MANAGING THE CONFIGURATION OF INFORMATION SYSTEMS WITH A FOCUS ON SECURITY

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Organizations have to make frequent changes to their information systems in order to implement new and updated hardware and software components, correct software flaws and other errors, address new security threats, and adapt to changing business objectives. These constant changes result in adjustments being made to the configuration of information systems; these activities could have an impact on the security of the systems and operations.

In developing information systems, organizations employ many components that can be interconnected in different arrangements to meet the organization's business, mission, and information security needs. To protect information systems and information, organizations need techniques for the secure configuration, operation, and management of system components, including mainframes, workstations, servers, networks, operating systems, middleware, and applications, and for the management and control of risks to systems and information.

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) has issued a new guide to help organizations develop a well-defined process for managing and controlling secure system configurations, and for managing risks in information systems. NIST Special Publication 800-128, *Guide to Security-Focused Configuration Management of Information Systems*, supports the application of configuration management concepts and principles, and the integration of security into the configuration management process throughout the life cycle of the system.

NIST Special Publication (SP) 800-128, *Guide to Security-Focused Configuration Management of Information Systems*

Written by Arnold Johnson, Kelley Dempsey, and Ron Ross of NIST, and by Sarbari Gupta and Dennis Bailey of Electrosoft, NIST SP 800-128 explains the fundamental concepts associated with security-focused configuration management and its relationship with general configuration management of information systems. Security-focused configuration management (SecCM) is the management and control of secure configurations for an information system to enable security and facilitate the management of risk. SecCM builds on the concepts, processes, and activities of general configuration management by focusing on the implementation and maintenance of the organization's established security requirements.

The guide discusses the relationship of SecCM and general configuration management, the major phases of SecCM, and the organizational responsibilities for carrying out SecCM. One section of the guide concentrates on the detailed process for applying SecCM practices to information systems within an organization. The topics covered include planning SecCM activities for the organization; identifying and implementing secure configurations; controlling configuration changes to information systems; monitoring the configuration of information systems to ensure that configurations are not inadvertently altered from the approved baseline; and the use of Security Content Automation Protocol (SCAP). SCAP includes standard specifications that support the use of automated tools for verifying information system configurations.

The appendices to the publication provide additional information and references, as well as sample plans and outlines that organizations can adapt for implementing SecCM, including references to supporting information; a glossary of terms and definitions; acronyms; an outline of a SecCM plan; a sample configuration change request template; a listing of best practices for establishing secure configurations in information systems; flow charts for SecCM processes and activities; a sample Configuration Control Board (CCB) charter that organizations can adapt for use in their SecCM programs; and a template for security impact analysis.

NIST SP 800-128 is available from the NIST Web page http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf.

Federal Requirements for Configuration Management

Under the Federal Information Security Management Act (FISMA) (P.L. 107-347, Title III), federal agencies are responsible for “including policies and procedures that ensure compliance with minimally acceptable system configuration requirements, as determined by the agency” within their information security programs. Federal organizations manage the security of their information systems and associated operational environments, and also assure the security of information that is processed, stored, and transmitted by external or service-oriented environments, such as cloud service providers.

NIST-developed standards, guidelines, and recommendations, which help federal agencies protect and improve the security of their information systems, include the following specifically related to configuration management: Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems,* which specifies minimum security requirements for 17 security-related areas, including configuration management; and NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations,* which defines security controls supporting implementation of the minimum security requirements identified in FIPS 200 for all aspects of information system security.

The security controls included in NIST SP 800-53 are organized into families, one of which is the Configuration Management family. Organizations select, implement, monitor, and assess security controls to meet requirements for protecting the confidentiality, integrity, and availability of federal information systems and information. The new guide, NIST SP 800-128, supports the implementation of the Configuration Management family of security controls that are defined in NIST SP 800-53.

FISMA also directs federal agencies to apply a risk-based policy to achieve cost-effective results for the security of their information systems. NIST SP 800-128 supports activities that are part of this risk-based approach to the management of information systems. NIST has developed a Risk Management Framework (RMF) that describes six activities related to the categorization, selection, implementation, assessment, authorization, and monitoring of information and information systems security controls for an effective information security program. These six activities can be applied to the system development life cycle of new and legacy information systems. SP 800-128 provides specific information for supporting three of the activities (the Implement, Assess, and Monitor steps) of the RMF.

