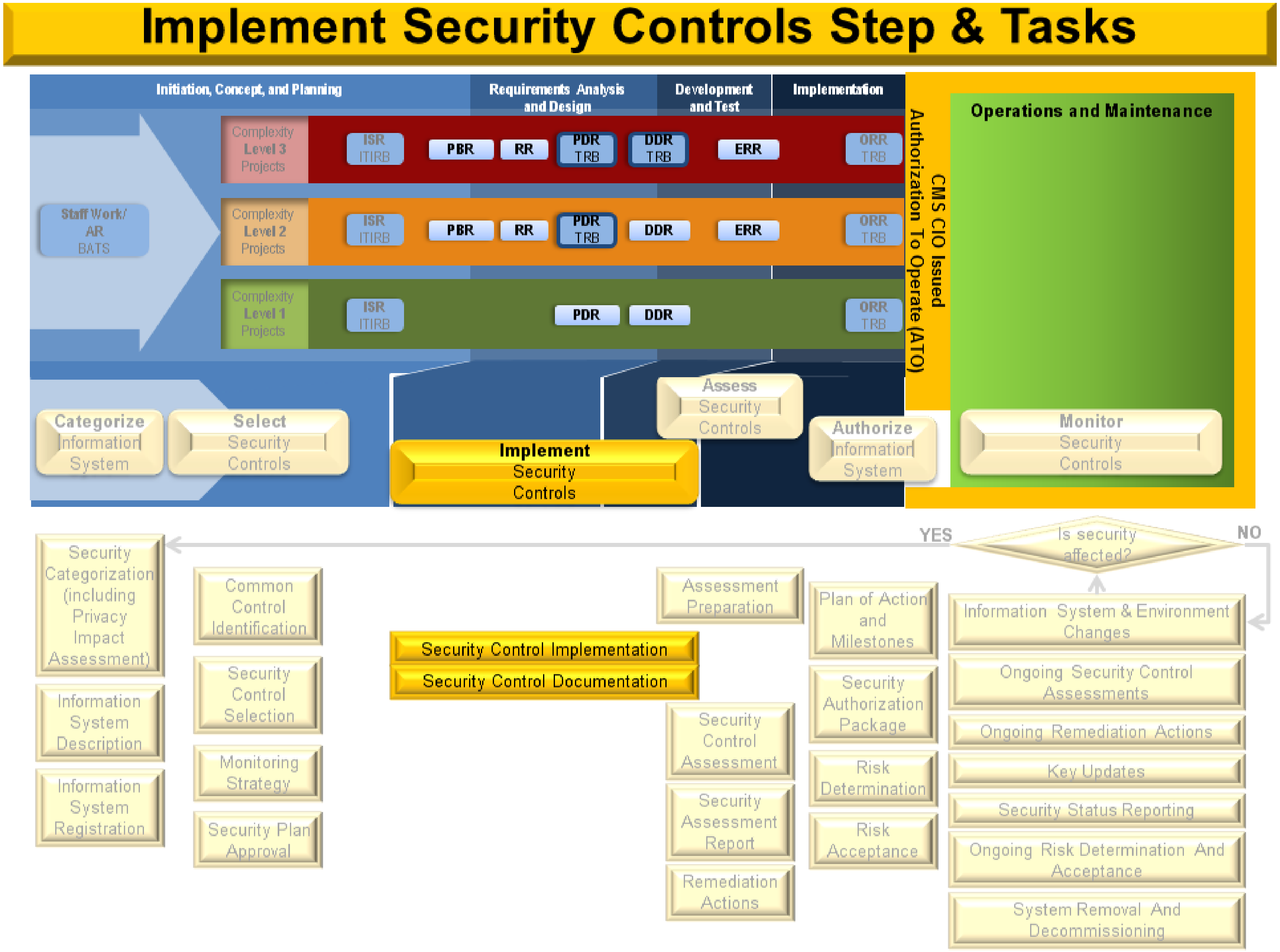
Table 4 Implement Security Controls Step by XLC Phase Segment

XLC Phase Segment	Security Control Implementation Task	Security Control Documentation Task
Requirements Analysis	For each planned control, analyze the requirement statement and develop the control statement to meet the requirement. **Software Assurance:** develop detailed requirements for identified misuse cases to enable the project to avoid creating the most common flaws within the software. These flaws include: Injection attacks (including cross site scripting, SQL injection, format string problems, command injection, and reflection injection) and Memory management attacks (including buffer overflow, buffer underflow, and stack mismanagement).	Enter control statements for each requirement into CFACTS as developed.’ **Software Assurance:** document each misuse case separately in the Planning for Security in the SDLC section of CFACTS.
Design	Develop a design for each analyzed control. Note: automation accomplishes some controls, some are manual, and others require a mixture of automated and manual components. Business stakeholders may design purely manual controls. **Software Assurance:** the technical system design will accommodate the misuse cases and provide test plans for each of them.	Enter designs for each requirement into CFACTS as developed. **Software Assurance:** document test plans for each misuse case in the appropriate project document.
Development	Develop each control consistent with the design specification. Note: the business unit that performs the manual controls should develop them. **Software Assurance:** development will include measures to protect against the misuse cases.	Update control documentation as needed. **Software Assurance:** update the record of completion of development related to all misuse cases within project documentation.
Test	Test each control to verify that it functions as required. **Software Assurance:** perform tests to ensure protection from each of the cases.	Document test results. **Software Assurance:** Update the Planning for Security in the SDLC section of CFACTS with test results.

This step begins in the *Requirements Analysis and Design Phase* and ends in the *Development and Test Phase* of the XLC.

Figure 6 portrays the tasks of the *Implement Security Controls* step as they occur within the XLC.

Figure 6 Implement Security Controls


Implement Security Controls Step & Tasks
Initiation, Concept, and Planning
Requirements Analysis and Design
Development and Test
Implementation
Operations and Maintenance
CMS CIO Issued Authorization To Operate (ATO)
Staff Work/ AR BATS
Complexity Level 3 Projects
Complexity Level 2 Projects
Complexity Level 1 Projects
ISR ITIRB
PBR
RR
PDR TRB
DDR TRB
ERR
ORR TRB
ISR ITIRB
PBR
RR
PDR TRB
DDR
ERR
ORR TRB
ISR ITIRB
PDR
DDR
ORR TRB
Categorize Information System
Select Security Controls
Implement Security Controls
Assess Security Controls
Authorize Information System
Monitor Security Controls
YES
Is security affected?
NO
Security Categorization (including Privacy Impact Assessment)
Information System Description
Information System Registration
Common Control Identification
Security Control Selection
Monitoring Strategy
Security Plan Approval
Security Control Implementation
Security Control Documentation
Assessment Preparation
Security Control Assessment
Security Assessment Report
Remediation Actions
Plan of Action and Milestones
Security Authorization Package
Risk Determination
Risk Acceptance
Information System & Environment Changes
Ongoing Security Control Assessments
Ongoing Remediation Actions
Key Updates
Security Status Reporting
Ongoing Risk Determination And Acceptance
System Removal And Decommissioning

5.3.1 SECURITY CONTROL IMPLEMENTATION

Within the *Security Control Implementation* task, work on each control requirement proceeds as appropriate for the specific XLC phase segment of the project: *Requirements Analysis, Design, Development* (or Acquisition), and *Test*. In addition, definition, design, development, and testing of the misuse cases occur for software assurance purposes. System security controls and software assurance build, in incremental fashion, over the XLC phases. Project controls (as discussed in section 4.2) are in place throughout the project.

The *Security Control Implementation* task, performed during two (2) lifecycle phases, begins during the requirements analysis segment of the *Requirements Analysis and Design Phase* and ends in the test segment of the *Development and Test Phase* of the XLC, parallel with the *Security Control Documentation* task within each segment of each phase.

The Business Owner (or Common Control Provider for common controls) is responsible for this task. The project team and ISSO provide support and the CTO provides guidance.

Failure to perform the *Security Control Implementation* task appropriately within the designated XLC phases will result in the system not meeting security requirements and may prevent obtaining an Authorization to Operate (ATO) for the system.

5.3.2 SECURITY CONTROL DOCUMENTATION

Within the *Security Control Documentation* task, document each control requirement incrementally as it proceeds through each segment of the *Requirements Analysis and Design Phase* and *Development and Test Phase* of the project, including all acquisition activities. In addition, documentation of misuse cases for software assurance proceeds through these phases of the XLC. Documentation serves as confirming evidence of performance for each control and misuse case in the *Security Control Implementation* task. In some cases, such as a contingency plan, the document is the implementation of the control.

The *Security Control Documentation* task, performed during each segment of two (2) lifecycle phases, begins during the requirements analysis segment of the *Requirements Analysis and Design Phase* and ends in the test segment of the *Development and Test Phase* of the XLC, parallel with the *Security Control Implementation* task within each segment of each phase.

The Business Owner (or Common Control Provider for common controls) is responsible for this task. The project team and ISSO provide support.

Failure to perform the *Security Control Documentation* task appropriately within the designated segments of XLC phases will result in the system not meeting security requirements, potentially having significant adverse impact on project cost and schedules, and other CMS systems.

5.4 ASSESS SECURITY CONTROLS

The *Assess Security Controls* step is the formal security testing of the system. For new systems, all system-specific controls and system-specific portions of hybrid controls undergo a security controls assessment. This includes a review of the controls employed during the project as well as proof of software assurance testing. In addition, verification of all inherited controls ensures they are operational, effective, and legitimately inherited by the system. CMS has independent third party assessors perform the security assessment[38] to avoid bias.

