FISMA

Its not just about security
Its about managing risk

Terry W. Freeman

Compliance

Dictionary... "the state or fact of according with or meeting rules or standards."

The compliance process presupposes the existence of a governing standard or standards and an authoritative body to which organizations are accountable. In the case of FISMA, the E-Government Act (Public Law 107-347) passed by the 107th Congress and signed into law by the President in December 2002, recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. This act further detailed that an effective information security program should include:

- ✦ **Periodic assessments of risk**, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization.
- ✦ **Policies and procedures** that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each organizational information system.
- ✦ **Subordinate plans** for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate.
- ✦ **Security awareness training** to inform personnel (including contractors and other users of information systems that support the operations and assets of the organization) of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks.
- ✦ **Periodic testing** and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually.
- ✦ **A process for planning, implementing, evaluating**, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the organization.
- ✦ **Procedures for detecting, reporting, and responding** to security incidents.
- ✦ **Plans and procedures** to ensure continuity of operations for information systems that support the operations and assets of the organization.

FISMA, along with the Paperwork Reduction Act of 1995 and the Information Technology Management Reform Act of 1996 (Clinger-Cohen Act), explicitly emphasizes a risk-based policy for cost-effective security. In support of and reinforcing this legislation, the Office of Management and Budget (OMB), through Circular A-130, Appendix III, Security of Federal Automated Information Resources, requires executive agencies within the federal government to:

Plan for security. and ensure that appropriate officials are assigned security responsibility.

Periodically review the security controls in their information systems.

Authorize system processing prior to operations and, periodically, thereafter.

These management responsibilities presume that responsible agency officials understand the risks and other factors that could adversely affect their missions. Moreover, these officials must understand the current status of their security programs and the security controls planned or in place to protect their information and information systems in order to make informed judgments and investments that appropriately mitigate risk to an acceptable level. The ultimate objective is to conduct the day-to-day operations of the agency and to accomplish the agency's stated missions with adequate security, or security commensurate with risk, including the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. As a key element of the **FISMA** *Implementation Project*, **NIST** (National Institute of Standards and Technology) also developed an integrated *Risk Framework* which effectively brings together all of the **FISMA**-related security standards and guidance to promote the development of comprehensive and balanced information security programs by agencies.

Risk, Vulnerabilities & Threats

The FISMA framework is not a simple checklist. It is a risk-based process based on the rigorous application of a variety of policy guidelines in combination with sources of information on asset value, vulnerability and threats. It is important to understand these variables.

Risk is the probability that a loss will occur combined with the magnitude of that loss. In short, Risk is often expressed in terms of $$$. It is important to understand this simplification as well. Many would argue for qualitative measures as well but I suggest that this is ineffective.

Risk must be mitigated through the expenditure of budget and since budgets are not unlimited then all risk has a monetary evaluation. If an organization is unwilling or unable to come up with the budget to mitigate a risk then it is not prudent to operate and the operation must be changed to avoid the risk or it must cease to operate. If risk does not equal $$$ then how would any organization determine their budget for mitigating it or the budget for organization change to avoid it?

Let’s use another example. If an organization has a known risk and spends $1M on the compensating capability, how would anyone know if the $1M budget is adequate if there wasn’t a commensurate value on the risk. If a vendor comes along and provides a way to perform the same risk reduction for half the cost then does not the organization gain a monetary advantage for opting for the cheaper solution? Again all risk = $$$$ and the expenditure of $$$$ should be commensurate with risk.

Vulnerability is an important aspect because, in the absence of vulnerability, there can be no risk, regardless of the magnitude of the threat. Vulnerability is absolute. You are either vulnerable or not. Humans are vulnerable to bullets. You can mitigate the threat but the vulnerability remains. In the world of risk management, vulnerabilities are dealt with via compensating controls (armor, early warning devices and speed). Fortunately, in the world of information systems, vulnerabilities can be eliminated through design or code changes but, just as with humans and bullets, threats are always evolving to exploit even the same vulnerability and the ability to define and respond to a vulnerability in broader terms provides an advantage.

Vulnerability is the area where greater security effort is applied in the information world. We obsess over patches and apply enormous resources to keeping track of new vulnerabilities and searching for patches. While it represents the largest cost of most efforts, it also provides the most opportunity for cost reduction. Automation of discovery, and tracking of vulnerabilities (and their impact on risk) with respect to a given system can provide an enormous advantage.

Unfortunately, the risk visibility of vulnerabilities eludes most organizations and they end up over-spending on efforts to “patch everything” immediately (a futile endeavor). Imagine the value of being able to asses the impact of vulnerabilities on your risk equation at any given time.

Threats are the last component of the equation. Humans are vulnerable to bullets but if there were no bullets, would the vulnerability be unimportant? Unfortunately the vulnerability to bullets also translates into a vulnerability to other projectiles so the elimination of bullets would not reduce the risk equation unless there were no other projectiles capable of causing trauma. It would be more effective to define the vulnerability as one of weakness against projectiles of a given mass X velocity value. However, back to the threat part. If you are standing on a street corner in Fallujah., the threat of dangerous projectiles would likely be greater than if you were standing in an Amish Town where violent crime is almost non-existent.

