DEPARTMENT OF VETERANS AFFAIRS
Office of Information Security (OIS)
Office of Cyber Security (OCS)

RiskVision (GRC)
Configuration Management Plan

August 14, 2013
V 1.0

This page left intentionally blank

Table of Contents

Document Change Control Sheet

Document Title: Configuration Management Plan

Date	Filename/Version #	Author	Revision Description
08/14/2013	DRAFT CMP Version 1.0	Martin DeLeo	

1 INTRODUCTION

Effective Configuration Management is a critical systems operations/maintenance phase success factor. This section provides the background, scope, and purpose associated with creation and use of the (RiskVision) GRC Configuration Management Plan (CMP).

1.1 Background

Configuration Management (CM) is the process of establishing and maintaining the security, integrity, reporting and audit capability of configuration items (CIs).

Proper and secure operation and maintenance of Department of Veterans Affairs (VA) information systems requires the application of configuration management (CM) principles to existing networks, hardware, and software to ensure that quality systems and software products are implemented and maintained. As a management tool, CM ensures that system components – whether hardware or software – are properly identified and controlled during the day-to-day operations at the VA, provides a disciplined set of techniques for controlling changes to identified baseline security configurations, and enhances consistency, compatibility, integrity and security of VA systems.

1.2 Purpose of this document

The purpose of this document is to define the practices and procedures required to accomplish configuration management throughout the life cycle of systems owned and maintained by the VA Central Office (VACO). It identifies CM requirements in the areas of naming conventions, library structure, configuration identification, change control, status reporting, auditing, archiving and storage. The intended audience for this document is the RiskVision support staff and management, contractor team(s), management within the VACO and Administrators for the Sterling, VA TIC, and other government management who have oversight responsibilities for VA Information Systems.

1.3 Scope

This plan applies to the RiskVision Application/Database. It does not include the CM for the hardware components on which the RiskVision Application/Database resides and which are managed and maintained by the Administrators for the Sterling, VA TIC.

CM is a system engineering discipline that formalizes the management of the configuration of a system and controls changes to the system throughout its life cycle. The key principles of CM ensure that all components of the system can be uniquely identified and managed and that any previous version of the system can be readily reproduced. CM activities that will be discussed in this plan are;

- Configuration Identification
- Configuration Control
- Configuration Status Accounting

- Configuration Audits

2 CM ROLES AND RESPONSIBILITIES

The purpose of this section is to define the Configuration Manager responsibilities and to identify the roles that will assume each of these responsibilities.

The following table provides roles and responsibilities. This is an all inclusive process for the following Systems: RiskVision Application/Database. Additional expert support teams will be formed as necessary.

Role	***Responsibilities***
Configuration Manager (RiskVision) Project Manager	• *Provide overall management and direction for CM personnel.* • *Implements the final RiskVision Working Group (RVWG) decisions and notifies the CM Administrator* • *Based on RVWG member recommendations, approve or disapprove the RiskVision Change Requests (SCR) into the security configuration baseline.*

Role	***Responsibilities***
RVWG Members: *System/Application/Database Managers*	• *Develop new security configuration baselines* • *Review and discuss proposed submitted changes* • *Determine or validate scope and priority of SCR(s)* • *Identify duplicate or associated SCRs* • *Evaluate the impact of the SCR to the existing security configuration baseline (both before and after testing (should that occur)* • *Approve/Deny SCRs* • *Assess technical, schedule, and cost impact* • *Determine implementation approach*
Information Security Officer (ISO)	• *Monitor VA-(Network Security Operations Center (NSOC), vendor web sites, etc. for announcement of new patches and software updates affecting VA security configuration baseline* • *Notify Help Desk* • *ISO Role consists of:* • *reviewing change proposals and problem reports to determine what, if any, impact the change/fix may have on the security configuration and policy;* • *making recommendations, if necessary, to appropriate Government personnel as to proposed changes/fixes to satisfy IT security policies;* • *reviewing completed System Problem Report(s) (SPR) to determine if the final change/fix that was implemented is compliant with all IT security policies.*