The *Assess Security Controls* step encompasses the following tasks:

- *Assessment Preparation*
- *Security Control Assessment*
- *Security Assessment Report*
- *Remediation Actions*

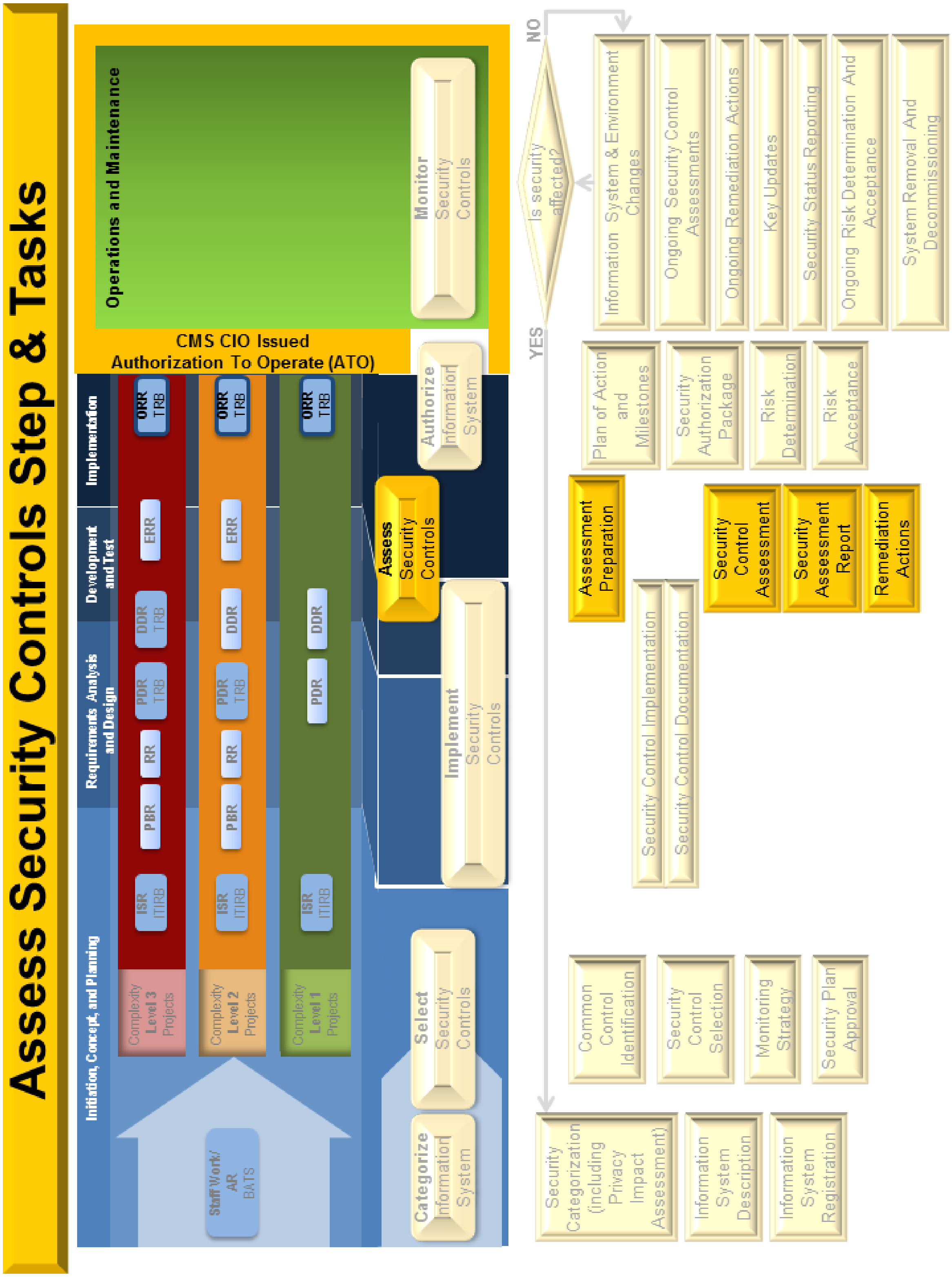
RMH Volume I, Chapter 5 contains in-depth coverage of considerations and activities for these tasks.

The *Assess Security Controls* step begins during the *Development and Test Phase* and concludes during the *Implementation Phase* of the XLC.

Figure 7 portrays the tasks of the *Assess Security Controls* step as they occur within the XLC.

[38] NIST SP 800-53A R1: *"Organizations are encouraged, whenever possible, to take advantage of the assessment results and associated assessment-related documentation and evidence available on information system components from previous assessments including independent third-party testing, evaluation, and validation."*

Figure 7 Assess Security Controls


Assess Security Controls Step & Tasks
Initiation, Concept, and Planning
Requirements Analysis and Design
Development and Test
Implementation
Operations and Maintenance
CMS CIO Issued Authorization To Operate (ATO)
Staff Work/ AR BATS
Complexity Level 3 Projects
Complexity Level 2 Projects
Complexity Level 1 Projects
ISR ITIRB
PBR
RR
PDR TRB
DDR TRB
ERR
ORR TRB
PDR
DDR
Categorize Information System
Select Security Controls
Implement Security Controls
Assess Security Controls
Authorize Information System
Monitor Security Controls
Security Categorization (including Privacy Impact Assessment)
Information System Description
Information System Registration
Common Control Identification
Security Control Selection
Monitoring Strategy
Security Plan Approval
Security Control Implementation
Security Control Documentation
Assessment Preparation
Security Control Assessment
Security Assessment Report
Remediation Actions
Plan of Action and Milestones
Security Authorization Package
Risk Determination
Risk Acceptance
Is security affected?
YES
NO
Information System & Environment Changes
Ongoing Security Control Assessments
Ongoing Remediation Actions
Key Updates
Security Status Reporting
Ongoing Risk Determination And Acceptance
System Removal And Decommissioning

5.4.1 ASSESSMENT PREPARATION

The *Assessment Preparation* task involves the development and approval of the *Security Assessment Plan*. The security assessment plan provides the objectives for and a detailed roadmap of how to assess the information system security controls. The CMSR assessment procedures for each control requirement describes the series of distinct steps that the assessment team should follow in developing a plan to assess the security controls in the information system. For existing systems, CMS encourages the use of results from prior assessments and continuous monitoring providing they are current and not affected by the change to the system. Tests conducted during the test segment of the *Development and Test Phase* for security controls and misuse cases may factor into the assessment plan, as long as they are sufficiently rigorous and unbiased to provide needed assurances. Evidence of such testing will aid assessors in reviewing the system.

The *Assessment Preparation* task begins in the test segment of the *Development and Test Phase* and is prerequisite to the *Security Control Assessment task*. **Note: scheduling security assessors requires five (5) to six (6) months advance notice.** Therefore, the initial contact with EISG to arrange for the assessment should precede the *Development and Test Phase*. Short duration projects should contact EISG during project initiation.

An independent assessor is required[39] for a security assessment. This establishes impartiality and helps to assure the security assessment is unbiased.[40]

The Business Owner (or Common Control Provider for common controls) is responsible for initiating this task. The EISG facilitates the security assessment. The security assessor develops the plan. The ISSO and project team provide support.

Failure to perform the *Assessment Preparation* task on a timely basis will affect the project schedule and put critical implementation dates at risk.

5.4.2 SECURITY CONTROL ASSESSMENT

A security assessor performs the *Security Control Assessment* task to determine that all security controls are in place and operating effectively. The assessor evaluates each control identified in the plan, and notes the status of each evaluation (pass/fail). For controls that do not completely pass assessment, the assessor records and evaluates findings and observations, identifies and explains weaknesses, and recommends corrective actions.

The *Security Control Assessment* task begins and ends within the *Implementation Phase* of the project. It is contingent upon the plan developed in the *Assessment Preparation* task.

[39] *CMS Reporting Procedure for Information Security (IS) Assessments*, March 19, 2009, located at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

[40] *CMS Information Security Assessment Procedure*, March 19, 2009, located at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

The security assessor is responsible for this task. The ISSO, Business Owner (or Common Control Provider for common controls), EISG, and project team provide support.

Failure to perform the *Security Control Assessment* task on a timely basis will result in delays in obtaining an ATO. This can cause the project to miss its targeted completion dates.

5.4.3 SECURITY ASSESSMENT REPORT

The security assessor performs the *Security Assessment Report* task. This task includes preparation of a formal *Security Assessment Report (SAR)* that indicates all controls tested, the tests performed and result of each test (pass or fail), and documents all findings, observations, and weaknesses. Amplifying detail (such as for deficiencies in an SSP, RA, or CP) may appear as an attachment to the report or a separate document, as appropriate. When completed, the assessor delivers complete electronic sets of all assessment documentation in its original form, including a copy to the EISG. CFACTS tracks assessment results in accordance with RMH Volume II, Procedure 5.6, *Documenting Security Control Effectiveness in CFACTS*.

Note: Results of one security control assessment can only be modified based on the findings of a subsequent security control assessment conducted with the same, or a higher, level of assessor independence.

The *Security Assessment Report* task takes place during the *Implementation Phase* of the project. It contains the results of the security assessment as well as any remediation actions accomplished during the assessment.

The security assessor is responsible for this task. The ISSO, Business Owner (or Common Control Provider for common controls), and the EISG provide support.

Failure to perform the *Security Assessment Report* task on a timely basis will result in delays in obtaining an ATO. This can cause the project to miss its targeted completion dates or fail to gain an ATO.

5.4.4 REMEDIATION ACTIONS

Remediation (e.g., fixing, eliminating, correcting) of weaknesses may occur during the *Security Control Assessment* task. Verification of weakness remediation is possible by retesting such fixes, which is highly desirable. Weaknesses corrected during the course of the assessment and documented within the final report have a *corrected during assessment* designation. This provides a complete picture of the status of enterprise risk, both before and after the assessment.

In addition, some corrective actions, completed after the *Security Control Assessment* task ends, may occur before the authorization decision. Full documentation of the actions taken and proof of the testing performed must be present and have association with the weakness in CFACTS. These weaknesses and their remediation receive the designation *pending verification*.

The *Remediation Actions* task begins in the *Implementation Phase* of the project and continues until completion of all remediation actions, referred to as “Milestones” associated with the Plan of Action and Milestones (POA&M) for each weakness. Initial remediation actions focus first on those weaknesses that pose the highest level of risk to CMS.

The Business Owner (or Common Control Provider for common controls) is responsible for this task. The project team, system developer/maintainer, ISSO, security control assessor, CTO, and the EISG provide support.

Failure to perform the *Remediation Actions* task on a timely basis causes elevated risk levels to the system, business unit, CMS, and, sometimes, other systems. Such elevation may raise risk to an unacceptable level. This will delay project implementation until completion and verification of corrective actions that bring the risk of operating the system within acceptable limits.

