IS audit basics

Navigating the US Federal Government Agency ATO Process for IT Security Professionals

IT security professionals such as risk managers and information security managers maintain a US federal government agency's information system using the Federal Information Security Management Act (FISMA) in a manner that is unique to the US federal government. To do so, they encounter the Authority to Operate (ATO) security authorization process, which is in place for the security of the agency's information systems.

The ATO is the authority to operate decision that culminates from the security authorization process of an information technology system in the US federal government, which is a unique industry requiring specialized practices. **Figure 1** provides information about an ATO.

Figure 1—Authority to Operate (ATO)

The authorizing official (AO) signs the formal statement of risk acceptance, accepting the system's security risk. This should be done before the system or upgrade goes into production.

There are usually three types of ATOs:
- **Initial ATO**—Must be done prior to the system "going live" and must occur at least every three years thereafter
- **Interim ATO**—A conditional ATO, generally in effect for six months, often during the development or prototype phase
- **Reauthorization**—Due after three years or a significant change to the system's risk level

NOTE: Agencies call this ATO process either the Certification and Authorization (C&A) or the Assessment and Authorization (A&A) security authorization process.

Source: J. Bennerson. Reprinted with permission.

Jo Anna Bennerson, CISA, CGEIT, CPA, ITILv3, PMP
Has more than 20 years of experience as a consultant in the role of information systems security officer for US federal government agencies, having launched her career as a certified public accountant and project manager working in the financial services industry. She has served as a Malcom Baldrige National Quality Award examiner. Bennerson can be reached at *joanna_bennerson@yahoo.com.*

This article discusses approaches to increase an information security professional's knowledge about the US federal government ATO security authorization process and one's duties in the narrow US federal government industry.

The ATO security process is in place for the federal government agency to determine whether to grant a particular information system authorization to operate for a certain period of time by evaluating if the risk of security controls can be accepted. The ATO process:

- Is not an audit, nor is it to be termed an ATO audit
- Documents the security measures taken and the security process in place for US federal government agencies by focusing on a specific system
- Produces documentation that can sometimes be used as evidence in another assessment such as an internal audit, for example, by sharing copies of change management requests that can be used. Shared documentation often can be used as part of an integrated assurance process.
- Often engages professionals across many areas of different federal agencies to cover security and privacy controls. No qualifications are spelled out for those engaged in the ATO process. For example, someone from the budget department may be asked about acquisition documents, a system administrator may be asked to provide a procedure about access provisioning, or a project manager may be requested to present a project plan that highlights the timeline for corrective actions to be implemented in the system.
- Has no current skill gap and does not denote the need for particular global certifications. However, Certified Information Systems Auditor® (CISA®), Certified in Risk and Information Systems Control™ (CRISC™), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) or other IT professional certification and experience will likely more rapidly engage one in the ATO process.

ATO Process Steps and Knowing the IT Governance Frameworks

To understand the ATO process, one needs to understand the IT governance frameworks. The required steps for conducting the ATO security authorization process are:

1. Categorize the information systems in the organization, i.e., determine the criticality of the information system based on potential adverse impact to the business.
2. Select baseline security controls.
3. Implement these security controls, i.e., implement security controls within the agency's enterprise architecture.
4. Assess the security controls to determine their effectiveness.
5. Authorize the system.
6. Monitor the system.

> **"To understand the ATO process, one needs to understand the IT governance frameworks."**

The information security professional works to gather the documentation for the system project deliverables from the phases (planning, requirements, design, development, testing,