Role	***Responsibilities***
Configuration Manager *Systems Administrator*	• *Manages the CM processes* • *Ensures the integrity of CM library* • *Manages CM activities to ensure compliance with the plan* • *Develops and maintains CM processes and procedures* • *Organizes and leads CM audits and publishes the audit reports* • *Acts as the main CM point of contact on CM-related matters* • *Ensures the functionality of automated CM tools including backup and catastrophic recovery* • *Actively monitor activity logs in times of heightened security alerts*
CM Librarian • *Identified by project at Local, network, or regional level.*	• *Creates and manages the CM library* • *Participates in other activities* • *Manages the list of authorized CM library users and level of authorized access* • *Coordinates with LAN team to guarantee security of the library and access to it* • *Manages and publishes CM library inventory listing* • *Archives obsolete material*

Role	***Responsibilities***
CM Administrator *appointed tasks to the following:* • *Network Manager* • *Systems Manager* • *Telecommunications Mgrs.* • *Imaging Manager*	• *Receiving, recording and tracking configuration change requests (SCRs) and all related decisions* • *Monitoring VA-Computer Incident Reporting Capability (VA-NSOC), vendor web sites, etc. for announcement of new patches and software updates affecting VA security configuration baselines (See Configuration Change Monitoring and Identification Process below)* • *Initiating SCRs* • *Prioritizing SCRs* • *Coordinating RVWG reviews* • *Coordinating all relevant information between entities involved in the CM and CC processes (including clarification from submitter should the request be unclear and coordination with entities of the VA ITSCAP)* • *Providing appropriate security configuration baseline modification information* • *Logging/Tracking security configuration baseline waivers* ***In relation to hardware CIs and COTS software CIs:*** • *Manages the implementation of approved Change Requests* • *Provides management with pertinent information in regards to a change request and potential impact on the account as a whole* • *Gives management an estimate of time and cost to implement a proposed solution to a Change Request* • *Submit change requests* • *Implement approved, controlled changes* • *Participate in the activities of the RVWG review process, as requested by the RVWG*

Role	*Responsibilities*
Help Desk *Automated process to provide data for:* • *Hardware/Software Support* • *Asset Management* • *Change Management* • *Needs Assessment*	• *Provides support of all Information Technology equipment or software supporting RiskVision.* • *With the use of Change Management, hardware and software-related change requests, are categorized by category, type and item and are built into the system and forwarded to the appropriate authority according to the nature of the request* • *Serves as the single point of contact for software and hardware issues, including procurement of new hardware, and problems with and enhancements to existing items.*

2.1 CM Plan Implementation

2.1.1 RiskVision Working Group (RVWG)

The RVWG and Change Control Board are synonymous for purposes of changes to RiskVision The RVWG is facilitated by the Director, Security Reports and Oversight Management or in his/her absence, the RiskVision Project Manager (aka RiskVision Team Lead) . The primary function of the RVWG is review and disposition of all proposed SCRs. The RVWG will conduct to the extent possible all discussions via email or through the meetings. Other formal meetings may be scheduled on an as needed basis. SCRs need the approval of a majority of the members of the RVWG to be accepted. The CM Administrator will resolve issues when the RVWG is deadlocked.

RVWG discussions will include the review and approval/disapproval of submitted SCRs. RVWG members are expected to participate in all reviews/discussions. Disposition on SCRs will be based on the opinion of the majority.

- All significant user interface (UI) or business logic changes must be approved by the RVWG.
- DB ad-hoc updates: A data-only change that cannot be accomplished through the user interface would be performed by RiskVision development staff. A copy of the SQL source code required to re-create that object is captured and checked into the source code management repository (described below). This provides a way to track changes to schema objects over time.
- Application changes, builds, hotfixes: Subversion is used for source control of all changes. After approval of any changes, the changes to the application are test on development servers; when development testing is complete, the changes are implemented on a pre-production server; when the pre-production server testing

shows the changes to be bug free, the changes are moved to the production server. All changes are documented via subversion and a transmittal letter.

- The latest changes/version of RiskVision is always located in the help section of RiskVision.
- Potential changes are requested via a RiskVision Change Request form then sent for review/approval/denial by the RiskVision Change Control Board.
- When changes are deployed to production, changes are documented via a RiskVision transmittal letter. All source code and database object changes are preserved and tracked through Subversion audit logs.

