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 III
Standard 7.2

Security Impact Analysis

FINAL
Version 1.0
June 25, 2014

Document Number: CMS-CISO-2014-vIII-std7.2

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN VOLUME III, STANDARD 7.2, *SECURITY IMPACT ANALYSIS* VERSION 1.0, DATED JUNE 25, 2014

1. Baseline Version.

(This Page Intentionally Blank)

TABLE OF CONTENTS

LIST OF TABLES

(This Page Intentionally Blank)

1 INTRODUCTION

1.1 PURPOSE

A *Security Impact Analysis (SIA)* is the analysis conducted by an organizational official to determine the extent to which changes to the information system will affect the security state of the system. These analyses are conducted as part of the *System Development Lifecycle (SDLC)* to ensure that security and privacy functional (and nonfunctional) requirements are identified and addressed during the development and testing of the system. The purpose of the SIA is to identify impacts of proposed system changes in order to develop additional security *design requirements* necessary to minimize the impact of proposed system changes.

At the Centers for Medicare & Medicaid Services (CMS), the SDLC requirements are addressed in the CMS *eXpedited Life Cycle (XLC)* processes[1]. The use and approval of a *Configuration (or Change) Control Board (CCB)* is required by both the *Acceptable Risk Safeguards (ARS)* manual control requirement CM-3, *Configuration Change Control*, and the *CMS Policy for Configuration Management*[2] (CM Policy). Both the ARS and the CM Policy require that the CCB analyze and evaluate changes to each information system to determine potential security impacts prior to change implementation, and that activities associated with configuration changes to the information system are authorized and audited. This requirement is specified and addressed in the ARS control requirements by ensuring that the organizational change/ configuration control processes both require and perform SIAs to identify any security impacts to proposed system changes.

What *is* the Purpose of an SIA

- An SIA helps planners, designers, and developers to identify potential risk areas (*real* and *possible*) of a proposed change.
- An SIA helps planners, designers, and developers to develop *effective* safeguards (design requirements) to address identified potential risks.
- An SIA helps planners, designers, and developers to develop effective security and privacy *testing*, to integrate into overall testing, prior to promotion of changes into a Production environment.

What *is Not* the Purpose of an SIA

- An SIA **does not** *waive* or *bypass* minimum Federal, Department, or CMS security or privacy control requirements required in the ARS, the CMS *Risk Management Handbook*

[1] The *CMS eXpedited Life Cycle Process: Detailed Description*, is available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/Downloads/XLC-DDD.pdf.
[2] The *CMS Policy for Configuration Management* is available at https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/SystemLifecycleFramework/downloads/cmpolicy.pdf.

(RMH), or other CMS or Department of Health and Human Services (HHS) Policies or procedures.

- An SIA **does not** *waive* CCB or XLC minimum requirements or Policies, and does not *bypass* required CCB or XLC phases or steps.
- Completion of an SIA **does not** *absolve* systems of identified (or unidentified) security or privacy deficiencies.
- An SIA **is not** a *"Risk Acceptance"* of identified (or unidentified) security or privacy deficiencies.

2 SECURITY IMPACT ANALYSIS

2.1 SIA AND THE XLC

For new systems *and* systems undergoing modifications, an SIA is started before the *Requirements Analysis* phase of the XLC (*Planning* phase) for a given change. The results of the SIA are presented to the change control processes and the *Technical Review Board (TRB)* at the earliest available stage review.

The overall SIA process, depending on the applicable CCB process, and embraces the following (See CM-3, SA-3, SA-15, and associated *change control* requirements):

1. The Business Owner organization determines that the system requires a change. (*Concept Phase*, see SA-3, and CM-9).
2. The Business Owner organization (or their empowered System Maintainer) develops a high-level plan for how to accomplish the change (*Concept, Planning Phase*, see SA-3, and SA-10).
3. The Business Owner organization (or their empowered System Maintainer) conducts an SIA to identify the security impacts of their plan (*Planning, Requirements Analysis Phase*, see CM-4 and SA-3).
4. The Business Owner organization (or their empowered System Maintainer) develops any applicable design requirements to mitigate the identified security impacts (*Requirements Analysis Phase*, see SA-3, SA-8, and SA-17).
5. The Business Owner organization (or their empowered System Maintainer) develops testing requirements to ensure that that the security impacts are verified as successfully mitigated (*Requirements Analysis, Design Phase*, see CA-2 and SA-11).
6. The Business Owner organization (or their empowered System Maintainer) builds out the system changes (*Development Phase*).
7. The Business Owner organization (or their empowered System Maintainer) test (*independently* as required by CA-2(1) and CA-7(1)) the system changes (using the security tests developed in step 5.) (*Test Phase*, see AC-5.Std.5, CA-2, CM-3(2), CM-4(1), and SA-11).