See the **For More Information** section below for references to additional NIST-developed standards and guidelines that support secure system configurations, and for information about SCAP, the RMF, and risk-based activities.

Configuration Management, SecCM, and Risk Management

Organizations apply **configuration management** (CM) for establishing baselines for their information systems and for tracking, controlling, and managing many aspects of business development and operation, such as products, services, manufacturing, business processes, and information technology. Configuration management activities are focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems. This process is important in establishing and maintaining secure information system configurations, and supporting the management of security risks in information systems.

The configuration of an information system is a representation of the system components, how each component is configured, and how the components are connected or arranged to implement the information system. These conditions and arrangements can affect the security posture of the information system. Configuration management activities include:

- Development of a **configuration management plan**, a comprehensive description of the roles, responsibilities, policies, and procedures that apply when managing the configuration of products and systems;

- Establishment of a **configuration control board**, a group of qualified people with responsibility for the process of controlling and approving changes throughout the development and operational life cycle of products and systems;

- Development of a **methodology for selecting and naming configuration items** that need to be placed under configuration management. A configuration item is an aggregation of information system components that is designated for configuration management and treated as a single entity throughout the CM process;

· Establishment of the **baseline configuration**, a set of specifications for a system, or configuration items within a system, that has been formally reviewed and agreed to, and which can be changed only through organizational change control procedures. The baseline configuration is used as a foundation for future activities such as additions and changes to the system;

· Development of a **configuration change control process** for managing updates to the baseline configurations and for the configuration items; and

· Development of a **process for configuration monitoring and reporting** to assess or test the level of compliance with the established baseline configuration and mechanisms for reporting on the configuration status of items placed under configuration management.

SecCM builds on the concepts, processes, and activities of general configuration management through the integration of information security requirements into the CM process. SecCM activities include:

· **Identification and recording of configurations** that impact the security posture of the information system and the organization;

· **Consideration of security risks** in approving the initial configuration;

· **Analysis of security implications of changes** to the information system configuration; and

· **Documentation** of the approved/implemented changes.

The initial implementation of a SecCM program may require considerable effort and resources as tools are acquired and implemented, system components are inventoried and recorded, and configuration management practices are modified. Once established, SecCM may require an ongoing investment in time and resources. Product patches, fixes, and updates must be analyzed for security impact as threats and vulnerabilities continue to exist. When changes are made to information systems, baseline configurations must be updated, specific configuration settings confirmed, and configuration items tracked, verified, and reported. SecCM is a continuous activity that has an impact on all stages of the system development life cycle, and that can lead to improved system security and more effective management of organizational risk.

To carry out an effective information security program, organizations need to **manage the risks** to their information systems. As threats continue to increase but resources to protect systems remain finite, organizations must balance the operational and economic costs of ensuring that a particular threat does not exploit a vulnerability against the needs of the organization to carry out its mission and business operations. When resources are limited, organizations need rigorous risk management practices to help set priorities for their information system security programs.

Phases of the Security-Focused Configuration Management Process

The activities for security-focused configuration management of information systems are organized into the following four major phases, which support security for an information system and its components, and the management of organizational risk. Some of these activities may be performed at the organizational level, where they are applied to more than one information system. Other activities may be more efficiently performed at the system level, where they are applied to a single information system. Each organization determines what activities are conducted at the organizational level and what activities are conducted at the system level in accordance with organizational management requirements.

- **Planning** includes developing policy and procedures to incorporate SecCM into the organization's existing information technology and security programs, and then disseminating the policy throughout the organization. The policy issues include the implementation of SecCM plans; the integration of SecCM plans into existing security program plans; the organization of Configuration Control Boards (CCBs); configuration change control processes, tools and technology; the use of common secure configurations and baseline configurations; and monitoring for compliance with established SecCM policy and procedures. The development and implementation of the SecCM plan, policies, procedures, and associated SecCM tools are most cost-effective when performed at the organizational level.