5.5 AUTHORIZE INFORMATION SYSTEM

The *Authorize Information System* step addresses the formal risk decision regarding running the system. The basis of the decision is the risk to CMS as identified by documentation developed during the project, results of the security assessment (including remediation actions that have been accomplished), and the plan to mitigate remaining risks. The *Authorize Information System* step consists of the following tasks:

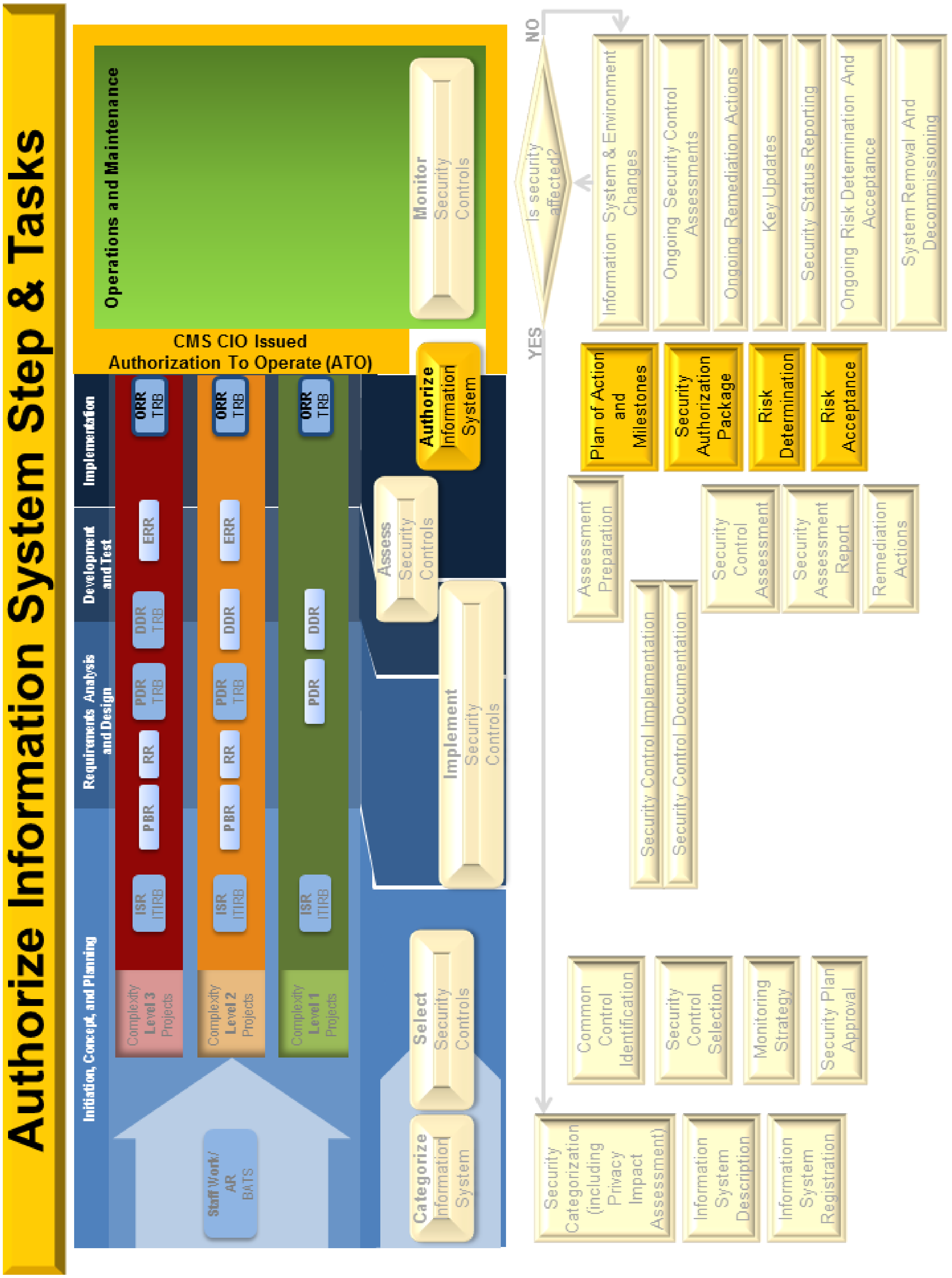
- *Plan of Actions and Milestones* (POA&M)
- *Security Authorization Package*
- *Risk Determination*
- *Risk Acceptance*

Chapter 6 of the RMH Volume I contains in-depth coverage of considerations and activities for these tasks.

Performance of the *Authorize Information System* step occurs entirely within the *Implementation Phase* of the XLC and, when successful, results in an ATO issued by the CMS Authorizing Official.

Figure 8 portrays the tasks of the *Authorize Information System* step as they occur within the XLC.

Figure 8 Authorize Information System


Authorize Information System Step & Tasks
Initiation, Concept, and Planning
Requirements Analysis and Design
Development and Test
Implementation
Operations and Maintenance
CMS CIO Issued Authorization To Operate (ATO)
Staff Work/ AR BATS
Complexity Level 3 Projects
Complexity Level 2 Projects
Complexity Level 1 Projects
ISR ITIRB
PBR
RR
PDR TRB
DDR TRB
ERR
ORR TRB
PDR
DDR
Categorize Information System
Select Security Controls
Implement Security Controls
Assess Security Controls
Authorize Information System
Monitor Security Controls
Is security affected?
NO
YES
Security Categorization (including Privacy Impact Assessment)
Information System Description
Information System Registration
Common Control Identification
Security Control Selection
Monitoring Strategy
Security Plan Approval
Security Control Implementation
Security Control Documentation
Assessment Preparation
Security Control Assessment
Security Assessment Report
Remediation Actions
Plan of Action and Milestones
Security Authorization Package
Risk Determination
Risk Acceptance
Information System & Environment Changes
Ongoing Security Control Assessments
Ongoing Remediation Actions
Key Updates
Security Status Reporting
Ongoing Risk Determination And Acceptance
System Removal And Decommissioning

5.5.1 PLAN OF ACTION AND MILESTONES

During the *Plan of Actions and Milestones* task, the business owner and/or the Common Control Provider, as appropriate, develops corrective action plans for identified weaknesses, complete with milestones and schedule completion dates, and enters and updates them in the POA&M. This POA&M contains current and historical information regarding the actions planned (and completed) to correct weaknesses in security controls and minimize residual risk associated with the information system (or common control). The POA&M must include each weakness found during the *Security Control Assessment* task, as well as any self-discovered weaknesses. The POA&M defines:

- Specific tasks to fix each weakness.
- The resources required for the tasks.
- The schedule for task completion.
- The status of each corrective action.

Development of the initial POA&M occurs during the *Implementation Phase* of the project. The POA&M is a living repository. It exists throughout the life of the system, as long as there are security control weaknesses, open findings from assessments or audits, or residual risks.

The Business Owner (or Common Control Provider for common controls) is responsible for this task. The system developer/maintainer and ISSO provide support. Typically:

- The Business Owner establishes priorities and provides funding to address the most significant first.
- The system developer/maintainer performs the tasks to remediate weaknesses found, following the established priorities and scheduling contained in the POA&M.
- The ISSO (or tasked support contractor) updates CFACTS regularly to track all POA&M items through milestone completion to complete remediation.

This positions CFACTS to provide continuous status of all POA&Ms to management.

Failure to complete the *Plan of Actions and Milestones* task on a timely basis increases risk to CMS, introduces delays in the risk determination process, and may even delay or prevent authorization of the system.

5.5.2 SECURITY AUTHORIZATION PACKAGE

NIST states:

> *The security authorization package contains: (i) the security plan; (ii) the security assessment report; and (iii) the plan of action and milestones.*

The NIST *security plan* includes the SSP, RA, CP, and CP Test (both the CP Test Plan and CP Test After Action Report). Because CMS uses the CFACTS automated tool, all of the information contained in these documents belongs in CFACTS. Once CFACTS contains all of the data, the Business Owner need only send a request for an ATO to the EISG to initiate the ATO process. This process is explained in the *Authorization to Operate Package Guide*, which is available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

The *Security Authorization Package* task occurs within the *Implementation Phase* of the project. It is dependent upon completion and entry of all documentation from all preceding tasks and steps of the NIST RMF into CFACTS.

The Business Owner (or Common Control Provider for common controls) is responsible for this task. The ISSO provides support.

Failure to submit a request for ATO on a timely basis will delay system authorization. Note: ATO processing requires submission of ATO request packages to the EISG at least 60 days prior to the required ATO date.[41] Project schedules should reflect this requirement.

5.5.3 RISK DETERMINATION

The *Risk Determination* task is the assessment of the current security posture of the system. It considers all control requirements, risk assessments, recommendations for addressing residual risks, and organizational risk implications. The final risk determination reflects the risk to CMS operations and assets, individuals, other organizations, and the nation resulting from use and operation of the information system.

The *Risk Determination* task occurs within the *Implementation Phase* and is completely dependent upon completion of all prior NIST RMF tasks and steps.

The EISG is responsible for this task. The CTO provides support.

Failure to perform the *Risk Determination* task on a timely basis can delay the project. This is commonly a result of not submitting the Security Authorization Package on a timely basis.

5.5.4 RISK ACCEPTANCE

Following the *Risk Determination* task, the CMS Authorizing Official will issue either an “Authorization to Operate” (ATO) or a “Denial of Authorization to Operate” (DATO). Granting an ATO occurs only if the risk to CMS associated with operating the system is acceptable. Risk deemed unacceptable to CMS results in a DATO that remains in effect until correction of all substantive weaknesses and the lowering of overall risk to CMS to acceptable levels.

Based on the determination of risk, the CMS Authorizing Official issues a formal document in the form of either an ATO or a DATO to the applicable business owner. Both of these documents contain conditions, some requiring action, and others prescriptive in nature.

Occasionally, the Authorizing Official permits a significant change to an existing system that has risk(s), normally deemed unacceptable to CMS, to operate for a short time due to enterprise business requirements. If this happens, the Authorizing Official issues an ATO for a limited time with the expectation of complete remediation of all risk(s) within this limited time to

[41] *CMS IS Authorization to Operate Package Guide*, which is available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

operate. **Note: If the weaknesses and vulnerabilities in the system are not mitigated, a formal DATO and rescission of the system's ATO results.**

The *Risk Acceptance* task occurs during the *Implementation Phase* of the project. The ATO is the security authorization for the system, or significant change to the system, to move into production.

The CMS Authorizing Official is responsible for this task. The CISO and CTO provide support.