8. The Business Owner organization (or their empowered System Maintainer) develops and implements any Plans of Action and Milestones (POA&Ms) necessary to correct identified failures from testing (*Development, Test Phase*, see CA-5).

9. The Business Owner either applies for a *new* Authorization To Operate (ATO), or an ATO *update*. (*Implementation Phase*, see CA-6).

2.2 SIA AND THE CONTINUOUS MONITORING PROCESS

The continuous monitoring program includes an ongoing assessment of security control effectiveness to determine if there is a need to modify or update the current deployed set of security controls based on changes in the information system or its environment of operation. In particular, the organization revisits, on a regular basis, the risk management activities prescribed in the *CMS Risk Management Framework (RMF)*[3] and the CMS XLC. In addition to the ongoing activities associated with the implementation of the RMF, there are certain events which can trigger the immediate need to assess the security state of the information system and if required, modify or update the current security controls. These events include, for example:

- An *incident*[4] results in a compromise of the information system, producing a loss of confidence by CMS in the confidentiality, integrity, or availability (CIA) of information processed, stored, or transmitted by the system. (See ARS requirement CA-6.)
- A newly identified, credible, information system-related *threat* to CMS operations and assets, individuals, other organizations, or the Nation, is identified based on intelligence information, law enforcement information, or other credible sources of information. (See ARS requirement CA-6.)
- Changes to the configuration of the information system through the removal or addition of new (or upgraded) hardware, software, firmware, user roles, or changes in the operational environment potentially degrade the security state of the system. (See ARS requirement CA-6.)
- Changes to the CMS risk management strategy, information security policy, supported missions, and/or business functions, or information being processed, stored, or transmitted by the information system. (See ARS requirement CA-6.)

2.3 EFFECTS OF CHANGE ON THE ATO

2.3.1 CONFIGURATION (CHANGE) MANAGEMENT

Information systems are in a constant state of change with upgrades to hardware, software, or firmware and modifications to the surrounding environments where the systems reside and

[3] For a full description of the *CMS Risk Management Framework*, see RMH Volume I, Chapter 1, *Risk Management in the XLC*, available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VI_Risk_Management_XLC.pdf.
[4] *Incidents* are defined (and explained) in RMH Volume III, Standard 7.1, *Incident Handling*, available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VIII_7-1_Incident_Handling_Standard.pdf.

operate. A disciplined and structured approach to managing, controlling, documenting, testing, and monitoring changes to an information system or its environment of operation is an essential element of an effective security control monitoring program.

Strict configuration management and control processes are established in the ARS, the XLC, and the CM Policy to support such monitoring activities. It is important to record any relevant information about specific changes to hardware, software, or firmware such as version or release numbers, descriptions of new or modified features/capabilities, and security implementation guidance. It is also important to record any changes to the environment of operation for the information system (e.g., modifications to hosting networks and facilities, mission/business use of the system, threats), or changes to the organizational risk management strategy, tolerance-level, or overall risk posture.

The information system business owner (and in many cases, common control providers) use this information in assessing the potential security impact of the system changes. Documenting proposed or actual changes to an information system or its environment of operation, and subsequently assessing the potential impact those changes may have on the security state of the system, *or other CMS systems*, is an important aspect of security control monitoring. Information system changes should not be undertaken prior to assessing the security impact of such changes. If the results of the security impact analysis indicate that the proposed or actual changes can affect, or have affected, the security state of the system; then corrective actions must be initiated *and* appropriate documents are revised and updated (e.g., the security plan, security assessment report, and plan of action and milestones, etc.).

The terms and conditions for the system ATO provide a description of any specific limitations or restrictions placed on the operation of the information system, or inherited controls, that must be followed by the business owner or common control provider in order to *maintain* the ATO granted. An authorization termination date, established by the Chief Information Officer (CIO), indicates when the security authorization expires. The maximum period of time that a full ATO remains valid for a CMS information system is three (3) years, provided certain conditions are met (i.e., a comprehensive and ongoing continuous monitoring program), and there are no significant changes to the system, or its security posture during the ATO period.