How do we deal with threats? A threat is the opportunity and means to exploit a vulnerability. This is actually the most expensive aspect of the equation as it requires enormous effort in observation, intelligence gathering and, in the area of information systems, global visibility and it must be exercised in real time. Just as remediation of vulnerabilities reduces the risk equation, knowledge of threats and their alignment to a position of attack reduces the risk equation.

While mitigating threats is the most expensive, it is also the most flexible part of the equation. Because it deals with information in real time, it can accommodate much more targeted responses than is possible with vulnerabilities. So what are our objectives in the area of threat mitigation? Imagine how much more effective the effort would be with the availability of real time correlated information pertaining to value, vulnerability and threat.

It is tempting to deal with these issues on isolated terms but we do so at our peril. To mitigate risk we must:

- Determine our operational goals
- Know our environment
- Understand the relative urgency of vulnerabilities
- Manage the combination of patches and compensating controls to mitigate them,
- Maintain situational awareness of the threats that exist in our environment while being able to respond within our budget and maintain mission viability.

The FISMA framework is a means of providing this fusion of capability with operation. As stated earlier, it is not a simple one and requires rigorous attention to detail and continuous management using ever escalating technological advantages to gain the upper hand with respect to both effectiveness and cost.

FISMA Guideline Documents

The core standards documents for the FISMA process are:

- ✦ **NIST Special Publication 800-60, Revision 1 (**Volumes I and II), Guide for Mapping Types of Information and Information Systems to Security Categories.
- ✦ **NIST Special Publication 800-30**, Risk Management Guide for Information Technology Systems.
- ✦ **NIST Special Publication 800-39** (second public draft), NIST Risk Management Framework.
- ✦ **NIST Special Publication 800-37 Revision 1** (initial public DRAFT), Guide for Security Authorization of Federal Information Systems: A Security Life-cycle Approach.
- ✦ **NIST Special Publication 800-53 Revision 2**, Recommended Security Controls for Federal Information Systems.
- ✦ **NIST Special Publication 800-53A,** Guide for Assessing the Security Controls in Federal Information Systems.

NIST consults with other federal agencies and offices as well as the private sector to improve information security, avoid unnecessary and costly duplication of effort, and ensure that **NIST** standards and guidelines are complementary with standards and guidelines employed for the protection of national security systems. In addition to its comprehensive public review and vetting process, **NIST** is working with the Office of the Director of National Intelligence (ODNI), the Department of Defense (DOD), and the Committee on National Security Systems (CNSS) to establish a common foundation for information security across the federal government. The common foundation for information security will provide the Intelligence, Defense, and Civil sectors of the federal government and their support contractors, more uniform and consistent ways to manage the risk to organizational operations, organizational assets, individuals, other organizations, and the Nation from the operation and use of information systems.

The Risk Assessment Framework

A point of confusion for most organizations is focused around determining precisely what the **FISMA** framework applies to. While this may sound improbable, we have seen organizations attempt to compile exhaustive lists of hardware, software and network components to track and report on. Fortunately, **FISMA** documents make it clear that the object of risk assessment and protection is information systems (a set of things working together as parts of a mechanism or an interconnecting network). We accept that aggregating assets into meaningful systems is not a trivial task, but the identification of information processed on an information system is essential to the proper selection of security controls and ensuring the confidentiality, integrity, and availability of the system and its information. The NIST Special Publication (SP) 800-60 has been developed to assist Federal government agencies in the categorization of information and information systems. It contains two volumes. Volume I contains the basic guidelines for mapping types of information and information systems to security categories. The appendices, including security categorization recommendations for mission-based information types and rationale for security categorization recommendations, are published in Volume II.

Volume I provides the following background information and mapping guidelines:

- ✦ Section 2: Provides an overview of the value of the categorization process to agency missions, security programs and overall information technology (IT) management and the publication’s role in the system development life-cycle, the certification and accreditation process, and the **NIST** Risk Management Framework.
- ✦ Section 3: Provides the security objectives and corresponding security impact levels identified in the Federal Information Processing Standard 199, Standards for Security Categorization of Federal Information and Information Systems [FIPS 199].
- ✦ Section 4: Identifies the process, including:
    - ✦ Guidelines for identification of mission-based and management and support information types and the process used to select security impact levels
    - ✦ General considerations relating to security impact assignment
    - ✦ Guidelines for system security categorization, and considerations and guidelines for applying and interrelating system categorization results to the agency’s enterprise, large supporting infrastructures, and interconnecting systems.

SP 800-53 Security Controls

The selection and employment of appropriate security controls for an information system are important tasks that can have major implications on the operations and assets of an organization. Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. Organizations, when addressing the security considerations for their information systems, should answer the following questions:

- ✦What security controls are needed to adequately protect the information systems that support the operations and assets of the organization in order for that organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals?
- ✦Have the selected security controls been implemented or is there a realistic plan for their implementation?
- ✦What is the desired or required level of assurance (i.e., grounds for confidence) that the selected security controls, as implemented, are effective in their application?

The answers to these questions are not given in isolation but rather in the context of an effective information security program for the organization that identifies, controls, and mitigates risks to its information and information systems. The security controls defined in SP 800-53 (as amended), and recommended for use by organizations in protecting their information systems should be employed in conjunction with and as part of a well-defined and documented information security program. An effective information security program should include:

- ✦Periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization;
- ✦Policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level and address information security throughout the life cycle of each organizational information system;
- ✦Plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate;
- ✦Security awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the organization) of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks;
- ✦Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually;
- ✦A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the organization;
- ✦Procedures for detecting, reporting, and responding to security incidents;
- ✦Plans and procedures for continuity of operations for information systems that support the operations and assets of the organization.