5.6 MONITOR SECURITY CONTROLS

Execution of the *Monitor Security Controls* step occurs, on an ongoing basis, over the course of the rest of the system's life in the *Operations & Maintenance (O&M) Phase* of the XLC. The *Monitor Security Controls* step encompasses the following tasks:

- *Information System and Environment Changes*
- *Ongoing Security Control Assessments*
- *Ongoing Remediation Actions*
- *Key Updates*
- *Security Status Reporting*
- *Ongoing Risk Determination and Acceptance*
- *Information System Removal and Decommissioning*

An essential component of this step is the CMS Continuous Monitoring Program.[42] The goal of the CMS Continuous Monitoring Program is to satisfy Federal Information Security Management Act of 2002 (FISMA) and HHS mandates to reduce information security risk in a cost effective manner across the CMS enterprise by automation and standardization. As it is already defined and therefore required within the ARS, systems must have automated mechanisms in place to provide ongoing coverage and reporting capabilities within the required Asset Management, Continuous Monitoring, and Vulnerability Management domains.

The CMS Continuous Monitoring Program will facilitate standard and effective information-security data collection and dissemination and data-call response capabilities at both Federal and contractor operated data centers. The program will provide senior management and business owners with easy-to-understand information specific to individual FISMA systems, as well as across the enterprise (as applicable), that is consistent, measureable, accurate, and current.

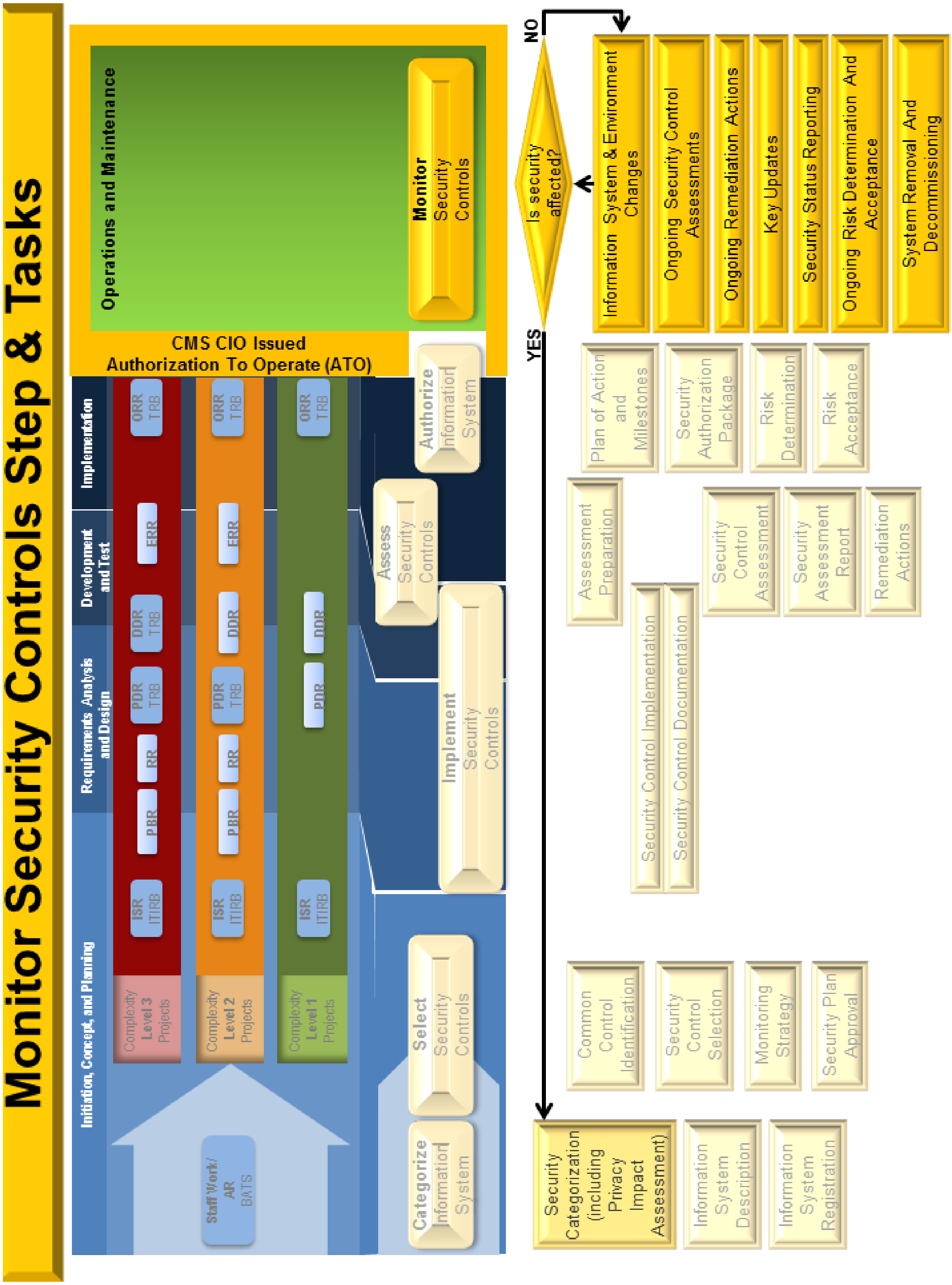
Performance of the *Monitor Security Controls* step occurs entirely within the *O&M Phase* of the XLC. **Please note: any changes that will affect the security state of the system require performance of all NIST RMF steps as part of the project that undertakes the changes.**

Chapter 7 of the RMH Volume I contains in-depth coverage of considerations and activities for these tasks.

Figure 9 portrays the tasks of the *Monitor Security Controls* step as they occur within the XLC.

[42] CMS *CIO Directive 11-02 – CMS Continuous Monitoring Program Implementation*

Figure 9 Monitor Security Controls


Monitor Security Controls Step & Tasks
Initiation, Concept, and Planning
Requirements Analysis and Design
Development and Test
Implementation
Operations and Maintenance
Staff Work/ AR BATS
Complexity Level 3 Projects
Complexity Level 2 Projects
Complexity Level 1 Projects
ISR ITIRB
PBR
RR
PDR TRB
DDR TRB
ERR
ORR TRB
PDR
DDR
CMS CIO Issued Authorization To Operate (ATO)
Monitor Security Controls
Categorize Information System
Select Security Controls
Implement Security Controls
Assess Security Controls
Authorize Information System
Is security affected?
NO
YES
Information System & Environment Changes
Ongoing Security Control Assessments
Ongoing Remediation Actions
Key Updates
Security Status Reporting
Ongoing Risk Determination And Acceptance
System Removal And Decommissioning
Security Categorization (including Privacy Impact Assessment)
Information System Description
Information System Registration
Common Control Identification
Security Control Selection
Monitoring Strategy
Security Plan Approval
Security Control Implementation
Security Control Documentation
Assessment Preparation
Security Control Assessment
Security Assessment Report
Remediation Actions
Plan of Action and Milestones
Security Authorization Package
Risk Determination
Risk Acceptance

5.6.1 INFORMATION SYSTEM AND ENVIRONMENT CHANGES

A key component of security and risk management is a disciplined and structured approach to managing changes to the system and its environment. Tracking and documenting the hardware, software, and firmware upgrades are required and performed as part of those upgrades. Changes made to systems must follow an orderly path with all security documentation updates occurring in lock step with the changes. Detection and correction of any unauthorized changes must be on a timely basis.

In addition, determining if a planned change is a significant change from the security/risk management perspective is a critical task that has risk, cost, and time implications for both the planned project and the enterprise. Understating the significance of the change (i.e., calling a significant change insignificant) can erode the effectiveness of security controls and create exposures where none existed. Overstating the significance creates excessive security assessments and needless expenditures.

It is during the *O&M Phase* of the XLC that the ongoing process of controlling information system and environmental changes occurs.

The Business Owner (or Common Control Provider for common controls) is responsible for this task. The ISSO, system maintainer, and system operator provide support. The CTO and the EISG provide guidance.

Failure to perform The *Information System and Environment Changes* task on an ongoing basis increases the risk level of systems and may expose the system and CMS to vulnerabilities and threats, both technical and legal.

5.6.2 ONGOING SECURITY CONTROL ASSESSMENTS

On an ongoing basis, a subset of security controls undergoes assessment each year (within every 365 days). The SAR issued by the assessor documents all assessment results. Results of assessments apply for current year FISMA reporting and accumulate over a three-year period for security authorization purposes. During any three-year period, each control must be assessed at least once. The CMS CISO may issue a list of controls to test each year to:

- Provide complete testing of each control across all systems and infrastructure.
- Detect any gaps in controls within the enterprise complex.

In addition, controls defined in each system’s monitoring strategy that require more frequent than triennial assessment may have additional assessments during years not designated by the CMS CISO.

NIST and CMS encourage the use of automated tools to achieve continuous monitoring of the environment and the effectiveness of security controls, where appropriate and effective. When employed, these tools provide a near real-time picture of the security status of these controls, providing a highly dynamic understanding of the risks faced by CMS.

Performance of the *Ongoing Security Control Assessments* task must occur at least annually (within every 365 days) during the *O&M Phase* of the XLC.

The Business Owner (or Common Control Provider for common controls) is responsible for this task. The ISSO, security control assessor, system maintainer, system operator, and the EISG provide support.

Failure to perform the *Ongoing Security Control Assessments* task on an ongoing basis increases the risk level of systems and may expose the system and organization to vulnerabilities and threats that could have been detected and mitigated.

5.6.3 ONGOING REMEDIATION ACTIONS

The *Ongoing Remediation Actions* task is continuous until the completion, verification, and closure of all corrective actions (POA&M milestones) for all weaknesses occurs. These actions must address weaknesses that pose the greatest level of risk to CMS, first. Remediation progress is entered into CFACTS regularly, thus keeping all POA&M milestone and weakness statuses current.

Correcting weaknesses may occur as part of the *Ongoing Security Control Assessment* task. Verification of weakness elimination is possible by retesting such fixes, which is highly desirable. Weaknesses corrected during the course of the assessment and documented within the final report have a *corrected during assessment* designation. This provides a complete picture of the status of enterprise risk, both before and after the assessment.

Remediation actions, completed at other times are designated *pending verification*. Supporting artifacts of the actions taken and proof of the testing performed must be present and have association with the weakness in CFACTS. Verification that remediation is complete occurs in a subsequent EISG review. During that review, if the actions are deemed appropriate and effective the weakness status is changed to *complete*. Otherwise, the ISSO is notified and the status will be changed to *ongoing* or *delayed*, as appropriate.