The information business owner, or common control provider(s) should consult with the Enterprise Information Security Group (EISG) (via the TRB review process of the XLC) *prior* to implementing any security-related changes to the information system, or its environment of operation. The SIA should be performed *before* this consult.

After the changes are approved via the appropriate CCB and XLC processes, the changes must be implemented *and tested* as required by the ARS requirements CA-2, CM-3(2), CM-4(1), SA-11, and a corresponding *Security Assessment Report (SAR)* must be completed.

The CIO uses the revised and updated security assessment report, in collaboration with the Chief Information Security Officer (CISO), to determine if a formal reauthorization action is necessary. Many routine changes to an information system or its environment of operation can be handled by the organization's continuous monitoring program, thus supporting the concept of near-real-time risk management. Conducting security impact analyses is part of the ongoing assessment of risk.

Significant changes require a formal reauthorization of the system. If a formal reauthorization action is required, the business owner should target only the specific security controls affected by the changes and reuse previous assessment results wherever possible. Most routine changes to an information system or its environment of operation can be handled by the business owner's continuous monitoring program. An effective monitoring program can significantly reduce the overall cost and level of effort of reauthorization actions.

2.3.2 SIGNIFICANT CHANGE

The National Institute of Standards and Technology (NIST) 800-37 R1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, says that *Significant Change* to an information system may include (for example): (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 for example: (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 being targeted by a threat source; or (iv) establishing new/modified laws, directives, policies, or regulations.[5]

Changes that affect the approved security posture should be tracked through the applicable system Configuration (Change) Management and XLC/CCB processes.

However, note that *"significant"* vs. *"not-significant"* does not dramatically change the overall *process* that must be followed for any proposed system changes. *All* system changes must be *tested* to ensure that the changes have not negatively impacted the overall system (and enterprise) security posture. The real difference between *"significant"* vs. *"not-significant"* is mostly seen in the *amount* of testing required to ensure that the implemented changes have *not* made the system less secure.

Many events can trigger change—*even* events that may not result in an actual system *"change"*. Table 1 below lists many of these trigger events that occur at CMS, and the likely minimum required actions for each.

[5] The examples of changes listed are only *significant* when they meet the threshold established in the definition of significant change (i.e., *a change that is likely to affect the security state of the information system*).

(This Page Intentionally Blank)

Table 1 Events as Triggers of Change

Events			Actions	
Trigger	**Type of Event**	**Nature of Event**	**Type of Change**	**Notes**
Policy/ Standards	New Revision of ARS	No addition or change to existing controls	Minor Change	Likely not necessary to perform a full system authorization. However, new and modified control implementations must be tested as part of the Configuration (Change) Management processes.
Time	No ATO exists	ATO has Expired for system	System is Non-Compliant	Get a full system ATO. No system should be operating without an ATO.
Time	No ATO exists	ATO does not exist for system	System is Non-Compliant	Get a full system ATO. No system should be operating without an ATO.
Environ.	System boundary	ATO Expired for host GSS	System is Non-Compliant	GSS get a full system ATO. Supported systems are not in compliance.
Environ.	System boundary	No ATO for host GSS	System is Non-Compliant	GSS get a full system ATO. Supported systems are not in compliance.
Change	Security Classification	Security Category lowered	Possible Significant Change	Likely not necessary to perform a full authorization—unless security control implementations are modified. New and modified control implementations must be tested as part of the Configuration (Change) Management processes.
Change	Mission/Business requirements	New Mission added	Possible Significant Change	Likely not necessary to perform a full authorization. However, pay particular attention to changes in user roles and/or data types. New and modified control implementations must be tested as part of the Configuration (Change) Management processes.
Change	Mission/Business requirements	Cessation of mission or function.	Possible Significant Change	Likely not necessary to perform a full authorization—unless security control implementations are modified. New and modified control implementations must be tested as part of the Configuration (Change) Management processes.