The **SP 800-53** security controls are organized into classes and families for ease of use in the control selection and specification process. There are three general classes of security controls (i.e., management, operational, and technical) and 17 security control families. Each family contains security controls related to the security functionality of the family.

SECURITY CONTROL IDENTIFIERS, FAMILIES, AND CLASSES

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Certification, Accreditation, and Security Assessments	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational

The security control structure consists of three key components:

✦ a control section;

✦ a supplemental guidance section;

✦ a control enhancements section.

The following example from the Auditing and Accountability family illustrates the structure of a typical security control.

AU-2 AUDIT-ABLE EVENTS

Control: The information system generates audit records for the following events: [Assignment: organization-defined audit-able events]

Supplemental Guidance: The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of audit-able events. The organization defines audit-able events that are adequate to support after- the-fact investigations of security incidents. **NIST** Special Publication 800-92 provides guidance on computer security log management.

Control Enhancements:

(1) The information system provides the capability to compile audit records from multiple components throughout the system into a systemwide (logical or physical), time-correlated audit trail.

(2) The information system provides the capability to manage the selection of events to be audited by individual components of the system.

(3) The organization periodically reviews and updates the list of organization-defined audit able events.

LOW AU-2	**MOD** AU-2 (3)	**HIGH** AU-2 (1) (2) (3)

SP 800-53A Control Assessment

Security control assessments are not just about checklists, simple pass-fail results, or generating paperwork to pass inspections or audits—rather, security controls assessments are the principal vehicle used to verify that the implementers and operators of information systems are meeting their stated security goals and objectives. SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, is written to facilitate security control assessments conducted within an effective risk management framework. The assessment results provide organizational officials:

- ✦ Evidence about the effectiveness of security controls in organizational information systems;
- ✦ An indication of the quality of the risk management processes employed within the organization; and
- ✦ Information about the strengths and weaknesses of information systems which are supporting critical federal missions and applications in a global environment of sophisticated threats.

SP 800-53A covers both the security control assessment and continuous monitoring steps in the Risk Management Framework and provides guidance on the security assessment process. This guidance includes how to build effective security assessment plans and how to manage assessment results. SP 800-53A has been developed with the intention of enabling organizations to tailor and supplement the basic assessment procedures provided. The concepts of tailoring and supplementation used in this document are similar to the concepts described in SP 800-53. Tailoring involves scoping the assessment procedures to match the characteristics of the information system under assessment. The tailoring process provides organizations with the flexibility needed to avoid assessment approaches that are unnecessarily extensive or more rigorous than necessary. Supplementation involves adding assessment procedures or assessment details to adequately meet the organization's risk management needs (e.g., adding assessment objectives or adding organization-specific details such as system/platform-specific information for selected security controls). Supplementation decisions are left to the discretion of the organization in order to maximize flexibility in developing security assessment plans when applying the results of risk assessments in determining the extent, rigor, and level of intensity of the assessments.

While flexibility continues to be an important factor in developing security assessment plans, consistency of assessments is also an important consideration. A major design objective for SP 800-53A is to provide an assessment framework and initial starting point for assessment procedures that are essential for achieving such consistency.

Finally, it should be noted that for environments with credible threat information indicating sophisticated, well-resourced threat agents and possible attacks against high-value targets, additional assurances may be required. **NIST** SP 800-53 indicates the need for explicit risk acceptance or additional assurances for moderate-impact and high-impact information systems whenever the organization is relying on one or more security controls to mitigate risks from more capable threat sources.

AN EXAMPLE ASSESSMENT PROCEDURE

The following example illustrates an assessment procedure for security control CP-1. The assessment procedure includes a set of assessment objectives derived from the basic security control statement and a set of potential assessment methods and objects that can be used to make the determinations that lead to achieving the assessment objectives.

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

Supplemental Guidance: The contingency planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The contingency planning policy can be included as part of the general information security policy for the organization.

Contingency planning procedures can be developed for the security program in general, and for a particular information system, when required. **NIST** Special Publication 800-34 provides guidance on contingency planning. **NIST** Special Publication 800-12 provides guidance on security policies and procedures.

For security control CP-1, the assessment objectives are expressed as follows:

ASSESSMENT OBJECTIVE #1

Determine if:

(i) the organization develops and documents contingency planning policy and procedures;

(ii) the organization disseminates contingency planning policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review contingency planning policy and procedures; and

(iv) the organization updates contingency planning policy and procedures when organizational review indicates updates are required.

ASSESSMENT OBJECTIVE #2

Determine if:

(i) the contingency planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the contingency planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and

(iii) the contingency planning procedures address all areas identified in the contingency planning policy and address achieving policy-compliant implementations of all associated contingency planning controls.