The *Ongoing Remediation Actions* task continues on an ongoing basis during the *O&M Phase* of the XLC.

The Business Owner (or Common Control Provider for common controls) is responsible for this task. The ISSO, system maintainer, system operator, security control assessor, and the EISG provide support.

Failure to perform the *Ongoing Remediation Actions* task on a continuous basis increases the risk level of systems and exposes the system and CMS to detected and real vulnerabilities and threats.

5.6.4 KEY UPDATES

The availability of accurate and timely information regarding the security state of each system is essential for achieving near real-time risk management, because it influences the security related decisions made by the CMS CISO, CIO, and other senior officials and the subsequent actions that result from those decisions. Key documents requiring updates include:

- Security Assessment Reports – updated as produced
- POA&M – updated monthly until closure of all open weaknesses

- Security Plan (including risk assessment) – updated as necessary to reflect current status of security controls, but reviewed no less than annually. **(Note: Annually means the activity is completed within every three hundred sixty-five (365) calendar days, but no later than three hundred seventy (370) days.)**
- Contingency Plan – updated as needed, but reviewed no less than once annually.
- Contingency Plan Test (Plan and After Action Report) – performed annually.

The *Key Updates* task is an ongoing process occurring during the *O&M Phase* of the XLC.

The Business Owner (or Common Control Provider for common controls) is responsible for this task. The ISSO provides support.

Failure to perform the *Key Updates* task accurately on an ongoing basis distorts senior management's understanding of the current risks faced by CMS. This may inhibit management's ability to take appropriate action on a timely basis when most needed.

5.6.5 SECURITY STATUS REPORTING

Results of monitoring activities are recorded and reported to the CMS CISO on an ongoing basis in accordance with the monitoring strategy and RMH procedures. The *Security Status Reporting* task is both event driven (e.g., when the information system or its environment of operations changes and the event of any compromise or breach of the system) and time driven (e.g., weekly, monthly, quarterly). These reports describe the monitoring activities employed by the business owner and/or Common Control Provider. Reports include vulnerabilities discovered in the security control assessment, security impact analysis, and security control monitoring and the plans for addressing such vulnerabilities. Timely updates made to the CFACTS can generate most of these reports.

Performance of the *Security Status Reporting* task is an ongoing process during the *O&M Phase* of the XLC to communicate to senior leaders the current state of security of the information system and its environment of operation with regard to operational missions and business functions.

The Business Owner (or Common Control Provider for common controls) is responsible for this task. The ISSO provides support.

Failure to perform the *Security Status Reporting* task accurately on an ongoing basis breaks the communication chain with senior leaders, thus decreasing their situational awareness of the security state of the system and placing them in a position of having to make decisions based on stale information, potentially involving unreported, but known risks.

5.6.6 ONGOING RISK DETERMINATION AND ACCEPTANCE

The CMS CISO reviews reported security status of the information system on an ongoing basis to determine the current risk associated with the information system to CMS operations, mission, and assets; individuals; other organizations; the nation; or its citizens. This includes periodic processes, such as the process of renewing an ATO. Because risks can be temporal, the ongoing process of determining how changes to the system and its environment of operation affects risk for CMS, the business process, and the information system is essential.

The *Ongoing Risk Determination and Acceptance* task occurs on an ongoing basis during the *O&M Phase* of the XLC to maintain each system's security authorization over time.

The CMS Authorizing Official is responsible for this task. The CISO and CTO provide support.

Failure to perform the *Ongoing Risk Determination and Acceptance* task on a timely and ongoing basis makes the organization's picture of risk fuzzy and may place the system's ATO in jeopardy.

5.6.7 INFORMATION SYSTEM REMOVAL AND DECOMMISSIONING

The *Information System Removal and Decommissioning* task addresses the activities performed at the end of a system's lifecycle to decommission the system and retire its data. These activities accomplish the appropriate disposal/disposition of hardware, software, and data. Development of an Information System Removal and Decommissioning Plan is the first activity. Execution of the plan follows with emphasis on ensuring that no security control gaps result from the decommissioning.

The *Information System Removal and Decommissioning* task begins during the *O&M Phase* of the XLC and ends after the system has been decommissioned.

The Business Owner is responsible for this task. The ISSO, EISG, and CTO provide support.

Failure to perform the *Information System Removal and Decommissioning* task properly can lead to unauthorized information disclosure, inappropriate records retention, and possibly violations of law.

6 PROCUREMENT

Procurement of goods and/or services may be done at any phase of the lifecycle and may span any number of phases. The information known about the project and the specificity of details will be different as the system progresses through life cycle phases. Because of these facts, both the enumerated requirements that any bid must satisfy and the expected deliverables for acquisition will vary.

Information security and assurance are requirements of FISMA[43] and CMSRs[44]. These requirements must be part of information systems and services contracts and purchases[45].

[43] FISMA, PL 107-347 is available at http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf.

[44] The *CMS Minimum Security Requirements (CMSR's)* are documented in appendices A through C, of the *CMS Acceptable Risk Safeguards (ARS)* and are available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

Evaluation of services and goods must include the evaluation of the ability of the service/product to meet security[46] and privacy[47] requirements. Each security and privacy requirement is non-negotiable. Meeting each requirement is mandatory for a system to enter production operations. **Please note: Accepting a bid from the lowest cost bidder who does not meet all security requirements implies further expenditures following the acquisition to correct missing or defective security requirements.** Some general parameters and expectations include:

- **Internet based service acquisitions must meet the Federal Risk and Authorization Management Program (FedRAMP) requirements via contractual provisions.**[48]
- Requests for work supporting the concept segment of the *Initiation, Concept, and Planning Phase* of a project must include statements of work (SOW) and deliverables that support the *Common Control Selection* (Section 5.2.1) and *Security Control Selection* (Section 5.2.2) tasks.
- Requests for work that includes activities in the planning segment of the *Initiation, Concept, and Planning Phase* of a project must include statements of work and deliverables for the *Monitoring Strategy* (Section 5.2.3) task and support for *Security Plan Approval* (Section 5.2.4) task.
- Any system or system service procurement involving requirements analysis, design, development, and testing will include a specific list of security requirements from the ARS. These individually enumerated requirements belong in the solicitation document, directly or via attachment to support the *Security Control Implementation* (Section 5.3.1) and *Security Control Documentation* (Section 5.3.2) tasks.
- Any system service procurement, where the length of the service will exceed one year, should have provision made to require support of evolving requirements. This stems from the fact that CMS security requirements derive from federal minimum requirements that are subject to change. On average, changes occur every two years.
- Acquisition of cloud computing services must be from a federally authorized vendor and in accordance with the *CMS Risk Management Handbook Vol. III Standard 3.2 CMS Cloud Computing Standard*.[49] Such vendors may already meet some of CMS's security requirements. Expect complete and specific articulation of the system specific requirements in the acquisition request. **Note: There will always be some system specific requirements.**
- Acquisitions of off the shelf software (COTS or GOTS) should include requirements for software assurance consistent with CMS misuse case testing requirements, in addition to security requirements.

[45] The *Federal Acquisition Regulation* (FAR) states in subsection 1.602-2 Responsibilities: *"Contracting officers shall- … (c) Request and consider the advice of specialists in audit, law, engineering, information security, transportation, and other fields, as appropriate."* The FAR is available at https://www.acquisition.gov/far/.
[46] The FAR, part 39, is available at https://www.acquisition.gov/far/.
[47] The FAR, subsection 24.103, is available at https://www.acquisition.gov/far/.
[48] FedRAMP is available at http://www.gsa.gov/portal/content/133675.
[49] The *CMS Risk Management Handbook Vol. III Standard 3.2 CMS Cloud Computing Standard* is available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

- Requests for hardware or hardware services at a non-CMS site should only originate from OIS with the approval of the CIO.

Chapter 8 of the RMH Volume I will provide more detailed guidance material for those directly involved in the procurement process.

7 GOVERNANCE AND REVIEWS

The CMS XLC provides for IT Governance, Technical Review Board, and project team reviews as key control points during various phases the XLC.[50] Note: usage of an alternate XLC does not eliminate responsibility to perform the stated reviews at the earliest point, consistent with those identified in this section. The NIST RMF introduces specific determinations needed at these key control points. From the risk management perspective, each control point is either a security path review or a security gate. The project team performs security path reviews to ensure the project is on course regarding security, privacy, and assurance. A review board performs security gates to ensure the project is on course, prevent the costliest mistakes, and enable the project to move forward efficiently to the next phase. In addition, security gates also identify *halt conditions*. These conditions define when a project must halt pending completion of specified risk management tasks.

> An analogy would be during new house construction at the time planned for wallboard installation. A *halt condition* would be completion of electrical and plumbing work. If the electrical and plumbing work is incomplete, proceeding with wall installation is a costly mistake because walls must be removed to complete and inspect the electrical and plumbing work. The alternative, delaying the start of wall installation, costs less and completes the house construction sooner.

This section contains a list of the NIST RMF determinations and associated questions to aid the determination, at each review point. In addition, security gates also identify the halt conditions that are appropriate for all projects. Table 5 lists each security gate, its XLC phase, and the related halt conditions.