Events			Actions	
Trigger	**Type of Event**	**Nature of Event**	**Type of Change**	**Notes**
Change	Equipment Upgrades	Laptops/desktops	Possible Significant Change	If the equipment is updated with similar vendor and models, then minimal testing may be needed. However, if the equipment is new models or vendors, with different configurations and settings, then it is considered a significant change. Equipment will need to be hardened, and at minimum, have vulnerability and configuration scans performed on them.
Change	Equipment Upgrades	Communications Equipment	Possible Significant Change	If the equipment is updated with similar vendor and models, then minimal testing may be needed. However, if they are new models or vendors, with different configurations and settings, then it is considered a significant change. Equipment will need to be hardened, and at minimum, have vulnerability and configuration scans performed on them.
Change	Equipment Upgrades	Other Equipment	Possible Significant Change	If the equipment is updated with similar vendor and models, then minimal testing may be needed. However, if they are new models or vendors, with different configurations and settings, then it is considered a significant change. Equipment will need to be hardened, and at minimum, have vulnerability and configuration scans performed on them.
Change	Major system Updates	New OS release	Possible Significant Change	If the software is updated with similar vendor and versions, then minimal testing may be needed. However, if they are significantly different versions (i.e.., not an “incremental version update”) or different vendors, with different configurations and settings, then it is considered a significant change. Affected systems will need to be hardened and, at minimum, have vulnerability and configuration scans performed on them.
Change	Major system Updates	New Anti-Malware Product	Possible Significant Change	If the software is updated with similar vendor and versions, then minimal testing may be needed. However, if they are significantly different versions (i.e.., not an “incremental version update”) or different vendors, with different configurations and settings, then it is considered a significant change. Affected systems will need to be hardened and, at minimum, have vulnerability and configuration scans performed on them.

Events			Actions	
Trigger	**Type of Event**	**Nature of Event**	**Type of Change**	**Notes**
Change	Patch Updates	Software	Possible Significant Change	Software patch updates that cause the baseline configuration, or security controls implementations, to change will need a re-authorization. All Software upgrades need to be tested pre-launch to prevent any issues. Affected systems will need to be hardened and, at minimum, have vulnerability and configuration scans performed on them.
Change	Patch Updates	Servers	Possible Significant Change	Server patch updates that cause the baseline configuration, or security controls implementations, to change will need a re-authorization. All Software upgrades need to be tested pre-launch to prevent any issues. Affected systems will need to be hardened and, at minimum, have vulnerability and configuration scans performed on them.
Change	System boundary	Changed Interconnections	Possible Significant Change	ISA update(s) required. New and modified control implementations must be tested as part of the Configuration (Change) Management processes.
Change	System boundary	Architecture or Topological Change	Possible Significant Change	This is likely a significant change because it changes the overall system design. New and modified control implementations must be tested as part of the Configuration (Change) Management processes.
Change	System boundary	Change to Logical Access Points	Possible Significant Change	Vulnerability scan is required
Environ.	Core Mission/ Business functions	Changes	Significant Change	Significant Change. Full ATO needed.
Environ.	Laws, Regulations, Directives	New or Changed	Possible Significant Change	Determine if the requirements of new or changed laws, regulations, and directives affect the security state of the system. New and modified control implementations must be tested as part of the Configuration (Change) Management processes.
Policy/ Standards	Issue or Update Other NIST Documents	New or Changed	Possible Significant Change	If new documentation changes the need for security controls or baseline configuration then a re-authorization is necessary. New and modified control implementations must be tested as part of the Configuration (Change) Management processes.

