



Checklist to Assess Security in IT Contracts

Federal Agencies that outsource or contract IT services or solutions must determine if security is adequate in existing and new contracts.

Executive Summary

This whitepaper examines the security threats and information technology (IT) security requirements associated with contracted IT services, websites, outsourced business processing and on-demand applications. When Government agencies contract for these services, agency Chief Information Officers (CIO), Chief Information Security Officers (CISO) and System Owners must ensure that Federal government information and services are adequately protected and in compliance with a series of national security policies and standards. This paper provides a checklist for system owners and security professionals to assist in reviewing current contracts and aid in planning for new acquisitions. Industry standard alternatives to the Federal government security frameworks are also presented as a means to aid in determining potential usage. Solutions are provided to enable Federal agency personnel responsible for IT, contracts, and business operations to perform these assessments, remediate non-compliance, address security risks and put in place sustainable cyber security programs.

Security and Privacy Threats

Threat Trends that Affect Government and its Contractors

Organizations, both government and industry, continually adapt and implement new security controls and countermeasures to thwart threats and attackers and protect against disclosure of sensitive information. In response, “bad actors” innovate to exploit new weaknesses. Recent events at government agencies and its contractors indicate attacks have evolved in new, targeted ways which include:

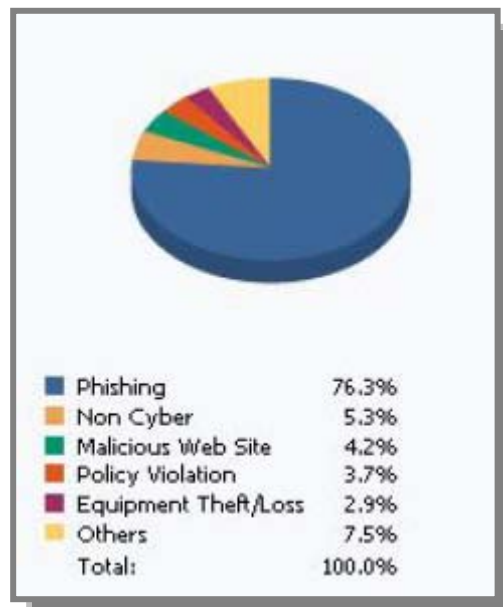
- Compromise of trusted internet websites and services with malicious software which either redirects the user to malicious website or installs malicious software on user computer that bypasses traditional security measures
- Targeting end users through email methods referred to as “spear phishing” succeeding in obtaining confidential and sensitive information
- Advanced networks of attackers and “bot nets” that enable attackers to rapidly adapt and target their techniques

Spear phishing is a highly targeted phishing attack that uses e-mail that includes information about your personnel or current business issues that make it appear genuine to employees. These attacks leverage social engineering to convince victims to open an attachment or follow a link to view additional information. These attacks frequently go undetected and can install malicious code on the victim’s computer. Documented attacks of this nature have resulted in the loss of government and industry sensitive information.

The [United States Computer Emergency Readiness Team](#) reports increasing threats to government and industry networks and systems in its August 2008 quarterly trend report.

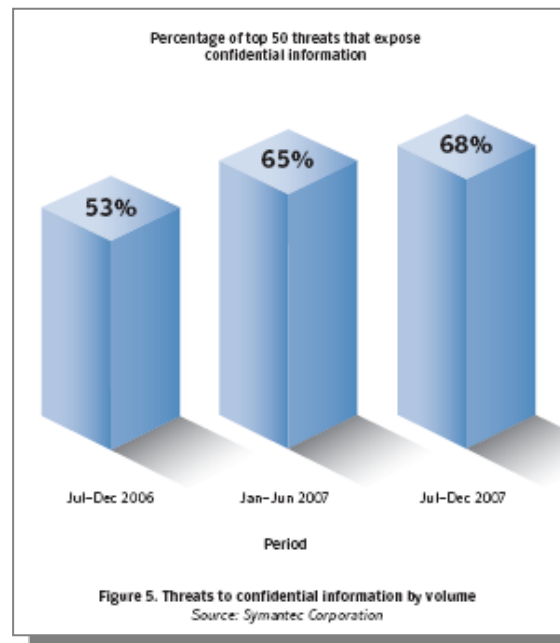
Symantec Corporation¹ identified the following trends in its recent Internet Security Threat Report:

- During this reporting period, the United States accounted for 31 percent of all malicious activity, an increase from 30 percent in the first half of 2007.
- Government was the top sector for identities exposed, accounting for 60 percent of the total, a significant increase from 12 percent in the first half of 2007.