- **Identifying and Implementing Configurations**. After the planning and preparation activities are completed, a secure baseline configuration for the information system is developed, reviewed, approved, and implemented. The approved baseline configuration for an information system and associated components represents the most secure state consistent with operational requirements and constraints. For most information systems, the secure baseline configuration may include configuration settings, software loads, patch levels, how the information system is physically or logically arranged, how various security controls are implemented, and documentation. Where possible, automation is used to enable interoperability of tools and uniformity of baseline configurations across the information system.

- **Controlling Configuration Changes**. In this phase of SecCM, the emphasis is placed on the management of change to maintain the secure, approved baseline of the information system. Through the use of SecCM practices, organizations ensure that changes are formally identified, proposed, reviewed, analyzed for security impact, tested, and approved prior to implementation. As part of the configuration change control effort, organizations can employ a variety of methods for restricting access to the process for making changes to the system, including access controls, process automation, abstract layers, change windows, and verification and audit activities.

· **Monitoring** activities are used to validate that the information system is adhering to organizational policies, procedures, and the approved secure baseline configuration. The activities for planning and implementing secure configurations and then controlling configuration change may not ensure that an information system will remain secure after changes are made. Monitoring identifies undiscovered and undocumented system components, misconfigurations, vulnerabilities, and unauthorized changes. All of these issues, if not addressed, can expose organizations to increased risk. Organizations can use automated tools to identify when the information system is not consistent with the approved baseline configuration and when remediation actions are necessary. In addition, the use of automated tools often facilitates situational awareness and the documentation of deviations from the baseline configuration.

Since the processes and requirements within these SecCM phases do not remain static, they should be reviewed and revised as needed to support the management of organizational risk. SecCM monitoring activities may also indicate that previous phases of the process should be reviewed and possibly changed.

SecCM monitoring is done through assessment and reporting activities. Reports address the secure state of individual information system configurations and are used as input to requirements for continuous monitoring that are contained in the Risk Management Framework. SecCM monitoring can also support the gathering of information for metrics to provide quantitative evidence that the SecCM program is meeting its stated goals, or that improvements may be needed.

Organizations can realize considerable savings in cost and effort through the use of automated tools in their configuration management activities. **Security Content Automation Protocol (SCAP)-enabled tools** can be used to maintain the security of enterprise systems by automatically verifying the installation of patches, checking system security configuration settings, and examining systems for signs of compromise. Also SCAP-expressed checklists can be customized to meet specific organizational requirements by mapping individual system configuration settings to their corresponding high-level security requirements. These mappings can help demonstrate that the implemented settings adhere to requirements. The mappings are embedded in SCAP-expressed checklists which allow SCAP-enabled tools to automatically generate standardized assessment and compliance evidence.

For More Information

NIST publications that provide information and guidance on managing and controlling information system configurations throughout the system development life cycle include:

Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*
FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*

NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
NIST SP 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*
NIST SP 800-53A, Rev. 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*
NIST SP 800-70, Rev. 2, *National Checklist Program for IT Products--Guidelines for Checklist Users and Developers*
NIST SP 800-117, *Guide to Adopting and Using the Security Content Automation Protocol (SCAP), Version 1.0*
NIST SP 800-126, Rev. 1, *The Technical Specification for the Security Content Automation Protocol (SCAP), Version 1.1*
Draft NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*

General information about the **Risk Management Framework (RMF)** and access to standards and guidelines that pertain to the RMF, are available from the NIST Web page http://csrc.nist.gov/groups/SMA/fisma/framework.html.

Security Content Automation Protocol (SCAP) was designed to organize, express, and measure security-related information in standardized ways. SCAP supports the use of standard reference data, such as identifiers for post-compilation software flaws and security configuration issues. SCAP can be used to maintain the security of enterprise systems by automatically verifying the installation of patches, checking system security configuration settings, and examining systems for signs of compromise. General information about the SCAP program is available from the NIST Web page http://scap.nist.gov/.

For information about NIST standards and guidelines, and related publications, see the NIST Web page http://csrc.nist.gov/publications/index.html.

Information about NIST's information security programs is available from the Computer Security Resource Center at http://csrc.nist.gov.

Disclaimer
Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.