In addition to specifying the assessment objectives, potential assessment methods and objects are also identified. The depth and coverage attributes associated with the assessment methods are implicit according to the impact level of the information system where the security controls are employed and assessed. Therefore, the expected level of effort expended by assessors in assessing a particular security control (i.e., the intensity and extent of the assessment activities) will vary based upon the impact level of the information system and the associated depth and coverage attributes. Appendix E provides more detailed information on assessment expectations and the values for depth and coverage attributes for each information system impact level. A complete assessment procedure for security control CP-1 consists of two assessment objectives and associated methods and objects as follows:

CP-1.1 ASSESSMENT OBJECTIVE:

Determine if:

(i) the organization develops and documents contingency planning policy and procedures;

(ii) the organization disseminates contingency planning policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review contingency planning policy and procedures; and

(iv) the organization updates contingency planning policy and procedures when organizational review indicates updates are required.

POTENTIAL ASSESSMENT METHODS AND OBJECTS:

Examine: *SELECT FROM:* Contingency planning policy and procedures; other relevant documents or records.

Interview: *SELECT FROM:* Organizational personnel with contingency planning and plan implementation responsibilities.

CP-1.2 ASSESSMENT OBJECTIVE:

Determine if:

(i) the contingency planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the contingency planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and

(iii) the contingency planning procedures address all areas identified in the contingency planning policy and address achieving policy-compliant implementations of all associated contingency planning controls.

POTENTIAL ASSESSMENT METHODS AND OBJECTS:

Examine: *SELECT FROM:* Contingency planning policy and procedures; other relevant documents or records.

Interview: *SELECT FROM:* Organizational personnel with contingency planning and plan implementation responsibilities.

If the security control has any enhancements, assessment objectives are developed for each enhancement using the same process as for the base control. The resulting assessment objectives within the assessment procedure are numbered sequentially.

Assessment Method Description

Assessing controls is accomplished via one or more of three methods which are:

(i) *examine*;

(ii) *interview*;

(iii) test.

The definitions include a set of attributes and attribute values for each of the assessment methods. The attribute values for the assessment methods (which describe the rigor and level of detail associated with the assessment) are hierarchical in nature. For the depth attribute, the focused attribute value includes and builds upon the assessment rigor and level of detail defined for the generalized attribute value; the detailed attribute value includes and builds upon the assessment rigor and level of detail defined for the focused attribute value. For the coverage attribute, the specific attribute value includes and builds upon the number and type of assessment objects defined for the representative attribute value; the comprehensive attribute value includes and builds upon the number and type of assessment objects defined for the specific attribute value.

Assessment Method: Examine

Assessment Objects Specifications (e.g., policies, plans, procedures, system requirements, designs)

Mechanisms (e.g., functionality implemented in hardware, software, firmware)

Activities (e.g., system operations, administration, management; exercises)

DEFINITION: The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time.

SUPPLEMENTAL GUIDANCE: Typical assessor actions may include, for example: reviewing information security policies, plans, and procedures; analyzing system design documentation and interface specifications; observing system backup operations, reviewing the results of contingency plan exercises; observing incident response activities; studying technical manuals and user/administrator guides; checking, studying, or observing the operation of an information technology mechanism in the information system hardware/software; or checking, studying, or observing physical security measures related to the operation of an information system.

ATTRIBUTES: Depth, Coverage

✦ The depth attribute addresses the rigor of and level of detail in the examination process. There are three possible values for the depth attribute: (i) generalized; (ii) focused; and (iii) detailed.

- **Generalized examination**: Examination that consists of high level reviews, checks, observations, or inspections of the assessment object. This type of examination is conducted using a limited body of evidence or documentation (e.g., functional-level descriptions for mechanisms; high-level process descriptions for activities; and actual documents for specifications). Generalized examinations provide a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors.
- **Focused examination**: Examination that consists of high-level reviews, checks, observations, or inspections and more in depth analyses of the assessment object. This type of examination is conducted using a substantial body of evidence or documentation (e.g., functional-level descriptions and where appropriate and available, high-level design information for mechanisms; high-level process descriptions and implementation procedures for activities; and the actual documents and related documents for specifications). Focused examinations provide a level of understanding of the security control necessary for determining whether the control is

implemented and free of obvious errors and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended.

- **Detailed examination**: Examination that consists of high-level reviews, checks, observations, or inspections and more in depth, detailed, and thorough analyses of the assessment object. This type of examination is conducted using an extensive body of evidence or documentation (e.g., functional-level descriptions and where appropriate and available, high-level design information, low-level design information, and implementation information for mechanisms; high-level process descriptions and detailed implementation procedures for activities; and the actual documents and related documents for specifications). Detailed examinations provide a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors and whether there are further increased grounds for confidence that the control is implemented correctly and operating as intended on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control.

✦The coverage attribute addresses the scope or breadth of the examination process and includes the types of assessment objects to be examined, the number of objects to be examined (by type), and specific objects to be examined. There are three possible values for the coverage attribute: (i) representative, (ii) specific, and (iii) comprehensive.

- **Representative examination**: Examination that uses a representative sample of assessment objects (by type and number within type) to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors.

- **Specific examination**: Examination that uses a representative sample of assessment objects (by type and number within type) and other specific assessment objects deemed particularly important to achieving the assessment objective to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended.

- **Comprehensive examination**: Examination that uses a sufficiently large sample of assessment objects (by type and number within type) and other specific assessment objects deemed particularly important to achieving the assessment objective to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors and whether there are further increased grounds for confidence that the control is implemented correctly and operating as intended on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control.

Assessment Method: Interview

ASSESSMENT OBJECTS: Individuals or groups of individuals.