Figure 2—US Federal Government IT Security Governance

Privacy Act of 1974[1]	Established a Code of Fair Information Practice that governs the collection, maintenance, use and dissemination of personally identifiable information (PII) about individuals that is maintained in systems of records by federal agencies.
Clinger-Cohen Act	The Information Technology Management Reform Act of 1996; emphasizes a risk-based policy for cost-effective security.[2, 3]
Federal Information Security Management Act of 2002 (FISMA) under Title III of the E-Government Act (Public Law 107-347)	Requires each federal agency to develop, document and implement an agencywide 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. Information security protections are to be commensurate with the risk and magnitude of the harm.[4] FISMA (2002) assigns roles to the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST).
Office of Management and Budget	The OMB, through Circular No. A-130, Appendix 111, Security of Federal Automated Information Resources[5] requires executive agencies in the federal government to: • Plan for security • 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 The director of OMB has oversight of agency information security policies and practices.[6]
National Institute of Standards and Technology	NIST develops information security standards: • Federal Information Processing Standards (FIPS), which are mandatory • Special Publications (SPs) in the 800-series for non-national security federal information systems, which provide guidance • Standards to be used by federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels • Guidelines recommending the types of information and information systems to be included in each category • Minimum information security requirements (management, operational and technical security controls) for information and information systems in each such category[7]

Source: J. Bennerson. Reprinted with permission.

implementation and maintenance) of the Software Development Life Cycle (SDLC)[8] or System Engineering Life Cycle (SELC)[9] frameworks. This information is needed as documentation in the ATO process and shows evidence of the categorize, select, implement and assess steps while simultaneously fulfilling the stated IT governance frameworks.

Figure 2 is a brief overview of US federal government IT security governance.

The key staff in the ATO process with whom one should quickly become acquainted are the authorizing official (AO), the information systems security officer (ISSO) and the security assessor.[10] Often, the chief information security officer (CISO) and/or privacy officer serve as the authorizing official. This person is referred to as the senior agency information security official (SAISO) who is the point of contact within a federal government agency and is responsible for its information system security.[11]

The ISSO works with the system owner serving as a principal advisor on all matters involving the security of the IT system. The ISSO has the detailed knowledge and expertise required to manage its security aspects.

The security assessor conducts a comprehensive assessment of the management, operational and technical security controls, and control enhancements employed within or inherited by an information system to determine the overall effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting its security requirements).

Generally, the ISSO works with the IT team to prepare the required documents—system security plan (SSP), privacy threshold analysis (PTA), contingency plan (CP), etc. Then, the security assessor evaluates the information and prepares a security assessment report (SAR). When all is completed, the AO grants the ATO. Often, auditors can leverage this information for their audits.

Figure 2—US Federal Government IT Security Governance *(cont.)*

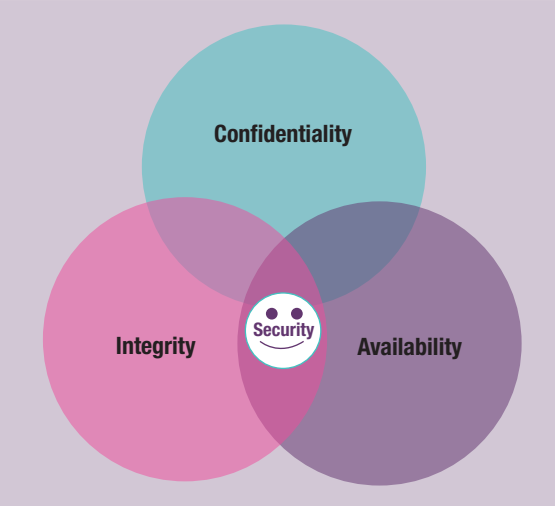
Federal Information Security Modernization Act of 2014 "FISMA 2014" Public Law No: 113-283 (12/18/2014)	FISMA was updated in 2014 to include cyberbreach notification requirements and roles were added for the Department of Homeland Security (DHS).[12]
Department of Homeland Security	DHS roles include: • Assisting the OMB director in administering the implementation of agency information and security practices for federal information systems • Providing operational and technical assistance to DHS agencies[13] DHS issues Homeland Security Presidential Directives (HSPDs).
US Computer Emergency Readiness Team (US-CERT)—The federal incidence response center created by Congress in 2002; operates under DHS since 2003.	US-CERT's critical mission activities include: • Providing cybersecurity protection to federal civilian executive branch agencies through intrusion detection and prevention capabilities • Developing timely and actionable information for distribution to federal departments and agencies; state, local, tribal and territorial (SLTT) governments; critical infrastructure owners and operators; private industry; and international organizations • Responding to incidents and analyzing data about emerging cyberthreats • Collaborating with foreign governments and international entities to enhance the nation's cybersecurity posture[14]
There are also Executive Orders (EOs) and Presidential Directives (PDs) for IT security and other legislation, standards and frameworks such as: • **Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)**—Generally for US military organizations[15] • **Committee on National Security Systems (CNSS)**—Generally for US intelligence agencies • **Federal Risk Authorization Management Program (FEDRAMP)**—Governmentwide program that provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services[16]	

Source: J. Bennerson. Reprinted with permission.