Table 5 Security Gates

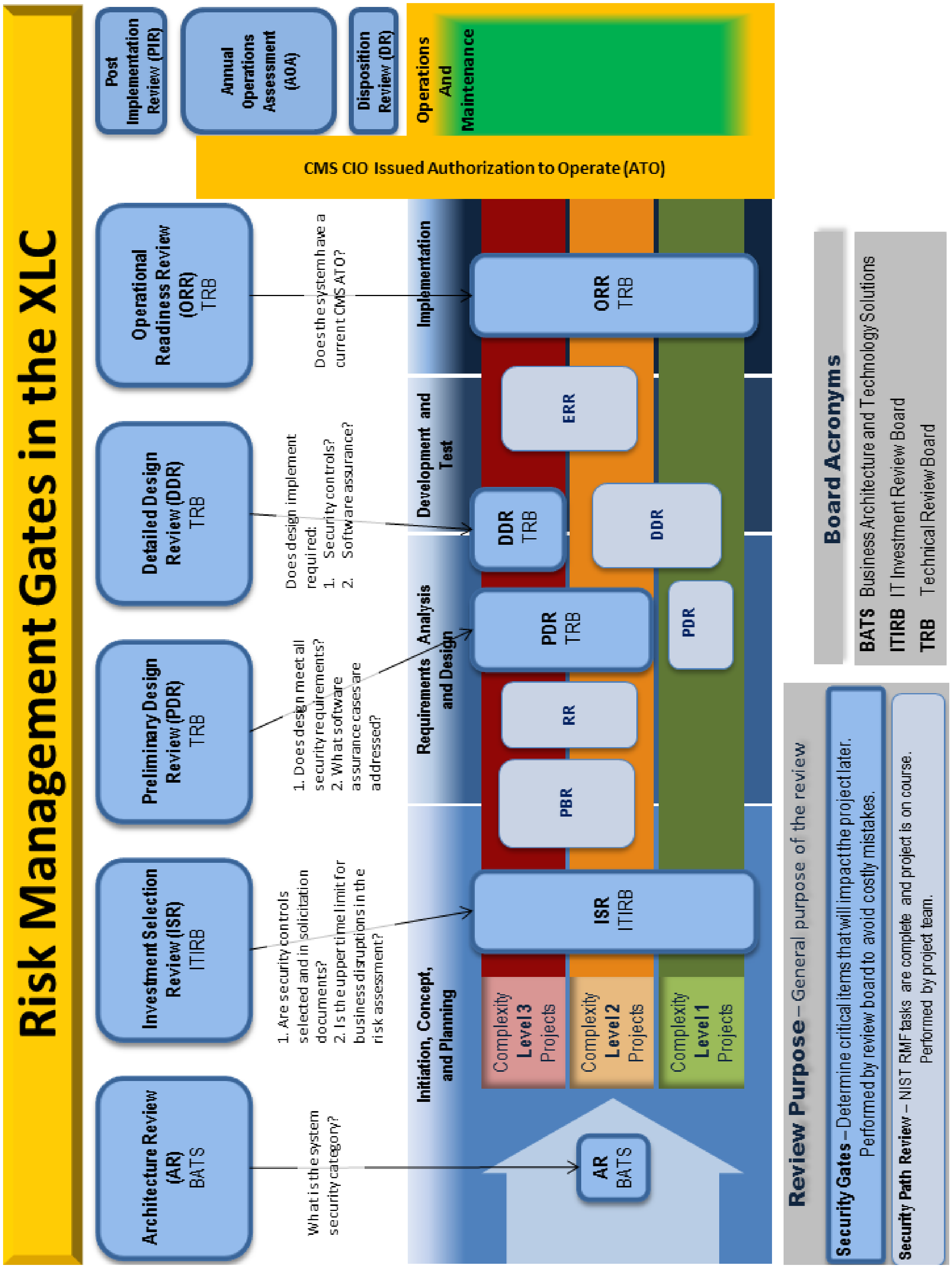
Security Gate	Halt Condition	XLC Phase
Architecture Review	System Security Category is not determined.	Initiation, Concept, and Planning
Investment Selection review	Security controls not defined or absent from solicitation documents.	
	Maximum tolerable period of business disruption is unknown.	
Preliminary Design Review	Not all security controls are in requirements.	Requirements Analysis and
	Assurance cases are missing from requirements.	

[50] The CMS XLC reviews and templates are available on the XLC Reviews & Templates web page, at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/Reviews.html.

Security Gate	Halt Condition	XLC Phase
Detailed Design Review	Security control design is incomplete.	Design
	Assessment case design is incomplete.	
Operational Readiness Review	System lacks a CMS ATO.	Implementation

Figure 10 contains a graphical representation showing the risk management security gates and halt condition determinations within the CMS XLC.

Figure 10   Risk Management Security Gates


Risk Management Gates in the XLC
Architecture Review (AR) BATS
Investment Selection Review (ISR) ITIRB
Preliminary Design Review (PDR) TRB
Detailed Design Review (DDR) TRB
Operational Readiness Review (ORR) TRB
Post Implementation Review (PIR)
Annual Operations Assessment (AOA)
Disposition Review (DR)
What is the system security category?
1. Are security controls selected and in solicitation documents?
2. Is the upper time limit for business disruptions in the risk assessment?
1. Does design meet all security requirements?
2. What software assurance cases are addressed?
Does design implement required:
1. Security controls?
2. Software assurance?
Does the system have a current CMS ATO?
CMS CIO Issued Authorization to Operate (ATO)
Initiation, Concept, and Planning
Requirements Analysis and Design
Development and Test
Implementation
Operations And Maintenance
Complexity Level 3 Projects
Complexity Level 2 Projects
Complexity Level 1 Projects
AR BATS
ISR ITIRB
PBR
RR
PDR TRB
PDR
DDR TRB
DDR
ERR
ORR TRB
Review Purpose – General purpose of the review
Security Gates – Determine critical items that will impact the project later. Performed by review board to avoid costly mistakes.
Security Path Review – NIST RMF tasks are complete and project is on course. Performed by project team.
Board Acronyms
BATS Business Architecture and Technology Solutions
ITIRB IT Investment Review Board
TRB Technical Review Board

7.1 ARCHITECTURE REVIEW

Halt Conditions:

- The security category of the proposed system, or system enhancement, is unknown.

  This condition arises because the *Categorizing an Information System* procedure was not performed. As a result, two (2) of the project characteristics (privacy implications and security implications) used to determine project complexity are unknown. Thus, the complexity level of the project cannot be determined. Additional potential project impacts include the inability to determine security requirements, missing security controls, and denial of an ATO until all controls are operating effectively.

  The remedy is to perform the *Categorizing an Information System* procedure immediately. The procedure is located at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html under the title *RMH Vol II Procedure 2-3 Categorizing and Information System*. Once complete, the project characteristics will be available for calculation of the project's complexity level.

Review Components

Determine that:

- The designated system security category is accurate.
- A maximum period of disruption is determined for the business process and documented in the risk assessment.

Key questions to answer are:

- Was a security categorization of the information system including the data processed, stored, and transmitted by the system completed?
- Are the results of the security categorization process for the information system consistent with CMS's enterprise architecture and commitment to protecting mission/business processes?

7.2 INVESTMENT SELECTION REVIEW

Halt Conditions:

- The security requirements are neither identified nor included in solicitation documents.

  Although there may be many causes for this condition, all result from a failure to follow the procedures and intent of the RMH and XLC. The immediate result is an understatement of work, cost, and time estimates for the project for each missing security requirement. The Project Process Agreement will understate the work needed. The cost and time to correct this deficiency rises with each succeeding XLC phase that passes while this condition is not resolved. Also, if these requirements are not included in solicitation documents: bids are underpriced, unplanned contract modifications can occur, and the system will not meet federal and CMS security and privacy requirements. The system without security controls that meet requirement will not receive an ATO.

- The maximum time of disruption that the business process can acceptably endure is not determined.

  This condition precludes Contingency Planning and definition of system availability requirements. This places the business process in jeopardy when unanticipated events cause unavailability of the system or its data. It is a significant cost consideration, because meeting different availability requirements represents a several fold increase in the ongoing cost of operating the system.

Review Components

Determine that:

- The maximum period of disruption for the business process is determined and documented in the risk assessment.
- Common controls are identified.
- Security control selection is complete.
- The list of security controls (to be acquired or developed) for the system is available for use in solicitation and contracting vehicles and project activities.

Key questions to answer are:

- Is the security category of the information system accurate?
- Is the allocation of all security controls (CMS Minimum Security Requirements) to the information system as system-specific, hybrid, or common controls complete?
- Is the list of security requirements available?
- Does the business risk assessment explain risks, define the maximum period of disruption as the MTD, and guide the process of system risk assessment?

7.3 PROJECT BASELINE REVIEW

Halt Conditions: Not Applicable to this review.

Review Components

Determine that:

- All planned controls are within the non-functional requirements documentation for the system.
- The continuous monitoring strategy documentation is complete.
- CFACTS contains complete information for:
  - System security category
  - Privacy Impact Assessment (PIA)
  - Information system description

  - System boundary
  - Business risks
  - Information system risks
  - CMS minimum security requirements that are appropriate for the system's security category
  - Identification and description of common controls and their provider(s)
  - Identification and description of the security controls requiring implementation
- System registration is complete

The key questions to answer are:

- Has the project team described all planned controls and included them as non-functional requirements of the system?
- Has the project team developed a continuous monitoring plan for the information system (including monitoring of security control effectiveness for system-specific, hybrid, and common controls) that reflects CMS's risk management strategy, continuous monitoring strategy, and commitment to protecting critical missions and business functions?
- Is the description of the characteristics of the information system adequate?
- Is registration of the information system complete for purposes of management, accountability, coordination, and oversight?
- Did the project team tailor and supplement the baseline security controls to ensure that the controls, if implemented, adequately mitigate risks to CMS operations and assets, individuals, other organizations, and the Nation?
- Has the project team established and documented minimum assurance requirements for the security controls employed within and inherited by the information system?
  - Assurance requirements are the activities and actions that the project team defines and applies to increase the level of confidence that the controls operate correctly, as intended, and produce the desired outcome with respect to meeting the security requirements for the information system.
  - Assurance requirements address the quality of the design, development, testing, and implementation of the security functions in the information system.
  - For higher-impact systems (i.e., potential high-value targets) in situations where specific and credible threat information indicates the likelihood of advanced cyber-attacks, additional assurance measures are considered.
- Has the project team checked when identifying common controls to ensure that the security capability provided by the inherited controls is sufficient to deliver adequate protection?
- Did the project team supplement common controls with system-specific or hybrid controls when the security control baselines of the common controls are at a lower security category than the information system inheriting the controls?
- Did the project team document any common controls inherited from external providers and review them with the EISG?

7.4 REQUIREMENTS ANALYSIS REVIEW

Halt Conditions: Not Applicable to this review.

Review Components

Determine that:

- Documentation for all controls (i.e., common controls, hybrid controls, and system-specific controls) is in CFACTS.
- Providers of the controls acknowledge their role and the inheritability of the specific controls.
- Business owner portions of hybrid controls are in the project requirements.
- System-specific controls are in the project requirements.
- The project employs sound information system and security engineering methodologies, as well as misuse cases.
- The controls required for projects are in place and effective.
- Software assurance misuse cases are defined for all forms of injection and memory mismanagement attacks.