Events			Actions	
Trigger	**Type of Event**	**Nature of Event**	**Type of Change**	**Notes**
Risk	Vulnerability (New or Existing)	Attacks Developed	Risk Level Evaluated	Risk Assessment update, additional work as required. New and modified control implementations must be tested as part of the Configuration (Change) Management processes.
Risk	Vulnerability (New or Existing)	Attacks Succeed Elsewhere	Risk Level Evaluated	Risk Assessment update, additional work as required. New and modified control implementations must be tested as part of the Configuration (Change) Management processes.
Risk	Vulnerability (New or Existing)	Found (No Attacks Known)	Risk Identified	Add to Risk Assessment. New and modified control implementations must be tested as part of the Configuration (Change) Management processes.
Change	Security Classification	Security Category Raised	Significant Change	Add and modify security and privacy controls as appropriate. New and modified control implementations must be tested as part of the Configuration (Change) Management processes. Obtain a new/ updated ATO.
Change	Mission/Business Requirements	Change of Status Regarding Mission Essential Functions	Significant Change	New and modified control implementations must be tested as part of the Configuration (Change) Management processes. Obtain a new/ updated ATO.
Change	Equipment Upgrades	New (Different) Servers	Significant Change	New and modified control implementations must be tested as part of the Configuration (Change) Management processes. Obtain a new/ updated ATO.
Change	Major System Updates	New (Different) OS	Significant Change	New and modified control implementations must be tested as part of the Configuration (Change) Management processes. Obtain a new/ updated ATO.
Change	Security Components	Cryptographic Modules	Significant Change	New and modified control implementations must be tested as part of the Configuration (Change) Management processes. Obtain a new/ updated ATO.
Change	Security components	Identification and Authentication	Significant Change	New and modified control implementations must be tested as part of the Configuration (Change) Management processes. Obtain a new/ updated ATO.
Change	Security Components	Security Controls	Significant Change	New and modified control implementations must be tested as part of the Configuration (Change) Management processes. Obtain a new/ updated ATO.

Events			Actions	
Trigger	**Type of Event**	**Nature of Event**	**Type of Change**	**Notes**
Change	System boundary	New processing location(s)	Significant Change	A new processing location will need to go thru an re-authorization to ensure the system is secure from any issues or attacks
Change	System boundary	New User Population	Significant Change	New and modified control implementations must be tested as part of the Configuration (Change) Management processes. Obtain a new/ updated ATO.
Change	System boundary	Protocol Change	Significant Change	Vulnerability scan is required
Environment	System boundary	Change or Addition of Hosting Infrastructure or Site	Significant Change	Full authorization of the GSS is required. New and modified control implementations (for applicable applications) must be tested as part of the Configuration (Change) Management processes. Application obtains a new/updated ATO.
Environment	Core Mission/ Business Functions	New Mission or Business Function added	Significant Change	New and modified control implementations must be tested as part of the Configuration (Change) Management processes. Obtain a new/ updated ATO.
Environment	Core Mission/ Business functions	Cessation of mission or function.	Significant Change	New and modified control implementations must be tested as part of the Configuration (Change) Management processes. Obtain a new/ updated ATO.
NIST	New Revision of ARS	Affects Existing Controls or Adds New Controls	Significant Change	New and modified control implementations must be tested as part of the Configuration (Change) Management processes. Obtain a new/ updated ATO.
Time	No ATO Exists	New System Implementation	Standard Operating Procedure	A&A and ATO required before commencement of operations.
Time	Current ATO Exist	System ATO Expires in X months	Standard Operating Procedure	If system has had annual assessments performed by independent assessors, those results can be used for the evaluation. Test any untested control implementations. Obtain a new/updated ATO.
Time	Current ATO Exist	Host GSS ATO Expires in X months	Standard Operating Procedure	If annual assessments have been performed by an independent assessor, and GSS ATO is maintained, then no action is needed for application re-authorization.
Change	Patch Updates	Anti-Malware	Standard Operating Procedure	Vulnerability scan is required.

Events			Actions	
Trigger	**Type of Event**	**Nature of Event**	**Type of Change**	**Notes**
Environment.	Target of Threat	Specific and Credible Information	Target of Risk	Incident Response, POA&Ms, and compensating controls required.
Risk	Vulnerability (New or Existing)	CMS Attacked	Target of Risk	Incident Response, POA&Ms, and compensating controls required.

3 THE SIA PROCESS

3.1 DEFINING THE SCOPE OF THE PROPOSED CHANGE

At CMS, Business Owners are required to develop and maintain a *Configuration (Change) Management Plan*[6] to ensure that changes are properly managed within systems. *Security Impact Analysis* assumes that there is an orderly process for initiating and managing change.

Assuming you have in hand a *Change Request (CR)* that desires to *"Upgrade System XXX"*, prepare a document that describes the extent of the change. Be specific, and list all boundaries for all systems. Without a clear understanding of the change, you cannot identify any *meaningful* (or *real*) risks. In a *mature* Configuration (Change) Management (CM) process, some of this will be in the applicable CR form. However, for the purposes of an SIA, you must capture *all* possible descriptions of the environment for the change. Take a tact of trying to identify what will (or even *possibly* will) occur, before, during, and after the change—and try to consider as many environments, or possibilities, as possible.