Securing With CIA

The overall objective of an information security program is to protect the information and systems that support the operations and assets of the agency via the security objectives shown in **figure 3**:

Figure 3—Confidentiality, Integrity, Availability



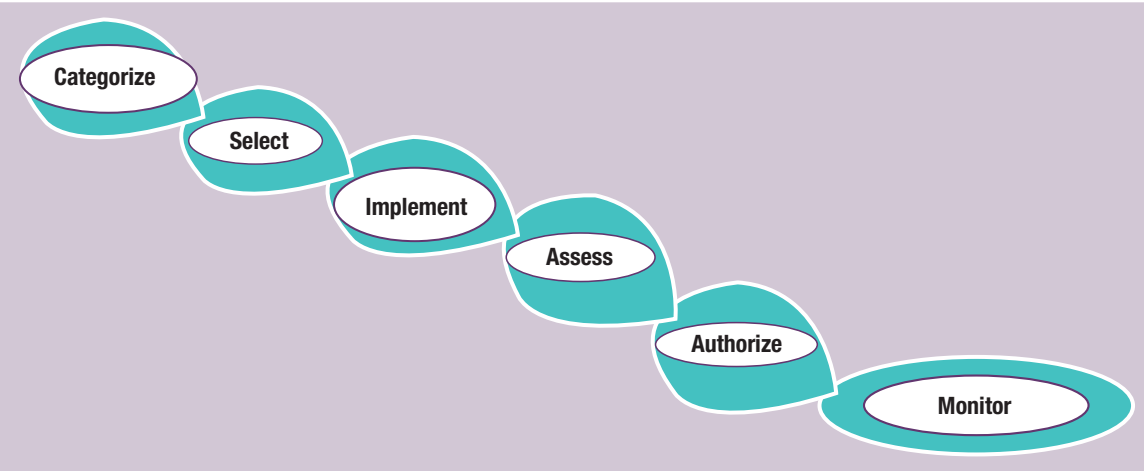
Source: J. Bennerson. Reprinted with permission

- **Confidentiality**—Preserving authorized restrictions on information access and disclosure
- **Integrity**—Guarding against unauthorized information modification or destruction
- **Availability**—Ensuring timely and reliable access to and use of information

Comprehending the NIST Risk Management Framework (RMF)[17] sets the foundation for understanding how the security life cycle of the IT system is being operated and evaluated. From the agency's inventory of its IT systems, the agency will use its own criteria to determine what may be a system that could be part of a FISMA audit, hence a FISMA reportable system. These tend to be the financial reporting systems, general support systems (GSS) and major applications (MA). To accomplish an ATO security authorization, there are six steps in the RMF to be completed (**figure 4**):