The RiskVision CM Process includes the following steps:

1. A RiskVision User submits an SCR (RiskVision Change Request) to the RVWG.
2. If the RVWG concurs, the SCR is sent to the RiskVision Team Lead.
3. If the RiskVision Team Lead concurs, it is sent to the Director, Security Reports and Oversight Management (SR&OM).
4. If the SR&OM Director concurs, it is sent to the ADAS (Associate Deputy Assistant Secretary) for Cyber Security (VA CISO) for final approval.
5. If the CISO approves, it is returned to the RiskVision Team Lead for implementation.
6. Once implemented, a transmittal is sent to notify the field of the change(s).

2.1.2 Schedules and Resource Requirements

- Internal Help Desk Software will be utilized as the CM tool to request Changes. Currently, a word document is used to request changes.
- Change requests are maintained on a SharePoint server for the RVWG.

2.2 Applicable Policies, Standards, and Procedures

Federal Law and general principles and value statements will guide the decisions made in planning, implementing and maintaining the systems discussed in this plan.

- Federal Law
  - Federal Information Security Management Act of 2002 (FISMA)

- Office of Management and Budget (OMB)
  - OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Information Resources, November 2000

- National Institute of Standards and Technology (NIST)
  - Federal Information Processing Standards (FIPS)
    - FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, December 2003
    - FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
  - NIST Special Publications (SP)

    - NIST SP 800-53, Recommended Security Controls for Federal Information Systems
    - NIST SP 800-70, Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers

- Department of Veterans Affairs
  - VA Directive 6500 - Information Security Program
  - VA Handbook 6500- Information Security Program

General Principals

- Change Items (CIs) will be identified, controlled, and made available to those with proper authorization.
- CM will be implemented throughout the system lifecycle.
- Changes to the baseline configuration items will be controlled according to documented procedures.
- There is a SharePoint CM library that acts as a repository for storing all non-hardware related CIs and the associated CM records.
- The latest changes are always available to all RiskVision users via the Help > Library > Transmittal links
- CM roles will be assigned by the Director, SR&OM to specific individuals or organizations that will assume specific CM responsibilities.
- Affected groups and individuals will be informed of the status of the SCRs.
- Configuration baselines and CM activities will be audited on a periodic basis.

3 CM ACTIVITIES

3.1 Configuration Identification

Configuration Identification is the selection of CIs, issuance of identification numbers to the CIs, and the management of baselines.

3.1.1 Configuration Items (CI)

The following items will be designated as CIs:

Non-Hardware CIs: Examples

- *Policy and procedure documents and templates*
- *Process documents (plans)*
- *Network/System Diagrams*
- *HTML files for Web pages*
- *Requirements documents for procurement of goods and services*
- *Contract documents with outside vendors for the supply of goods and services*
- *COTS software*

Hardware CI will be defined and managed by Administrators for the Sterling, VA TIC.

3.1.2 Identification Criteria

The criteria for identifying work product CIs are: CI number, version number, filename, description, author(s), and date baselined.

The criteria for identifying hardware CIs are defined and managed by Administrators for the Sterling, VA TIC Configuration Management Plan.

3.2 Base Lining a CI

The term "Baseline" is defined as a specification or product that has been formally reviewed and agreed upon, and serves as a basis for further development, which can be changed only through change management procedures. Baseline includes requirements, source code, executable programs, data files, hardware and associated documentation. These items collectively are also referred to as a "System." The assigned responsibilities for managing and baselining CIs are shown in the following table:

Type of CI	Responsibility
Work products	RiskVision Team Lead
Web-related CIs	RiskVision Team Lead
Responses to RFPs	Director, SR&OM
Requirements documents	Director, SR&OM
Contract Documents	COTR
Hardware	Administrators for the Sterling, VA TIC
COTS software	Director, SR&OM / RiskVision Team Lead

3.2.1 Non-Hardware CI Baselines

Baselines for non-hardware CIs will be established when the author(s)/owner of a work product has completed the item and offers it for review. Different baselines will be established at different points within the review cycle. All major baselines that are designated to carry version label in whole numbers (1.0, 2.0, 3.0 etc.) will undergo a RVWG review. The review cycle for major baselines will be every six months.

3.2.2 Hardware and Software Baselines

Hardware. All Change Requests pertaining to hardware will be managed in accordance with Administrators for the Sterling, VA TIC Configuration Managements policy and procedures.