Remember, this step is occurring *before* you have made any designs or plans for how a given CR will be *fulfilled*. That is, nothing has been *designed* yet. The goal here is to describe, as fully as possible, the environment and possible scenarios for the change. The more detail, the better. Use the CR form (part of the *Configuration (Change) Management Plan* developed under the CM-9 or XLC process) to gather and aggregate this information to the maximum extent possible. A typical CR form will consist of something similar to Table 2. However, while variants to the CR forms are allowed, over-simplifying the required detail on the CR form will only make the SIA process harder.

Table 2 Initiative/Release Background

[NOTE: Pre-filled information in this Table is for illustrative purposes only and may be modified and enhanced with information applicable to individual system and Configuration (Change) Management Process.]

Element	Description
CR Number	
Date	
Submitter (and contact information)	
Initiative/Release Name (Title)	
Priority	

[6] Required for *Moderate* and *High* systems under ARS requirement CM-9, *Configuration Management Plan*. The CMS XLC process may also require a CM plan (available here: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/index.html), depending on the *project complexity level*.

Element	Description
Project Type	*[Examples only]:* • New Development: *[insert description]* • Enhancement: *[insert description]* • Maintenance: *[insert description]* *[Insert project types and descriptions as applicable]*
Description of System Changes	*[Provide an overview of the changes.]*
Known Baseline Changes (to Security Configuration Baselines)	*[Provide description of the new or modified baseline, and why these changes will/might be required.]*
Security Risks	*[Provide any risks or impacts on the system.]*
Planned Deployment Initiation Date	
Planned Deployment Completion Date	
System(s) and Subsystems impacted by change	
Current Security Categorization of Impacted System(s)	
[Insert initiative/release background info required by the organization as applicable]	

Some sort of CR form (above) should already be part of the Configuration (Change) Management process. Therefore, there should be no need to create a *separate* artifact to facilitate this requirement. However, the detail necessary to continue on with the SIA may necessitate some modifications to the CR form to ensure that the process is properly optimized for each CCB.

3.2 DETERMINING THE KEY CHANGES

Now that we understand the *basics* of the requested changes, planners now need to determine *Key* differences in the *changed* state (proposed) from the *original* state. These Key changes will help to determine the appropriate level of diligence and effort necessary to ensure that the end-state security (after the change has been fully implemented) has been assured.

The idea for this step is to breakdown what the proposed change will entail; where within the system those changes may need to be made, and the scope of change required within those identified areas.

Table 3, Table 4, and Table 5 are sample tables for an SIA that might be used within the CM-9 and XLC-required Configuration (Change) Management processes. Organizations and Business Owners are encouraged to adapt it, and integrate it into their configuration (change) control processes, as appropriate. This will make identifying potential "security issues" much easier.

By identifying these *initial* items, planners can quickly identify *obvious* security impacts, before they even start addressing some of the more esoteric "down-in-the-weeds" issues

[NOTE: Pre-filled information in this Table is for illustrative purposes only and may be modified and enhanced with information applicable to individual system and Configuration (Change) Management Process.]

Table 3 Application Changes

Impact ID	Change	Yes/No
AP-1	Change in the operating system, security software, firmware, or hardware that affects the accredited security countermeasure implemented	
AP-2	Change to the configuration of the system (e.g., a workstation is connected to the system outside of the approved configuration)	
AP-3	Change to the system hardware that requires a change in the approved security countermeasures	
AP-4	Change in the user interface that affects security controls	
AP-5	Change in the security policy (e.g., access control policy)	
AP-6	Change in supporting security components or functionality	
AP-7	Change in the activity that requires a different security mode of operation	
AP-8	Creation or modification of an external connection	
AP-9	Creation or modification of Trust Relationships[7]	
AP-10	Modification of a subscribing system that affects the security of that system	
AP-11	*[Additional security impacts from business-specific application changes]*	
AP-x	*[…repeat as necessary…]*	

Table 4 Network (GSS) Changes

Impact ID	Change	Yes/No
NT-1	Change in the operating system, security software, firmware, or hardware that affects the accredited security countermeasure implemented	
NT-2	Change to the configuration of the servers or network architecture	
NT-3	Changes to core, distribution, and perimeter IT security infrastructure or devices	
NT-4	Inclusion of an additional (separately accredited) system(s)	
NT-5	Modification of system ports, protocols, or services	
NT-6	Creation or modification of an external connection	
NT-7	*[Additional security impacts from business-specific network changes]*	
NT-x	*[…repeat as necessary…]*	

[7] A trust relationship is a codified arrangement between two domains where users and/or services exist. One domain (A) trusts the other (B) to identify, authenticate and authorizer B's users to access A's resources. Simple trust relationships are two-way, while complex ones may have groups of multi-way trust (i.e., any organization in a group trusts any other to make assertions about its own users).