DEFINITION: The process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence, the results of which are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time.

SUPPLEMENTAL GUIDANCE: Typical assessor actions may include, for example, interviewing agency heads, chief information officers, senior agency information security officers, authorizing officials, information owners, information system and mission owners, information system security officers, information system security managers, personnel officers, human resource managers, facilities managers, training officers, information system operators, network and system administrators, site managers, physical security officers, and users.

ATTRIBUTES: Depth, Coverage

✦The depth attribute addresses the rigor of and level of detail in the interview process. There are three possible values for the depth attribute: (i) generalized; (ii) focused; and (iii) detailed.

- **Generalized interview**: Interview that consists of broad-based, high-level discussions with individuals or groups of individuals. This type of interview is conducted using a set of generalized, high-level questions. Generalized interviews provide a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors.

- **Focused interview**: Interview that consists of broad-based, high-level discussions and more in depth discussions in specific areas with individuals or groups of individuals. This type of interview is conducted using a set of generalized, high-level questions and more in depth questions in specific areas where responses indicate a need for more in depth investigation. Focused interviews provide a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended.

- **Detailed interview**: Interview that consists of broad-based, high-level discussions and more in depth, probing discussions in specific areas (including other assessment results) with individuals or groups of individuals. This type of interview is conducted using a set of generalized, high-level questions and more in depth, probing questions in specific areas where responses indicate a need for more in depth investigation or where called for by assessment procedures. Detailed interviews provide a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors and whether there are further increased grounds for confidence that the control is implemented correctly and operating as intended on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control.

✦The coverage attribute addresses the scope or breadth of the interview process and includes the types of individuals to be interviewed (by organizational role and associated responsibility), the number of individuals to be interviewed (by type), and specific individuals to be interviewed. There are three possible values for the coverage attribute: (i) representative, (ii) specific, and (iii) comprehensive.

- **Representative interview**: Interview that uses a representative sample of individuals in key organizational roles to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors.

- **Specific interview**: Interview that uses a representative sample of individuals in key organizational roles and other specific individuals deemed particularly important to achieving the assessment objective to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended.

- **Comprehensive interview:** Interview that uses a sufficiently large sample of individuals in key organizational roles and other specific individuals deemed particularly important to achieving the assessment objective to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors and whether there are further increased grounds for confidence that the control is implemented correctly and operating as intended on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control.

Assessment Method: Test

ASSESSMENT OBJECTS: Mechanisms (e.g., hardware, software, firmware)

DEFINITION: The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time.

SUPPLEMENTAL GUIDANCE: Typical assessor actions may include, for example: testing access control, identification and authentication, and audit mechanisms; testing security configuration settings; testing physical access control devices; conducting penetration testing of key information system components; testing information system backup operations; testing incident response capability; and exercising contingency planning capability.

ATTRIBUTES: Depth, Coverage

✦The depth attribute addresses the types of testing to be conducted. There are three possible values for the depth attribute: (i) generalized testing; (ii) focused testing; and (iii) detailed testing.

- **Generalized testing:** Test methodology (also known as black box testing) that assumes no knowledge of the internal structure and implementation detail of the assessment object. This type of testing is conducted using a functional specification for mechanisms and a high-level process description for activities. Generalized testing provides a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors.

- **Focused testing:** Test methodology (also known as gray box testing) that assumes some knowledge of the internal structure and implementation detail of the assessment object. This type of testing is conducted using a functional specification and limited system architectural information (e.g., high-level design) for mechanisms and a high-level process description and high-level description of integration into the operational environment for activities. Focused testing provides a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended.

- **Detailed testing:** Test methodology (also known as white box testing) that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. This type of testing is conducted using a functional specification, extensive system architectural information (e.g., high-level design, low-level design) and implementation representation (e.g., source code, schematics) for mechanisms and a high-level process description and detailed description of integration into the operational environment for activities. Detailed testing provides a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors and whether there are further increased grounds for confidence that the control is implemented correctly and operating as intended on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control.

✦The coverage attribute addresses the scope or breadth of the testing process and includes the types of assessment objects to be tested, the number of objects to be tested (by type), and specific objects to be tested. There are three possible values for the coverage attribute: (i) representative; (ii) specific; and (iii) comprehensive.

- **Representative testing:** Testing that uses a representative sample of assessment objects (by type and number within type) to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors.

- **Specific testing**: Testing that uses a representative sample of assessment objects (by type and number within type) and other specific assessment objects deemed particularly important to achieving the assessment objective to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended.

- **Comprehensive testing:** Testing that uses a sufficiently large sample of assessment objects (by type and number within type) and other specific assessment objects deemed particularly important to achieving the assessment objective to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors and whether there are further increased grounds for confidence that the control is implemented correctly and operating as intended on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control.

ASSESSMENT EXPECTATIONS

The following section establishes the expectations for security control assessments based on the assurance requirements defined in **NIST** Special Publication 800-53. The assessment expectations provide assessors with important reference points for the level of assurance (i.e., grounds for confidence) needed for the determination of security control effectiveness.

LOW-IMPACT INFORMATION SYSTEMS

Assurance Requirement: The security control is in effect and meets explicitly identified functional requirements in the control statement. Supplemental Guidance: For security controls in low-impact information systems, the focus is on the controls being in place with the expectation that no obvious errors exist and that, as flaws are discovered, they are addressed in a timely manner.