Key questions to answer are:

- Is documentation readily available regarding the implementation of the common controls inherited by the information system?
- Has the project team documented the planned implementation of system-specific and hybrid security controls within the information system, taking into account specific technologies and platform dependencies?
- Did the project team take minimum assurance requirements into account when specifying/ implementing security controls?
- Does the project require the use of sound information system and security engineering methodologies in developing, testing, and integrating information technology products into the information system and in implementing the security controls contained in the security plan?
- Are control CM-4 and the entire SA family of controls in place and effective for this project?
- What misuse cases are defined?

7.5 PRELIMINARY DESIGN REVIEW

Halt Conditions:

- The design for the system does not account for all security requirements.

  This condition arises because incomplete specification of security requirements or incomplete design. As a result, required controls will not exist and there will be findings in the security control assessment. The design, development, testing, and integration of missing controls within the system are prerequisites to obtaining an ATO.

Adding the controls after subsequent XLC phases typically involves rework of system components that interface with each control and increases the total project cost and timeframe.

- Software assurance misuse cases are absent.

  This condition arises due to a failure to define the misuse cases for all forms of injection and memory mismanagement attacks during the requirements analysis segment of the *Requirements Analysis and Design Phase*.

Review Components

Determine that:

- Architectural designs are consistent with CMS architecture and security requirements.
- All security requirements are addressed in requirements and the preliminary design.
- Software assurance misuse cases are defined.

Key questions to answer are:

- Do the designs satisfy all security control requirements?
- Does the system boundary span architectures?
- Are the designated common controls and hybrid controls consistent with CMS architecture?
- Are misuse cases defined for all forms of injection and memory mismanagement attacks?

7.6 DETAILED DESIGN REVIEW

Halt Conditions:

- The system, as designed, does not implement all required security controls.

  This condition usually arises because incomplete specification or design of security requirements or environmental limitations. As a result, required controls will not exist and there will be findings in the security control assessment. The design, development, testing, and integration of missing controls within the system are prerequisites to obtaining an ATO.

  Adding the controls after subsequent XLC phases typically involves rework of system components that interface with each control and increases the total project cost and timeframe. In the case of incomplete specification or design, the project needs to incorporate the missing elements before proceeding further. In the case of environmental limitations, the project should immediately contact the CISO for help, which may include definition and implementation of a compensating control to counteract the weakness caused by the environment.

- Test plans for misuse cases are absent.

  This condition arises due to a failure to develop the plan to test and verify that defined misuse cases are not present in the system. Develop specific test plans for each misuse case prior to proceeding.

Review Components

Determine that:

- The architectural designs for all controls are complete, adequate, and consistent with CMS architecture and security requirements.
- All security requirements are addressed in requirements and the preliminary design.
- Software assurance misuse cases are defined.

Key questions to answer are:

- Do the designs satisfy all security control requirements?
- Does the system boundary span architectures?
- Are the designated common controls and hybrid controls consistent with CMS architecture?
- Are software assurance misuse case test plans developed for all forms of injection and memory mismanagement attacks?

7.7 ENVIRONMENTAL READINESS REVIEWS

7.7.1 VALIDATION READINESS REVIEW

Halt Conditions: Not Applicable to this review.

Review Components

Determine that developers tested:

- Misuse cases.
- All security controls (i.e., system-specific, hybrid, and common controls).

Key questions to answer are:

- Did developers perform testing?
- Was the testing sufficient to address all concerns?

7.7.2 IMPLEMENTATION READINESS REVIEW

Halt Conditions: Not Applicable to this review.

Review Components

Determine that:

- Misuse cases were thoroughly tested.
- All security controls were tested.
- CFACTS and security artifacts are updated and current.
- An independent security assessment schedule exists.

Key questions to answer are:

- Are the system-specific, hybrid, or common controls thoroughly tested and consistent with the enterprise architecture and information security architecture?
- Did the project employ sound information system and security engineering methodologies in integrating or developing the information system and in implementing the security controls contained in the SSP?
- Does CFACTS information describe the implementation of common controls inherited by the information system and system-specific and hybrid security controls contained within the information system, taking into account specific technical and platform dependencies?
- Do the implemented security controls meet established minimum assurance requirements?
- Were all system-specific and hybrid controls in the SSP tested (No planned controls remaining)?
- When will the security control assessment occur?

7.7.3 PRODUCTION READINESS REVIEW

Halt Conditions: Not Applicable to this review.

Review Components: Not Applicable to this review.

7.8 OPERATIONAL READINESS REVIEW

Halt Conditions:

- The system does not have a current CMS CIO issued ATO.

  Federal law mandates that all information systems have a current ATO signed by the designated authorizing official who, for CMS, is the CMS CIO. Without a current ATO, a system may not be placed into production, nor may it access production data.

Review Components

Determine that the system has a current CMS CIO issued ATO.

Key questions to answer are:

- Has the ATO letter been presented and reviewed?

7.9 POST IMPLEMENTATION REVIEW

Halt Conditions: Not Applicable to this review.

Review Components: Not Applicable for this review.

7.10 ANNUAL OPERATIONAL ANALYSIS REVIEW

Halt Conditions: Not Applicable to this review.

Review Components

Determine any new, changed or tested security requirements and report status.

Determine that effective ongoing monitoring is providing management with the information needed to achieve near real-time risk management.

Key questions to answer are:

- Will recent or planned changes to the information system and its environment of operation impact the effectiveness of deployed security controls?
- Have CMS Minimum Security Requirements for the information system(s) changed? If so, are the changes operational?
- Are the necessary remediation actions an ongoing activity to address identified weaknesses and deficiencies in the information system and its environment of operation?
- Is security status for the information system and its operational environment reported to authorizing officials and other designated senior leaders within the CMS?
- Are critical risk management documents updated based on this review and ongoing monitoring activities?
- Are responsible operating units effectively monitoring changes to the information system and its operational environment including the effectiveness of deployed security controls in accordance with the continuous monitoring strategy and continuous monitoring plans?
- Are responsible operating units effectively analyzing the security impacts of identified changes to the information system and its operational environment?
- Do responsible operating units conduct ongoing assessments of security controls in accordance with the monitoring plans?
- Are necessary remediation actions an ongoing activity used to address identified weaknesses and deficiencies in the information system and its operational environment?
- Is an effective process in place to report the security status of the information system and its environment of operation to the authorizing official and other designated senior leaders within CMS on an ongoing basis?
- Do critical risk management documents reflect ongoing monitoring activities?
- Are authorizing officials conducting ongoing security authorizations by employing effective continuous monitoring activities and communicating updated risk determinations and acceptance decisions to information system owners and Common Control Providers?

7.11 DISPOSITION REVIEW

Halt Conditions: Not Applicable to this review.

Review Components

Determine that:

- All equipment and media was properly disposed.
- All records archival requirements are met.

Key questions to answer are:

- What are the appropriate disposal procedures?
- What records must be archived?
- Does the project plan account for disposition requirements?
- Are all destruction certificates in order?

8 CROSSWALK BY XLC PHASES

This section is provided as an aid for project teams. It outlines the NIST RMF tasks that occur within a given phase of the XLC and relates NIST RMF information in other project documents. When tasks need to occur within a limited portion of an XLC phase that portion is identified as a segment. Document and phase references conform to the XLC framework. If referenced project documentation is not used within any given project, teams develop the security related information at the specified time, as there is no alternative source for the equivalent information. Referenced project documents may have content that expedites the RMF task or may contain information the RMF task creates.

Roles and responsibilities for NIST RMF tasks are in the task descriptions in Section 5 of this chapter. Table 6 shows XLC Phases and the NIST RMF steps and tasks that occur within them.

Table 6 XLC Phases and Associated NIST RMF Steps and Tasks

XLC Phase(s)	NIST RMF Step	NIST RMF Task
Initiation, Concept, and Planning	Categorize Information System	Security Categorization
Initiation, Concept, and Planning		Information System Description
Initiation, Concept, and Planning		Information System Registration
Initiation, Concept, and Planning	Select Security Controls	Common Control Identification
Initiation, Concept, and Planning		Security Control Selection
Initiation, Concept, and Planning		Monitoring Strategy
Initiation, Concept, and Planning		Security Plan Approval
Requirements Analysis and Design through Development and Test (includes Acquisition)	Implement Security Controls	Security Control Implementation

XLC Phase(s)	NIST RMF Step	NIST RMF Task
Requirements Analysis and Design through Development and Test (includes Acquisition)		Security Control Documentation
Development and Test	Assess Security Controls	Assessment Preparation
Implementation		Security Control Assessment
Implementation		Security Assessment Report
Implementation		Remediation Actions
Implementation	Authorize Information System	Plan Of Action And Milestones
Implementation		Security Authorization Package
Implementation		Risk Determination
Implementation		Risk Acceptance
Operations and Maintenance	Monitor Security Controls	Information System And Environment Changes
Operations and Maintenance		Ongoing Security Control Assessments
Operations and Maintenance		Ongoing Remediation Actions
Operations and Maintenance		Key Updates
Operations and Maintenance		Security Status Reporting
Operations and Maintenance		Ongoing Risk Determination And Acceptance
Operations and Maintenance		Information System Removal And Decommissioning

8.1 INITIATION, CONCEPT, AND PLANNING PHASE

8.1.1 INITIATION SEGMENT

Only one NIST RMF task occurs during the initiation segment of the *Initiation, Concept, and Planning Phase*:

- *Security Categorization* (see Section 5.1.1 for task description)

No project documents contain related information, at this time. RMH Volume II Procedure 2-3, *Categorizing an Information System*, contains the categorization procedure.

8.1.2 CONCEPT SEGMENT

The *Security Categorization* task must complete prior to commencing with the following NIST RMF tasks:

- *Information System Description* (see Section 5.1.2 for task description)
- *Information System Registration* (see Section 5.1.3 for task description)
- *Common Control Identification* (see Section 5.2.1 for task description)
- *Security Control Selection* (see Section 5.2.2 for task description)

Perform each of the tasks listed above serially due to dependency on the preceding task. All of these tasks must complete within the concept segment of the *Initiation, Concept, and Planning Phase*. Detailed explanations of the first two tasks will be in Chapter 2 of the RMH Volume I. The others will be in Chapter 3.