Table 5 Environmental (AP/GSS) Changes

Impact ID	Change	Yes/No
EV-1	Change to the physical structure of the facility or to the operating procedures	
EV-2	Change in criticality and/or sensitivity level that causes a change in the countermeasures required	
EV-3	Findings from security assessments and audits including internal IT security scans, physical or information security inspections, and internal/external control reviews	
EV-4	A breach of security, a breach of system integrity, or an unusual situation that appears to invalidate the accreditation by revealing a flaw in security design	
EV-5	Change in the threat or system risk	
EV-6	Modifications to cryptographic modules or services, especially deviations from Federal Information Processing Standards (FIPS) 140	
EV-7	*[Additional security impacts from business-specific environmental changes]*	
EV-x	*[…repeat as necessary…]*	

Changes (marked as *Yes* above) should be identified as potential security impacts (see Section 3.3), tracked through the applicable system Configuration (Change) Management processes, and appropriate mitigations should be developed—along with appropriate security *testing* procedures necessary to ensure that the impacts have been properly mitigated.

3.3 POSSIBLE EFFECTS OF THE KEY CHANGES

Once planners have identified the Key changes that will *likely* have a security impact on the system, they now need to determine the *actual* effects of those changes. At this point, planners are still in the *Planning Phase* of the XLC.

Most projects tend to (incorrectly) focus on the differences between *"significant"* changes vs. *"not significant"* changes—mainly just to determine any impact on an existing ATO (i.e., *"Do I need to get a new ATO?"*) However, that is *not* the primary purpose of determining the impact of change. The real reason planners want to know the impact is to help them *design* the system changes (in the *Design Phase* of the XLC) in a secure way, to minimize the amount of re-work necessary to correct *unplanned* security deficiencies identified in the late stages of the *Implementation Phase*. This step is simply for *planning* changes in a secure and thoughtful way.

In order for planners to *plan* for the design implications of Key changes, they need to analyze each Key change and i) identify various scenarios for how these key changes might be designed and implemented, and ii) determine the security effects/impacts of each design scenario.

Again, this analysis is similar to any other design process analysis that should be performed as part of the XLC and the Configuration (Change) Control process. All planners are doing as part of the SIA is singling-out the security impacts.

For *each* Key change identified, identify the relevant change information to identify *nonfunctional* design requirements (see Table 6) that identify the relevant key changes and any applicable (*nonfunctional*) design requirement(s) necessary to address the impacts identified.

Note that Table 6 is derived from what a mature Configuration (Change) Management process would use to develop *User Requirements* (see XLC template for the *Requirements Document*[8].)

It is understood that local Configuration (Change) Management processes will differ from program-to-program. As such, it is highly encouraged that individual Configuration (Change) Management programs and *CM Plans* (see XLC *Configuration (Change) Management Plans*) *integrate* the requirements of Table 6 into the existing *Requirements* analysis and documentation processes.

[NOTE: Pre-filled information in this Table is for illustrative purposes only and may be modified and enhanced with information applicable to individual system and Configuration (Change) Management Process.]

Table 6 Impact Requirements Table(s)