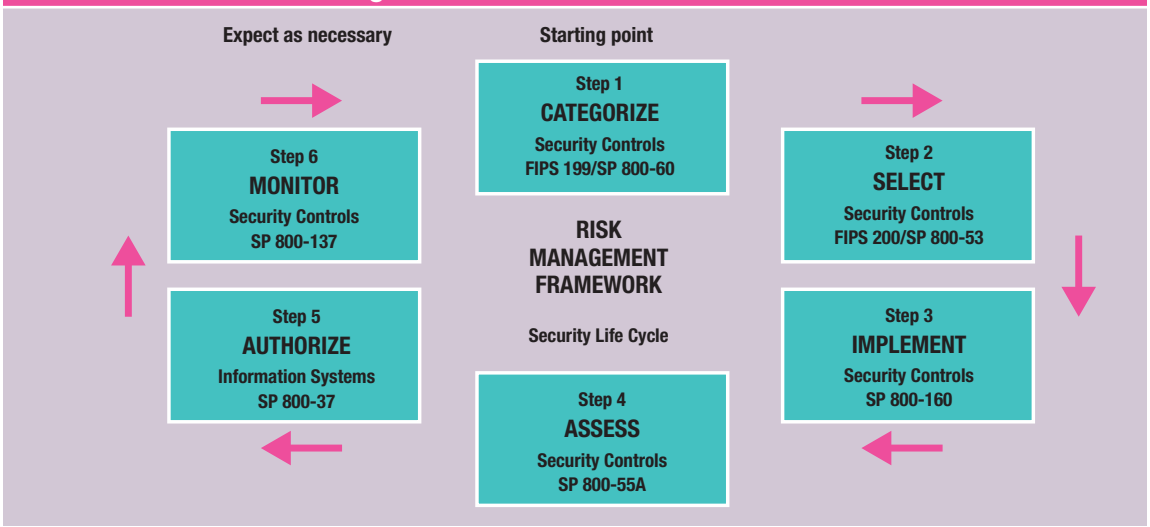
1. **Categorize**—What is the system's overall risk level, based on the security objectives of confidentiality, integrity and availability? Has it been categorized as high, moderate or low impact? Is it a GSS, MA, minor application or subsystem? Delineating and documenting the system boundary is key.[18]
2. **Select**—Using the system's categorization, have the appropriate level of controls been chosen? Systems will be assessed at the operating system, application and database layers. What controls are being selected to mitigate risk? Baseline security controls of the safeguards or countermeasures employed and specifying minimum assurance requirements are in this step.
3. **Implement**—Are the individual controls implemented or planned, or are there compensating controls in place? Are the controls inherited from another system or from common controls, or are they system specific or hybrid? What can demonstrate the controls?

Figure 4—Six Steps in RMF



Source: J. Bennerson. Reprinted with permission

Figure 5—NIST RMF From SP 800-37



Source: US National Institute of Standards and Technology. Reprinted with permission.

4. **Assess**—Through verification of evidence, the controls are tested to determine if they are in place and operating as intended.
5. **Authorize**—Documents are submitted to the AO, who will either accept or deny the system's risk in an accreditation decision. An accreditation package consists of:[19]
   - Accreditation decision letter
   - System security plan (SSP)—Criteria provided on when the plan should be updated
   - Security assessment report (SAR)—Updated on an ongoing basis for changes made to either the security controls in this information system or to inherited common controls
   - Plan of action and milestones (POAMs) for any remaining remediation of outstanding issues or deficiencies
6. **Monitor**—NIST states that the objective of a continuous monitoring program is to determine if the complete set of planned, required and deployed security controls within an information system or inherited by the system continue to be effective over time in light of the inevitable changes that occur. POAMs address changes to the system;[20] NIST SP, 800-137 provides guidance (**figure 5**).[21]

Security Controls

Figure 6 shows the NIST RMF steps for ATO. There are three classes of security controls: management, operational and technical (MOT). These controls are divided into 18 control families. **Figure 7** shows security control families and MOT controls.

Engaging With the ATO Process

The assess step involves answering the following questions:

- Is the system a GSS or MA or minor application or subsystem?
- Learning its history, the roles and responsibilities, current state, its system boundaries and which controls are in place or planned?
- Who executes the controls and where to get evidence such as IP and user access lists (ACLs)?

Figure 6—RMF Steps for ATO

Security controls are the management, operational and technical safeguards or countermeasures employed within an information system to protect the confidentiality, integrity and availability of the system and its information.[22, 23]		
RMF	**SP 800-37 Rev. 1**	"Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach"[24]
Step 1: CATEGORIZE Security impact value (low, moderate, high) for the security objectives of confidentiality, integrity or availability.		
	FIPS 199	"Standards for Security Categorization of Federal Information and Information Systems"[25]
	SP 800-60	"Guide for Mapping Types of Information and Information Systems to Security Categories"[26, 27]
Step 2: SELECT Choosing a set of baseline security controls and specifying minimum assurance requirements (safeguards or countermeasures employed), as appropriate.		
	FIPS 200	Minimum Security Requirements for Federal Information and Information Systems[28]
	SP 800-53 Rev 4	"Security and Privacy Controls for Federal Information Systems and Organizations"[29]
Step 3: IMPLEMENT Controls are: A. Implemented/Compensated/Planned B. System Specific/Inherited/Hybrid		
	SP 800-160	Draft document
Step 4: ASSESS By verification of evidence, test that the controls are in place and operating as intended.		
	SP 800-53A	"Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans"[30]
Step 5: AUTHORIZE		
	SP 800-37	"Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach"[31, 32]
Step 6: MONITOR POAMS		
	SP 800-137	"Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations"[33]