3.3 Work Product CI Numbering

Each work product CI will be given a unique identification number according to the CI numbering scheme.

3.4 Naming Convention

General page:
http://vaww.vairm.vaco.va.gov/vanic/docs/coverpage.html

Function codes:
http://vaww.vairm.vaco.va.gov/vanic/reports/FunctionCodeListing.asp

Location codes:
http://vaww.vairm.vaco.va.gov/vanic/reports/LocationCodeListing.asp

NT & Win2K naming:
http://vaww.vairm.vaco.va.gov/vanic/docs/naming.asp

3.5 Change Control

Change control will include requesting, evaluating, approving or disapproving, and implementing changes to baselined CIs. Changes will encompass correction of errors, enhancements to existing CIs, and creation or acquisition of new CIs.

Any change to an item, or an addition of an item, in the baselined system requires tracking using SPR or SCR. The SPR is used to identify and initiate work to resolve a system problem. A system problem occurs when the system, or any of its components, malfunctions or does not meet defined requirements or specifications. They are also used to initiate corrective maintenance and typically generated by operational personnel as a result of routine monitoring or analysis. The anomalous system is identified and appropriate personnel notified.

The SCRs is used to propose changes, enhancements, or additions to the system. The change may be required to support adaptive or perfective maintenance. SCRs are also to be used to change system requirements or specifications. Figure 3.1 presents an overview of the change control procedures.

3.5.1 Change Request for Work Products

All changes will be assigned according to category, type and as appropriate for approval. The RVWG will authorize the implementation schedule of a major change.

All change requests pertaining to minor changes will be forwarded according to category, type and item and classified for approval. The System Manager will coordinate with the Chief Information Officer (CIO) for authorization and the implementation schedule of a minor change.

3.5.2 Change Request for Hardware

All Change Requests pertaining to hardware will be managed in accordance with Administrators for the Sterling, VA TIC Configuration Managements policy and procedures.

3.6 Archiving, Storage and Disposal

The most recent versions of CIs that carry version numbers will be retained in the current library. Older versions may be archived on a convenient medium. The media storing any older versions will be clearly marked to make it uniquely identifiable.

Obsolete and irreparable hardware will be disposed of in accordance with Medical Center Directive pertaining to Logistics Operating Procedures and OI&T processes for disposition electronic media. Center Directive 00-08-4 Disposition of Automated Information Systems Electronic Storage and Memory Devices.

4 CM STATUS ACCOUNTING

CM status accounting activities will record and report the status of CIs. At a minimum, the following types of reports will be generated by the Configuration Management Team as appropriate.

- A report providing a summary of open change requests for tracking purposes
- A report providing a summary of the change activity on a quarterly basis for assessing current work load, based upon open requests and requests processed during the reporting period
- A report providing a summary of contents of the CM baseline library
- A report providing a history of a baselined CI, including the dates and description of changes made to it
- Audit reports

The reports will be made available to the VISN CIO, Chief Technology Officer (CTO), Region Director as requested.

5 AUDITS AND REVIEWS

CM baseline audits will be conducted on a yearly basis. The Configuration Manager will be responsible for ensuring that CM audits are conducted in terms of the guidelines provided in this section. To conduct the audit adequately, the Configuration Manager will secure resources, including trained manpower and support tools. CM audits will be independent of any Quality Assurance audits conducted by the Quality Assurance Team in terms of the Quality Assurance Plan.

5.1 CM Baseline Audits

CM baseline audit will be led by the Configuration Manager and will comprise the following activities:

- The audit will be planned. The scope of the audit will be defined and items relevant to the audit will be gathered before the start of the audit. The audit report template(s) will also be created before the start.
- The audit will assess the integrity of the baselines by verifying that all baselined CIs exist within the CM Library. For hardware CIs, their designated location will be verified.
- The correctness and completeness of a given CI will verified by validating that the CI matches its documented description. Implementation of approved change requests for a given CI according to approved and documented procedures will also be verified.
- CM activities will be reviewed to verify compliance to CM standards and procedures in this document, the CM Plan.
- On the basis of the audit report, action items to correct deficiencies and resolve audit issues will be generated.
- The action items will be monitored to closure.
- Subversion can provide a report (audit log) of all changes made to either the production or development baselines. Major changes made by development staff are also documented in the monthly status reports.