The following XLC documents may contain useful information for, or consume it from, the *Information System Description* task:

- High Level Technical Design
- Business Case
- Requirements Document (overview)

At the completion of the *Security Control Selection* task, security information for common controls, system-specific controls, software assurance, and business risk is available for inclusion in the following XLC deliverables:

- Requirements Document (global standards security section and Software Assurance section)
- High Level Technical Design
- Project Management Plan
- Project Charter
- Project Process Agreement
- Business Case

8.1.3 PLANNING SEGMENT

During the planning segment of the *Initiation, Concept, and Planning Phase*, completion of two NIST RMF tasks is a requirement. These are:

- *Monitoring Strategy* (see Section 5.2.3 for task description)
- *Security Plan Approval* (see Section 5.2.4 for task description)

Detailed explanations of these tasks will be in Chapter 3 of the RMH Volume I. The *Monitoring Strategy* task identifies how the business owner proposes to monitor appropriate controls throughout the project and on an ongoing basis after implementation of the system. Upon completion of the *Monitoring Strategy* task, CFACTS will have sufficient information to produce an initial SSP for approval.

At the conclusion of the *Monitoring Strategy* task, information regarding the monitoring done during the system acquisition process is available for placement in the *Project Management Plan*[51] or one of its subordinate plans. At the end of the *Security Plan Approval* task, information detailing the planned system-specific security requirements is available for inclusion in:

- Acquisition requests
- Contracts
- Statements of Work

8.2 REQUIREMENTS ANALYSIS AND DESIGN PHASE

8.2.1 REQUIREMENTS ANALYSIS SEGMENT

During the requirements analysis segment of the *Requirements Analysis and Design Phase*, two NIST RMF tasks are starting:

- *Security Control Implementation* (see Section 5.3.1 for task description)
- *Security Control Documentation* (see Section 5.3.2 for task description)

Detailed explanations of these tasks will be in Chapter 4 of the RMH Volume I. Each planned security requirement in the approved security plan is analyzed and the associated control statements are developed. The control statements are entered into CFACTS. Work on the contingency plan begins in this phase.

When reviewing non-automatable controls, pay careful attention to the potential interaction with implied system features that may be necessary to support the control. For example, the process for reviewing audit logs may require a review once a week, but the capability to capture and report audit events may not exist within the system or its environment of operation.

In addition, identification of specific misuse cases for software assurance purposes avoids having weaknesses created within the software. Specific weaknesses to address include injection attacks (including all forms of cross-site scripting, SQL injection, format string problems, command injection, and reflection injection) and memory management attacks (including buffer overflow, buffer underflow, and stack mismanagement).

The *Requirements Document* and the *Test Plan* are updated to include documentation of each analyzed security control, control enhancement, and misuse case. **Note: Testing is mandatory for these items.**

[51] The CMS XLC artifacts are available on the XLC Artifacts and Templates web page, at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/Artifacts.html.

8.2.2 DESIGN SEGMENT

During the design segment of the *Requirements Analysis and Design Phase*, two NIST RMF tasks continue. These are:

- *Security Control Implementation* (see Section 5.3.1 for task description)
- *Security Control Documentation* (see Section 5.3.2 for task description)

Detailed explanations of these tasks will be in Chapter 4 of the RMH Volume I. The design and associated documentation for each analyzed system-specific control and system-specific portion of each hybrid control becomes final during the design segment of the *Requirements Analysis and Design Phase*.

The information system portion of the risk assessment begins early in this phase because these risks both influence and result from system design. Except for discovery of new threats and vulnerabilities, this portion of the RA is complete by the end of this phase.

The design of non-automatable controls requires looking ahead to how the system will operate when it is complete. Designs for control procedures should dovetail with the technical and architectural components of the system. For example, work on the contingency plan continues in this phase. Backup plans for the system and its data and recovery strategies become final. This includes the backup methodologies to be employed, frequency of backups, and identification of alternate recovery sites. Parallel activities on the mission/business process tier of the risk hierarchy deal with the business continuity aspects of these plans, often addressed outside the scope of the project.

Specification of test case scripts for all misuse cases, each designed system-specific control, and system-specific portion of each hybrid control occurs in this phase. Test case specification documentation belongs in the *Test Case Specification* artifact of the XLC when that artifact is used.

8.3 DEVELOPMENT AND TEST PHASE

8.3.1 DEVELOPMENT SEGMENT

During the development segment of the *Development and Test Phase*, two NIST RMF tasks continue. These tasks are:

- *Security Control Implementation* (see Section 5.3.1 for task description)
- *Security Control Documentation* (see Section 5.3.2 for task description)

Detailed explanations of these tasks will be in Chapter 4 of the RMH Volume I. The development and associated documentation for each analyzed system-specific control and system-specific portion of each hybrid control occurs during the development segment of the *Development and Test Phase*. Development of automatable security controls occurs in accordance with the design specifications from the *Requirements Analysis and Design Phase* and guided by the misuse cases. Developer testing includes tests of all misuse cases, each designed system-specific control, and system-specific portion of each hybrid control. Note: The test case specification documentation is in the *Test Case Specification* artifact of the XLC, when that artifact is used.

Development of manual security controls occurs in accordance with both the information provided during the Requirements Analysis and Design Phase and published CMS security procedures. The development team needs to exercise close coordination to make sure the automatic and manual controls conform to achieve the necessary protections. Completion of the contingency plan occurs during this phase.

8.3.2 TEST SEGMENT

Completion of two NIST RMF tasks occurs during the test segment of the *Development and Test Phase.* These tasks are:

- *Security Control Implementation* (see Section 5.3.1 for task description)
- *Security Control Documentation* (see Section 5.3.2 for task description)

Detailed explanations of these tasks will be in Chapter 4 of the RMH Volume I. Complete testing of security controls (system-specific, hybrid, and common controls) and each misuse case occurs during the test segment of the *Development and Test Phase*. This includes the Contingency Plan Test and CP Test Report. Misuse cases will have testing logs and documentation separate from but imported to CFACTS.

The XLC artifact *Test Summary Report* contains the results of testing.

One additional NIST RMF task occurs during the test segment of the *Development and Test Phase*. This is:

- *Assessment Preparation* (see Section 5.4.1 for task description)

Detailed explanation of this task will be in Chapter 5 of the RMH Volume I. The *Assessment Preparation* task of the NIST RMF starts in the *Development and Test Phase*. In this task, the security assessor develops a plan for assessing all security controls. The assessor will also plan to review all misuse case testing. **Note: Performing the Assessment Preparation task in the Development and Test Phase reduces potential delays in system migration to production operations during the Implementation Phase.**

8.4 IMPLEMENTATION PHASE

During the *Implementation Phase,* seven (7) NIST RMF tasks from two (2) NIST RMF steps occur. These tasks will culminate in the *Risk Acceptance* task. From the *Risk Acceptance* task either an ATO, allowing the system to move into production, or a DATO, requiring completion of corrective actions prior to reconsideration of risk, issues. The tasks are:

- *Security Control Assessment* (see Section 5.4.2 for task description)
- *Security Assessment Report* (see Section 5.4.3 for task description)
- *Remediation Actions* (see Section 5.4.4 for task description)
- *Plan of Action and Milestones* (see Section 5.5.1 for task description)

- *Security Authorization Package* (see Section 5.5.2 for task description)
- *Risk Determination* (see Section 5.5.3 for task description)
- *Risk Acceptance* (see Section 5.5.4 for task description)

Detailed explanations of the first three of these tasks will be in Chapter 5 of the RMH Volume I. The last four will be in Chapter 6.

8.5 OPERATIONS & MAINTENANCE PHASE

The *O&M Phase* is where the system will spend most of its lifetime. There are seven NIST RMF tasks within the *O&M Phase*, six of which occur on a continuous and/or cyclical basis. The seventh task starts during this phase in preparation for disposal of the system, which will happen during the *Operations and Maintenance Phase*. The tasks are:

- *Information System and Environment Changes* (see Section 5.6.1 for task description)
- *Ongoing Security Control Assessments* (see Section 5.6.2 for task description)
- *Ongoing Remediation Actions* (see Section 5.6.3 for task description)
- *Key Updates* (see Section 5.6.4 for task description)
- *Security Status Reporting* (see Section 5.6.5 for task description)
- *Ongoing Risk Determination and Acceptance* (see Section 5.6.6 for task description)
- *Information System Removal and Decommissioning* (see Section 5.6.7 for task description)

Detailed explanations of these tasks will be in Chapter 7 of the RMH Volume I. A major consideration during the *O&M Phase* is controlling changes to the system and monitoring status on an ongoing basis. This includes evaluating proposed changes to determine if they constitute a *significant* change to the system from a security/risk perspective.

Even when there are no changes to the system or its environment of operation, information system-related security risks can appear and risk impact levels can change. Both internal and external factors that are either planned or unplanned have influence. Some examples include:

- Sharing of information with new systems or organizations
- New threats to attack the system through known or unknown flaws
- Escalated threat levels from known sources
- Obsolescence of software or hardware upon which the system relies
- Natural and manmade disasters

The ongoing processes of assessment, remediation, updating security documentation, and reporting status provide the information necessary to determine the current risk and provide for the continuing authorization of the information system at an acceptable level of risk to CMS.

The final stage of the system's life involves the *Information System Removal and Decommissioning* task. Disposal and cleanup follows a disposition plan. The disposition plan derives from ARS requirements and applicable federal law, regulation, guidance, and executive order. At the end of this phase, a post disposition review occurs. Publication of a final disposition report that includes all lessons learned follows. Effectively, this is the end of the system. However, certain legal requirements for maintaining records exist and appropriate provision for such occurs in this phase.

9 GLOSSARY AND ACRONYMS

The glossary for this document and all other CMS information security and risk management documents is contained in Chapter 10 of RMH Volume I, *CMS Risk Management Terms, Definitions, and Acronyms*. The document is available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

10 APPROVED

teresa.fryer
@cms.hhs.g
ov

Digitally signed by teresa.fryer@cms.hhs.gov
DN: cn=teresa.fryer@cms.hhs.gov
Date: 2012.12.17 13:47:30 -05'00'

Teresa Fryer
CMS Chief Information Security Officer and
Director, Enterprise Information Security Group

This document will be reviewed periodically, but no less than annually, by the Enterprise Information Security Group (EISG), and updated as necessary to reflect changes in policy or process. If you have any questions regarding the accuracy, completeness, or content of this document, please contact the EISG at mailto:ciso@cms.hhs.gov.