Element	Description
CR Number	
Impact ID	
Summary of Security Impact	*[This is the "actual security effects" of the proposed change request. This should be a* custom *description of the* specific *impact for this change. Please do not "cut-and-paste" from the tables in Section 3.2. Be specific and relevant.]*
Supported Business Requirement	*[Explain how this impact is necessary to support a specific Business Function.]*
Primary Proposed Solution	
Primary Proposed Solution	*[Explain the primary proposed solution that would be implemented that would generate the identified impact. Within the description, include the Drivers for why this solution is the Primary proposed solution. The Primary proposed solution may be driven by ease-of implementation, scheduling constraints, architectural efficiencies, etc.]*
Primary Proposed Solution Impact Mitigation	*[Explain how the impact would be mitigated if the Primary solution were chosen as the preferred design. This explanation should address all of the items identified in the "*Summary of Security Impact*" above.]*
Primary Proposed Solution Expected Results	*[Explain how the proposed solution impact mitigation could be measured as achieving the desired result if the Primary solution were chosen as the preferred design.]*
Primary Proposed Solution Validation Technique	*[Explain how the proposed impact would be mitigated if the Primary solution were chosen as the preferred design.]*
Alternate Proposed Solution #x	
Alternate Proposed Solution	*[See instructions for Primary Proposed Solution.]*
Alternate Proposed Solution Impact Mitigation	*[See instructions for Primary Proposed Solution.]*

[8] XLC Templates are available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/Artifacts.html.

Element	Description
Alternate Proposed Solution Expected Result	*[See instructions for Primary Proposed Solution.]*
Alternate Proposed Solution Validation Technique	*[See instructions for Primary Proposed Solution.]*
Alternate Proposed Solution #x	
…repeat as necessary…	

3.4 SORT AND PRIORITIZE

From this point forward, the process is much more straight-forward. After all of the various *Solutions* and *Alternatives* have been identified, it now becomes part of the normal change management and requirements analysis processes for designing a system. Designers should sort and prioritize the available solutions, weigh the impacts of the various proposed solutions against *functional* design requirements and associated *project risks* identified in the applicable XLC *Project Management Plan*.

3.5 MAKE DECISIONS

Make a decision using the results. At this point, the change process should be firmly entrenched in the *Design Phase* of the XLC (and the applicable Configuration [Change] Management process). The CCB and the applicable XLC reviews should now be adhered to and followed in order to choose the appropriate design and implementation solutions. Note that any attempts to *"accept risk"* must still follow proscribed processes for approvals (***prior to finalizing*** designs), and that *"Risk Acceptance"* is never appropriate for minimum *legal* or *statutory* standards (such as the Privacy Act, Health Insurance Portability and Accountability Act [HIPAA], Health Information Technology for Economic and Clinical Health Act [HITECH], CFO Act, Federal Managers Financial Integrity Act of 1982 [FMFIA], etc.)

3.6 FINALIZE TESTS AND TEST PLANS

After the designs elements are finalized, develop the appropriate test plans, to incorporate testing the nonfunctional design modifications necessary to address the identified security impacts. For *Moderate* and *High* level system, these tests should be performed by independent parties, and documented in CMS Federal Information Security Management Act of 2002 (FISMA) Control Tracking System (CFACTS).

Table 7 Testing Worksheet

[NOTE: Pre-filled information in this Table is for illustrative purposes only and may be modified and enhanced with information applicable to individual system and Configuration (Change) Management Process.]

Please describe the tests that need to be conducted against the change?
Please provide a description of the test results for each change (or provide reference to another document with test results).

3.7 THE COMPLETED SIA

The objective of performing an SIA is ***not*** to generate an SIA artifact (document). The purpose is to integrate the *security impact analysis* into the configuration (change) management process. As such, it is ***highly encouraged*** that the documentation of the SIA process, and its results, be integrated into the formal Configuration (Change) Management processes and artifacts. However, note that ARS requirement CM-4 requires that the *process* of a security impact analysis be completed—and independent assessors of the CM-4 requirement will require documentation to validate that the SIA process was completed. If properly integrated, completed Configuration (Change) Management documentation should suffice.

If Business Owners desire to generate *separate* documentation of the SIA, the same principles outlined in this Section apply, and the following information should be added.

Table 8 Analysis Worksheet

[NOTE: Pre-filled information in this Table is for illustrative purposes only and may be modified and enhanced with information applicable to individual system and Configuration (Change) Management Process.]

Analysis, Recommendations, and Requirements
[Reviewed by: Name (Title)]

Signature

_____ _____
[Insert relevant Developer/Maintainer role] Date

Signature

_____ _____
Information System Security Officer (ISSO) Date

4 APPROVED

Teresa Fryer

Digitally signed by Teresa Fryer
DN: cn=Teresa Fryer, o, ou, email=teresa.fryer@cms.hhs.gov, c=US
Date: 2014.07.02 18:46:09 -04'00'

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.gov*.*