5.2 CM Reviews

CM reviews are conducted by the RVWG prior to baselining a work product, as defined in Section 3.2. *Base Lining a CI*.

6 CM METRICS

CM measurements will be used by the CM Manager and the RVWG to measure the effectiveness of the CM processes and to identify improvements. When improvement areas are identified and modifications are implemented, measurements will be used to assess the impact of the modifications. Measurement will then be used on an ongoing basis to assess the current state and stability of software processes. A Process Satisfaction Survey will be conducted annually. At a minimum, the following metrics will be collected as part of CM Measurement Process:

- Number of change requests received per month
- Response time to closure for each change request
- Work completed and resources expended in CM activities
- Profiles of the types of changes over time, i.e. patches applied, etc.

7 CM TOOLS

This section identifies the automated tools that will be utilized to record and maintain configuration items.

- WMI scripts
- SQL Server Logs
- Subversion Logs

8 CI RETENTION, ARCHIVING, STORAGE AND DISPOSAL

The most recent versions of CIs that carry version numbers will be retained in the current library. Older versions are archived on a restricted SharePoint site. (External media is not used.)

Obsolete and irreparable hardware will be disposed off in accordance with VA OI&T Disposition of Electronic Media and VA Directive 6500.

APPENDIX A: GLOSSARY OF TERMS

Baseline	Per NIST SP 800-53 - The baseline configuration provides information about a particular component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component's logical placement within the information system architecture. The baseline configuration also provides the organization with a well-defined and documented specification to which the information system is built and deviations, if required, are documented in support of mission needs/objectives.
Configuration Item	The hardware and software components of an information system as well as all relevant ownership documentation information.
Configuration Management	The process of establishing and maintaining the security, integrity, reporting, and audit capability of configuration items.
Work Products	Used for Configuration management and identifying and tracking configuration items. All relevant Configuration management-related information system ownership documentation and information including but not limited to policy and procedures.
Major Change	Any major change requires analysis to determine its impact on system security requirements. Examples of a major (or significant) change from NIST SP 800-37 include (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 or firmware component; or (iv) modifications to cryptographic modules or services. Changes in laws, directives, policies, or regulations, while not always directly related to the information system, can also potentially affect the security of the system and trigger a reaccreditation action.
Minor Change	Many of the changes made to a system do not require the extensive analysis performed for major changes. Each change can involve a limited risk assessment that weighs the cost versus benefits and that can even be performed on-the-fly at meetings. Even if the analysis is conducted informally, decisions should still be appropriately risk based.

APPENDIX B: LIST OF ABBREVIATIONS

CAB	Change Advisory Board
CC	Configuration Change
CCR	Configuration Change Request
CGI	Common Graphical Interface
CI	Configuration Items
CIO	Chief Information Officer
CM	Configuration Management
CMP	Configuration Management Plan
CMWG	Configuration Management Working Group
COTR	Contracting Officer’s Technical Representative
COTS	Commercial Off-The-Shelf
CPU	Central Processing Unit
CR	Change Request
DCIO	Deputy Chief Information Officer
FAR	Federal Acquisition Regulation
GUI	Graphical User Interface
GUID	Globally Unique Identifier
HTML	Hyper Text Markup Language
IMC	Internal Medicine Clinic
ISO	Information Security Officer
IT	Information Technology
LAN	Local Area Network
OI&T	Office of Information and Technology
PMO	Program Management Office
POC	Point of Contact
QA	Quality Assurance
RFP	Request For Proposal
SOP	Standard Operating Procedures
SPR	System Problem Reports
RVWG	RiskVision Working Group
VA	Department of Veterans Affairs
VA NSOC	Veterans Affairs Network and Security Operations Center

VPN	Virtual Private Network

APPENDIX C: SOFTWARE PATCH MANAGEMENT

1. **PURPOSE:** To delineate operational procedures to be followed by RiskVision development staff in software development.

2. **POLICY:** In daily operations RiskVision development staff shall provide maintenance, deployment and development of software in a manner to maximize efficient operation, availability, and data security.

3. **RESPONSIBILITIES:**
The RiskVision Program Manager is responsible for overall software maintenance, development, deployment and ensuring appropriate measures are in place to maintain effective oversight for the software activities for RiskVision, and for insuring that software personnel follow the policies and conventions in the SOP. Development staff are responsible for adhering to the procedures outlined in this standard operating procedure.