Assessment Expectations: Generalized interviews, examinations, and tests are conducted using a representative set of assessment objects to demonstrate that the security control is implemented and free of obvious errors.

ASSESSMENT OBJECTIVES:

For specifications, determine if:

(i) the specification exists;

(ii) the specification, as written, has no obvious inconsistencies with the functional requirements in the security control and no obvious internal errors.

For mechanisms, determine if:

(i) the mechanism is implemented and operational;

(ii) the mechanism, as implemented, has no obvious inconsistencies with the functional requirements in the security control and no obvious implementation errors.

For activities, determine if:

(i) the activity is being performed;

(ii) the activity, as performed, has no obvious inconsistencies with the functional requirements in the security control and no obvious internal errors.

MODERATE-IMPACT INFORMATION SYSTEMS

Assurance Requirement: The security control is in effect and meets explicitly identified functional requirements in the control statement. The control developer/implementer provides a description of the functional properties of the control with sufficient detail to permit analysis and testing of the control. The control developer/implementer includes as an integral part of the control, assigned responsibilities and specific actions supporting increased confidence that when the control is implemented, it will meet its required function or purpose. These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination.

Supplemental Guidance: For security controls in moderate-impact information systems, the focus is on actions supporting increased confidence in the correct implementation and operation of the control. While flaws are still likely to be uncovered (and addressed expeditiously), the control developer/implementer incorporates, as part of the control, specific capabilities and produces specific documentation supporting increased confidence that the control meets its required function or purpose. This documentation is also needed by assessors to analyze and test the functional properties of the control as part of the overall assessment of the control.

Assessment Expectations: Focused interviews, examinations, and tests are conducted using a specific set of assessment objects to demonstrate that the security control is implemented and free of obvious errors, and that there are increased grounds for confidence that the security control is implemented correctly and operating as intended.

ASSESSMENT OBJECTIVES:

For specifications, determine if:

(i) the specification exists;

(ii) the specification, as written, has no obvious inconsistencies with the functional requirements in the security control and no obvious internal errors;

(iii) if the organization provides an assignment of responsibilities, specific actions, and appropriate documentation to support increased grounds for confidence that the specification is complete, internally consistent, correct, and meets its required function or purpose; and

(iv) the organization identifies and documents anomalies or problems with the application or use of the specification.

For mechanisms, determine if:

(i) the mechanism is implemented and operational;

(ii) the mechanism, as implemented, has no obvious inconsistencies with the functional requirements in the security control and no obvious implementation errors.

(iii) if the organization provides an assignment of responsibilities, specific actions, and appropriate documentation to support increased grounds for confidence that the mechanism is implemented correctly, operating as intended, and meets its required function or purpose; and

(iv) the organization identifies and documents anomalies or problems with the implementation or operation of the mechanism.

For activities, determine if:

(i) the activity is being performed;

(ii) the activity, as performed, has no obvious inconsistencies with the functional requirements in the security control and no obvious execution errors.

(iii) if the organization provides an assignment of responsibilities, specific actions, and appropriate documentation to support increased grounds for confidence that the activity is being performed and meets its required function or purpose; and

(iv) the organization identifies and documents anomalies or problems with the conduct or execution of the activity.

HIGH-IMPACT INFORMATION SYSTEMS

Assurance Requirement: The security control is in effect and meets explicitly identified functional requirements in the control statement. The control developer/implementer provides a description of the functional properties and design/implementation of the control with sufficient detail to permit analysis and testing of the control (including functional interfaces among control components). The control developer/implementer includes as an integral part of the control, assigned responsibilities and specific actions supporting increased confidence that when the control is implemented, it will continuously and consistently (i.e., across the information system) meet its required function or purpose and support improvement in the effectiveness of the control. These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination.

Supplemental Guidance: For security controls in high-impact information systems, the focus is expanded to require, within the control, the capabilities that are needed to support ongoing consistent operation of the control and continuous improvement in the control's effectiveness. The developer/implementer is expected to expend significant effort on the design, development, implementation, and component/integration testing of the controls and to produce associated design and implementation documentation to support these activities. This documentation is also needed by assessors to analyze and test the internal components of the control as part of the overall assessment of the control.

Assessment Expectations: Detailed interviews, examinations, and tests are conducted using a comprehensive set of assessment objects to demonstrate that the security control is implemented and free of obvious errors and that there are further increased grounds for confidence that the security control is implemented correctly and operating as intended on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control.

ASSESSMENT OBJECTIVES:

For specifications, determine if:

(i) the specification exists;

(ii) the specification, as written, has no obvious inconsistencies with the functional requirements in the security control and no obvious internal errors;

(iii) if the organization provides an assignment of responsibilities, specific actions, and appropriate documentation to support increased grounds for confidence that the specification is complete, internally consistent, correct, and meets its required function or purpose; and

(iv) the organization identifies and documents anomalies or problems with the application or use of the specification.

(v) if the organization applies the specification consistently across the information system; and

(vi) if the organization supports improvements in the effectiveness of the specification by taking specific actions to correct identified deficiencies.

For mechanisms, determine if:

(i) the mechanism is implemented and operational;

(ii) the mechanism, as implemented, has no obvious inconsistencies with the functional requirements in the security control and no obvious implementation errors.