Source: J. Bennerson. Reprinted with permission.

Figure 7—Security Control Families and MOT

ID	Family	ID	Family
AC	Access Control	**MP**	Media Protection
AT	Awareness and Training	**PE**	Physical and Environmental Protection
AU	Audit and Accountability	**PL**	Planning
CA	Security Assessment and Authorization	**PS**	Personnel Security
CM	Configuration Management	**RA**	Risk Assessment
CP	Contingency Planning	**SA**	System and Services Acquisition
IA	Identification and Authentication	**SC**	System and Communications Protection
IR	Incident Response	**SI**	System and Information Integrity
MA	Maintenance	**PM**	Program Management

NIST SP 800-53 Rev. 4
18 Control Families–Comprised of three classes:
- Management controls—Normally addressed by management
- Operational controls—Primarily implemented and executed by people
- Technical controls—Focus on security controls that the computer system executes

Source: US National Institute of Standards and Technology. Reprinted with permission.

- Who provisions access, when are scans run and how are incident reports handled?
- Who is the contact?
- What is the evidence of other IT controls (including written documentation, i.e., policies, standard operating procedures [SOPs], service level agreements [SLAs], delegations of authority, common controls, URLs, screen shots)?
- What is the level of privacy, including PII?

One should request or set a significant lead time to start collecting information for a preliminary or draft of what is historically termed an auditor's request, the Provided by Client (PBC) list, of schedules, documents, questions, requested spreadsheets, or read-only access to certain repositories or systems.

In summary, one should make full use of NIST 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," which emphasizes security and privacy controls.[34] Then, use NIST 800-53A, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans," to assess the controls.[35] In the federal government, there is usually:

- The ISSO or ISSO team
- A separate independent assessment team (security assessors) that reviews what the ISSO team has done

These two teams get everything ready for the authorization package in the C&A or A&A security authorization process.

The authorizing official reviews the package to make an ATO decision to grant or deny authorization of the system to operate for three years. If there is significant change to the system, it will need to be reauthorized.[36] Remember continuous monitoring and think POAMs.

Conclusion

As an information security professional, one can quickly navigate the US federal government's industry-specific practices by understanding its ATO process. Using traditional IT security knowledge and becoming familiar with the IT governance of the US federal government, one can understand the process that results in an ATO decision. This is the decision that the information security professional's federal agency AO makes to accept the risk of the IT system. The ISSO and security assessor teams have documentation that has been developed through the agency's C&A or A&A security process.

When undertaking work from a FISMA perspective, one should also learn more about the NIST RMF and how controls are planned and implemented to mitigate risk through use of NIST guidance—FIPS 199, FIPS 200, SP 800-53 Rev.4 and SP 800-53A. This knowledge will not only build a sturdy introductory foundation, but will also serve as the baseline protocol for federal government IT security guidance.

Endnotes

1 Executive Office of the President of the United States, Office of Management and Budget, "M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," 26 September 2003, *www.whitehouse.gov/omb/memoranda_m03-22*

2 The National Partnership for Reinventing Government, Archive, "Summary: Information Technology Management Reform Act of 1996," *http://govinfo.library.unt.edu/npr/library/misc/itref.html*

3 National Institute of Standards and Technology, Federal Information Security Management Act of 2002, "Detailed Overview," USA, 25 August 2016, *http://csrc.nist.gov/groups/SMA/fisma/overview.html*

4 *Ibid*.