4. **PROCEDURES:**
Once approved, development staff will install updates as required ensuring current system/data state is captured as necessary in the event a roll back is needed. As applicable, RiskVision staff will test patch changes for any adverse effects. Development staff will track patches as software revisions.

APPENDIX D: SERVER SOFTWARE BASELINE

Operating System:	Windows Server 2008 R2
Web Application:	.aspx
Web Server:	TomCat
Database:	Oracle

APPENDIX E: CHANGE MANAGEMENT REQUEST FORM

RISKVISION CHANGE REQUEST (SCR)

SCR #:

REQUIREMENT #:

CHANGE REQUEST INITIATION: Originator: Phone#:

E-Mail Address: Date Submitted: Version Number:

CONFIGURATION ITEM: Software: Documentation: ______

CHANGE TYPE: New Requirement: ______ Requirement Change: ______ Design Change: Other: ______

REASON: Legal: ______ Business: ______ Performance Tuning: Defect: ______

PRIORITY: Emergency: Urgent: ______ Routine: ______ ***Date Required:*** ____/____/____

CHANGE DESCRIPTION: ***(Detail functional and/or technical information. Use attachment if necessary.)***

Attachments: Yes / No

TECHNICAL EVALUATION: ***(To be completed by RiskVision Project Staff. Use attachment if necessary.)***

Received By: _______________________ Date Received: ___/___/___ Assigned To: _______________________ Date Assigned: ___/___/___

Part of RiskVision Affected:
____

Modules/Screens/Tables/Files Affected:
____

Documentation Affected: **<u>Section #</u>** **<u>Page #</u>**

<u>Date Completed</u> **<u>Initial</u>**

Requirements Specification

____
__ ________
______/__
____/______
____

System Design Specification

____
__ ________
______/__
____/______
____

User System Reference Manual

____
____
______/__

____/______ _______

System Maintenance Manual

_________ __ ________ ______/__

____/______ _______

Other (Specify)

_________ __ ________ ______/__

____/______ _______

TIME ESTIMATES: ***(To be completed by RiskVision Project Staff. Use attachment if necessary.)***

Lifecycle Stage **Est. Time Act. Time Date Comp.**

Remarks

Analysis/Design __________ __________ ____/____/____ _________________________ ____________

Coding/Testing/Acceptance __________ __________ ____/____/____ _________________________ ____________

Total Hours: ___________ ___________ _________________________ ___________________

Impact Analysis Needed: **Yes / No** ***(If yes, include impact on technical performance, resources, schedule, etc.)***

APPROVALS: Change Approved: ______ Change Not Approved: ______ Hold (Future Enhancement): ______

1. Signature ____ (Change Control Board) Date: ____/____/____

2. Signature ____ (Change Control Board) Date: ____/____/____

3. Signature ____ (Project Manager) Date: ____/____/____

RiskVision Form 1.0 (10/01/2005)

See Reverse for Instructions

INSTRUCTIONS FOR COMPLETING AND PROCESSING THE SCR FORM

This form will be used to request changes to the Security Management and Reporting Tool (RiskVision). The form is appropriate for all stages in the lifecycle, and may be initiated by Government or Contractor personnel. All change requests will be evaluated and will require approvals. A RiskVision Change Request (SCR) should contain only one change item. A separate SCR should be completed for each requested change. The form is a tool for initiating, evaluating, and tracking project change control requests. It may be modified or tailored to accommodate specific client/project requirements. The RiskVision Change Control Log is used to record and provide final disposition for any requested change.

(Initiators Complete the Shaded Areas; RiskVision/FISMA Project Staff Completes the TECHNICAL EVALUATION and TIME ESTIMATES Sections)

FIELD DEFINITION

SCR #: A sequential number beginning with the **organizational code** (e.g.,VHA194). For requests initiated by the Contractor, a sequential number beginning with the alpha character **C** (e.g., C194). The **numbers will be assigned and controlled** by RiskVision/FISMA Project Staff or designees, and tracked in the RiskVision Change Control Log. Initiators will be notified as to the specific SCR numbers assigned.

REQUIREMENT #: Number of the requirement to be changed (if known). A Requirement Number is provided and documented in the RiskVision Change Control Log once the SCR has been approved. If not approved, a Requirement Number will not be provided.