(iii) if the organization provides an assignment of responsibilities, specific actions, and appropriate documentation to support increased grounds for confidence that the mechanism is implemented correctly, operating as intended, and meets its required function or purpose;

(iv) the organization identifies and documents anomalies or problems with the implementation or operation of the mechanism.

(v) if the organization implements the mechanism consistently across the information system; and

(vi) if the organization supports improvement in the effectiveness of the mechanism by taking specific actions to correct identified deficiencies.

For activities, determine if:

(i) the activity is being performed;

(ii) the activity, as performed, has no obvious inconsistencies with the functional requirements in the security control and no obvious execution errors;

(iii) if the organization provides an assignment of responsibilities, specific actions, and appropriate documentation to support increased grounds for confidence that the activity is being performed and meets its required function or purpose;

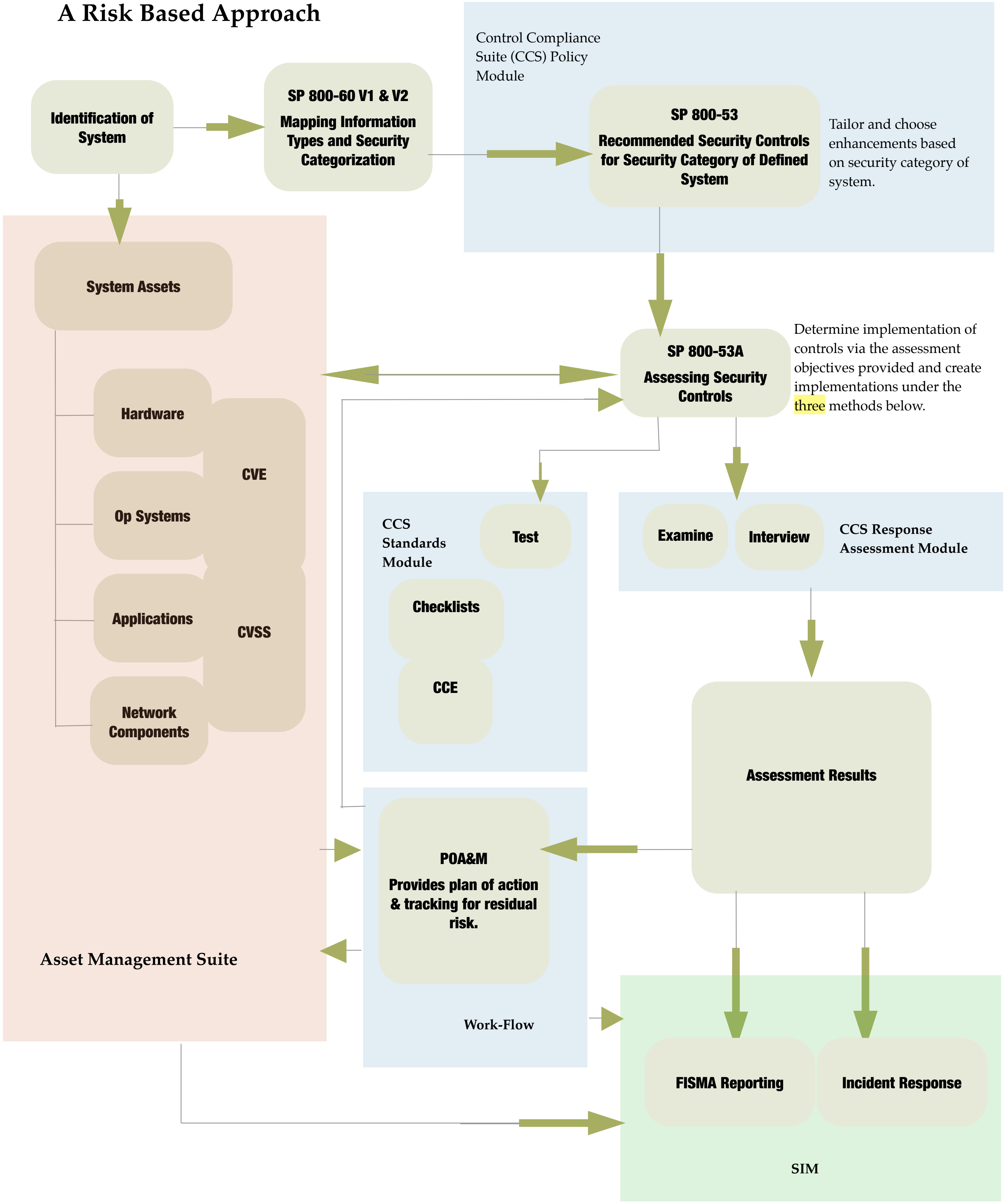
(iv) the organization identifies and documents anomalies or problems with the conduct or execution of the activity.

(v) if the organization performs the activity consistently across the information system; and

(vi) if the organization supports improvement in the effective actions to correct identified deficiencies.