5 Executive Office of the President of the United States, Office of Management and Budget, "Circular No. A-130 Revised," 28 November 2000, *www.whitehouse.gov/omb/circulars_a130_a130trans4*

6 *Op cit,* National Institute of Standards and Technology, 25 August 2016

7 National Institute of Standards and Technology, "NIST Special Publications (SP)," USA, 8 April 2016, *http://csrc.nist.gov/publications/PubsSPs.html*

8 *ComputerWorld*, "System Development Life Cycle," 14 May 2001, *www.computerworld.com/article/2576450/app-development/app-development-system-development-life-cycle.html*

9 Department of Homeland Security, Office of Inspector General, "CBP Information Technology Management Strengths and Challenges," USA, June 2012, fig. 4, p. 12, *www.oig.dhs.gov/assets/Mgmt/2012/OIG_12-95_Jun12.pdf*

10 National Institute of Standards and Technology, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, Revision 1," NIST SP 800-37, USA, February 2010, Appendix D, *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf*

11 Department of Homeland Security, "DHS Sensitive Systems Policy, Directive 4300A, Version 11.0," USA, 14 January 2015, *www.dhs.gov/xlibrary/assets/foia/mgmt_directive_4300a_policy_v8.pdf*

12 Department of Homeland Security, "Federal Information Security Modernization Act (FISMA)," USA, 3 October 2016, *www.dhs.gov/fisma*

13 *Ibid*.

14 Department of Homeland Security, United States Computer Emergency Readiness Team, "About Us," USA, *www.us-cert.gov/about-us*

15 Department of Defense, Personnel and Readiness Information Management, "Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)," USA, *www.prim.osd.mil/Documents/DIACAP_Slick_Sheet.pdf*

16 General Services Administration, "FedRAMP Federal Risk and Authorization Management Program," USA, *www.gsa.gov/portal/category/102371*

17 *Op cit,* National Institute of Standards and Technology, February 2010

18 *Op cit,* Department of Homeland Security, 14 January 2015

19 *Ibid*.

20 National Institute of Standards and Technology, "Frequently Asked Questions, Continuous Monitoring," USA, *http://csrc.nist.gov/groups/SMA/fisma/documents/faq-continuous-monitoring.pdf*

21 National Institute of Standards and Technology, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations," NIST SP 800-137, USA, September 2011, *http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf*

22 *Op cit,* National Institute of Standards and Technology, 8 April 2016

23 National Institute of Standards and Technology, "FIPS Publications," USA, 16 October 2015, *http://csrc.nist.gov/publications/PubsFIPS.html*

24 *Op cit,* National Institute of Standards and Technology, February 2010

25 National Institute of Standards and Technology, "Standards for Security Categorization of Federal Information and Information Systems," FIPS Publication 199, USA, February 2004, *http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf*

26 National Institute of Standards and Technology, "Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories," SP 800-60 vol. I, Rev. 1, USA, August 2008, *http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf*

27 National Institute of Standards and Technology, "Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories," SP 800-60 vol. II, Rev. 1, USA, August 2008, *http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf*

28 National Institute of Standards and Technology, "Standards for Security Categorization of Federal Information and Information Systems," FIPS Publication 199, USA, March 2006, *http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf*

29 National Institute of Standards and Technology, "Security and Privacy Controls for Federal Information Systems and Organizations," NIST SP 800-53 Revision 4, USA, April 2013, *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf*
30 National Institute of Standards and Technology, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations," NIST SP 800-53A Revision 4, USA, December 2014, *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf*
31 *Op cit,* National Institute of Standards and Technology, February 2010
32 National Institute of Standards and Technology, "Supplemental Guidance on Ongoing Authorization: Transitioning to Near Real-Time Risk Management," USA, June 2014, *http://csrc.nist.gov/publications/nistpubs/800-37-rev1/nist_oa_guidance.pdf*
33 *Op cit,* National Institute of Standards and Technology, September 2011
34 *Op cit,* National Institute of Standards and Technology, April 2013
35 *Op cit,* National Institute of Standards and Technology, December 2014
36 Department of Homeland Security, "DHS Security Authorization Guide, Version 11.1," USA, March 2015, *www.dhs.gov/publication/dhs-security-authorization-process-guide*