CHANGE REQUEST INITIATION: Information about the initiator of the change request, and the software/documentation impacts.

Originator: Name of person initiating the SCR.
Phone #: Phone number of originator.
Date Submitted: Date form submitted to the FISMA Project Staff.
E-Mail Address: Full e-mail address of initiator.
Version Number: Version number of RiskVision. (Located in the Help section of RiskVision).

CONFIGURATION ITEM: Configuration item affected. Place an "X" in the appropriate area.

Software: System component (e.g., POA&M, Assessment, Report Generator).
Documentation: System component (e.g., User Guide, other published documentation).

CHANGE TYPE: Type of change being requested. Place an "X" in the appropriate area. Specify other.

New Requirement: Requirement was not identified in original specifications.
Requirement Change: Requirement needs to be altered.
Design Change: Original design needs to be changed.
Other: Indicates other than above change types. Specify in the CHANGE DESCRIPTION area.

REASON: Place a "X" in the appropriate area. Prepare a brief justification identifying the basis for initiating the SCR and the expected benefits. Use the CHANGE DESCRIPTION area of the form if sufficient space is available; otherwise, use an attachment. Assist the appropriate personnel in ranking priorities.

Legal: Mandate by changes in Federal regulations and laws, OMB or NIST guidance.
Business: Mandated change related to VA or OCIS business practices and policy changes.
Performance Tuning: Change(s) required to improve application usability (e.g., improved screen layout, conversions), or platform/operating software performance.
Defect: A problem within RiskVision that requires a change (e.g., program error).

PRIORITY: Ranking to identify action or response to an SCR. Place an "X" in the appropriate area. In most cases, the Priority level will be Routine.

Emergency: A change in operational characteristics that, if not accomplished without delay, will impact system operability.
Urgent: A change that, if not accomplished promptly (e.g., prior to the next production cycle), will impact system effectiveness.
Routine: A change that can be planned, scheduled, and prioritized.
Date Required: The date the change is needed.

CHANGE DESCRIPTION: Detailed functional and/or technical information about the change. Use an attachment, if necessary, to provide adequate detail or supporting documentation (e.g., statement of new requirement).

Attachments: If attachments are included, circle "Yes," if not, circle "No."

TECHNICAL EVALUATION: To be completed by RiskVision/FISMA Project Staff. Provides tracking data of technical approach.

Received By: Name of person who initially received the SCR.
Date Received: Date SCR received by RiskVision/FISMA Project Staff.
Assigned To: Person who is being assigned the responsibility for the technical evaluation.
Date Assigned: Date assigned to assignee.
Type of Software Identify type(s) of software affected by the change (e.g., operating system software, application software). Also identify all dependent or
Affected: subordinate interfacing applications that may be affected by the change. Include name(s) and version number(s) if applicable. If necessary, use the CHANGE DESCRIPTION area or an attachment for additional information.
Modules/Screens/ Identify modules/screens/tables/files affected by the change. Include name(s) and version number(s) if applicable. If necessary, use the
Tables/Files Affected: CHANGE DESCRIPTION area or an attachment for additional information.
Documentation Identify documentation affected by the change. Include section and page number(s). Enter the date completed and the initials

Affected: of the author. If necessary, use the CHANGE DESCRIPTION area or an attachment for additional information.

TIME ESTIMATES: To be completed by RiskVision/FISMA Project Staff. Identify the lifecycle stage(s) affected by the change. Post the estimated and actual time required, and date(s) completed. Total the estimated times and provide any remarks.

Impact Analysis Needed: If an impact analysis is needed or received, circle "Yes" and attach to the SCR form; otherwise, circle "No." An impact analysis of the change request should have details on impacts to the Project Plan (i.e., available technical staff, schedule, costs, etc.).

APPROVALS: Acquire the approval signatures for authorizing the SCR. The SCR must be approved by at least two members of the RiskVision Change Control Board with the concurrence of the Project Manager. Full consensus by the Change Control Board can override the disapproval of the Project Manager. Select one option by placing a "X" in the appropriate action area: Change Approved, Change Not Approved, or Hold (Future Enhancement). **Note:** Individuals authorized to approve change requests are identified in the project Configuration Management Plan.