-

A Risk Based Approach


Control Compliance Suite (CCS) Policy Module
Identification of System
SP 800-60 V1 & V2
Mapping Information Types and Security Categorization
SP 800-53
Recommended Security Controls for Security Category of Defined System
System Assets
Hardware
Op Systems
Applications
Network Components
CVE
CVSS
SP 800-53A
Assessing Security Controls
CCS Standards Module
Test
Checklists
CCE
Examine
Interview
CCS Response Assessment Module
Assessment Results
POA&M
Provides plan of action & tracking for residual risk.
Work-Flow
Asset Management Suite
FISMA Reporting
Incident Response
SIM

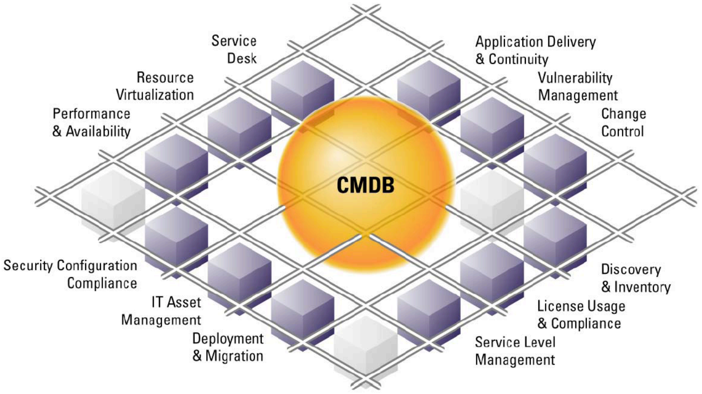
Tailor and choose enhancements based on security category of system.

Determine implementation of controls via the assessment objectives provided and create implementations under the three methods below.

Symantec's -Risk Based Approach

Identifying the system : Identifying a system requires that an organization have an active management system for its asset inventory. This is not a simple scan of the network for OS, versions etc. but a comprehensive inventory of hardware, operating system, images, network connectivity, patch levels and life-cycle information. All this and more aggregated into groups that share in the processing of a particular type of information such as HR, Public Affairs, Finance etc.

Symantec's Service & Asset Management Suites meet this requirement with exhaustive capability to manage all of the critical asset information from procurement to retirement as well as ongoing patching and work flow control. Consider how an accrediting authority would track FISMA compliance if he/she did not know when the system configuration changed.



One of the major obstacles to FISMA compliance is that there is rarely budget to accommodate it so wouldn't it be great if it could actually represent a cost savings that would enable its execution. Gartner estimates that organizations that begin a asset management program experience up to 30 percent reduction in cost per asset in the first year. This includes people, process and technology costs. Continued savings of 5 to 10 percent annually over the following five years is typical.

Generating the control set : Once identified, a system is categorized for risk on the basis of the information it processes. In the case of FISMA this categorization is in terms of Low, Moderate or High risk. NIST SP 800-53 specifically itemizes the minimum set of controls for systems by security category providing a quick population of Symantec's Control Compliance Suite (CCS) Policy Module. These controls are not rigid but are guidelines and can be tailored and enhanced to meet specific organizational needs. The power of implementing this automated control set generation is that the Certification & Accreditation (C&A) process becomes repeatable and predictable.

Consider the amount of time and money that a typical organization spends performing a C&A on a system manually with MS Word Documents and MS Excel spreadsheets. SANS institute estimated that agencies are spending from $25,000 to $400,000 per system on C&A. Also consider that a study of lessons learned from the first year under the FISMA Act pinpointed that certification and accreditation is the most important aspect of compliance and that a program that addresses security problems proactively instead of waiting for an annual evaluation can reduce C&A costs to $5500 per system. These are savings that, even if estimates, can not be ignored.

Assessing the control set : So, what do you do with a control set once you have tailored it to your specific environment and made the appropriate enhancements? Symantec's CCS provides three ways to assess a control per FISMA policy. 1) You can test the control through a checklist or standard in the "Standards Module" if the control lends itself to a technical check. 2) You can user the CCS Response Assessment Module to create a template for a member of the assessment team or IT to complete through examination of the system to satisfy the "examine" requirements. 3) You can use the Response Assessment Module to create a questionnaire for organizational personnel to answer to satisfy the interview requirement.

This is another area of significant time and cost savings. Besides that the turnaround time for completing an assessment is radically reduced due to the manageability of the process through online validation and verification throughout the work-flow.

Managing the POA&M : Now we come to everyone's worst nightmare. How do you stay up to date with your real risk. Its one thing to go through a C&A and say "Congratulations to us we're compliant".... for now. Its another to actually be able to perform the continuous monitoring and risk management that FISMA calls for without breaking the bank. Remember the whole idea of risk management is mission assurance. If you run out of money, your mission fails. Symantec's work-flow solution provides a flexible way to manage the changes and varied organizational processes that are required to assess the impact of new vulnerabilities and effectiveness of new patches against the changing configurations of an organization's many systems. There is also the problem of identifying and processing incidents which arise from unexpected vulnerabilities and threats to your assets.

The other aspect of continuous monitoring is the plethora of reporting demands that the FISMA program or any regulatory mandate imposes. With Symantec's management console, CMDB, and incident management system, all information needed for accurate and timely reporting is available on demand.

The Challenge: Ask yourself this question: How much does my organization spend tracking its systems, patching its systems, repairing and restoring systems, maintaining patch levels and assessing risk. Now ask yourself another question. How accurately and timely are we in performing these operations.

Remember:

- **Risk** is infinite... Budgets are not
- Risk compromises **mission**
- Visibility & Control is prerequisite to **action**
- Action reduces **risk**

Symantec's solution stack for IT infrastructure and risk management enables action at reduced cost and ensures mission success.