¹ http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf

- Theft or loss of computer or other data-storage medium was the cause of the most data breaches that could lead to identity theft during this reporting period, accounting for 57 percent of the total. It accounted for 61 percent of the identities exposed in the second half of 2007, more than any other sector.
- The United States was the country most frequently targeted by denial-of-service attacks, accounting for 56 percent of the worldwide total. This is a decrease from 61 percent reported in the first half of 2007.
- In the second half of 2007, 58 percent of all vulnerabilities affected Web applications. This is less than the 61 percent in the first half of 2007.
- Symantec identified 11,253 site-specific cross-site scripting vulnerabilities in the last six months of 2007, compared to 6,961 in the first half (though with measurement beginning only in February).
- In the second half of 2007, 499,811 new malicious code threats were reported to Symantec, a 136 percent increase over the first half of 2007.
- Threats to confidential information made up 68 percent of the volume of the top 50 potential malicious code infections.
- Of all confidential information threats detected this period, 76 percent had a keystroke logging component and 86 percent



Technology Trends that Introduce New Vulnerabilities and Risks

Web-based Applications



Web-based applications custom built for a Federal government agency or commercial products provided as web-based application services continue to grow in use by Federal agencies. Hundreds of vulnerabilities are reported each week in the underlying commercial software products and open source technology that power these web applications. These vulnerabilities are rapidly exploited and often times go undetected by the operators of these applications.

Cloud Computing

Increasing use of Cloud Computing as a means for Government agencies to obtain applications and storage as a service without internal implementation and support is a growing trend due to its appeal for reduction of costs. However, Cloud Computing can introduce new risks to an agency. Typically, these approaches require Government agencies to provide or enter sensitive data into a contractor-owned and operated system. In these instances, the Government must rely on the overall cyber security program of the contractor to ensure the data is adequately protected. Cloud computing requires special attention in areas such as data integrity, privacy, contingency, and an evaluation of incident response, compliance and auditing. Existing, common methods for assessing risk do not address the challenges posed by the lack of boundaries of the system and the location and control of data. If not

Cloud computing is Internet ("cloud") based development and use of computer technology. It is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet. Organizations do not require knowledge of, expertise in, and are not in control of the technology infrastructure "in the cloud". The concept incorporates infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) as well as Web 2.0.

properly addressed, organizations can be exposed to significant risks and not meet compliance requirements.

Portable and Removable Mass Media



Loss of laptops and removable media has become a major problem for corporations and government agencies. There have been a number of instances where the loss of government sensitive information or personal identifying information was traced back to the loss of a single laptop or USB device. Laptops, USB devices and portable digital assistants (PDA) such as Blackberry are commonly used to connect to enterprise networks. These devices can store large amounts of data which can contain sensitive information. These devices designed to be portable which means they are connected to different computer systems. This provides a means for malware to propagate. Agencies and industry struggle to meet operational demands while implementing security measures to ensure safe use.

Web 2.0

Web 2.0 is gaining adoption by Federal agencies and the businesses that provide web-based services to government. These solutions offer agencies the ability to overcome the traditional silo and stovepipe approaches as well as enable collaboration, information sharing and citizen communication not previously possible. Like all technology, security risks exist and increase as they are used on the Internet. Web applications can be compromised through unauthorized software insertion which can launch scans of data, ports and devices. Worms can be embedded and rapidly transmitted. Organization must ensure security best practices are followed and that they are validated through testing and assessment. Some examples of best practices for Web 2.0 include:

- Define and ensure security policies are implemented and strictly enforced.
- Use monitoring tools to enforce security policy, standards and guidelines
- Make sure web browsers are locked down to Federal Desktop Core Configuration (FDCC) and that your Web 2.0 application operates on FDCC desktops
- Ensure an effective endpoint strategy for your organization's fixed and mobile assets
- Deploy intrusion prevention and detection with a security information management system which provides near real time security situational awareness

Web 2.0 is a catch-all term that encompasses a suite of tools and techniques which make web applications interactive. These tools and techniques include blogs, wikis, podcasting, RSS, virtual worlds, social networking, social bookmarking, mashups, and widgets.

Virtualization

Organizations are rushing to convert servers and desktops to use new virtualization technology. Virtualization technology offers many benefits not the least of which include:

- the ability to reduce physical space through consolidation of computing resources in the data center
- load balancing, redundancy and failover
- cheaper software development and test environments

- standardized desktop configuration and reduced maintenance / support costs
- application delivery via virtual machine sandbox

Virtualization offers many security benefits as well which include:

- Additional insulation from malware and other attacks
- Greater control of user access to applications and the application permissions
- Damage and exposure is limited to the effected virtual machine

However, in all cases of technology, there are always weaknesses which can be exploited. Organizations need to be mindful to ensure the operational and security benefits of virtualization are not undone through lack of security planning, engineering and testing. Standards and policies for security configuration and continuous monitoring of controls must not be overcome by the consolidation that often time results from these efforts.

Voice over IP (VOIP)

The conversion from traditional dedicated phone circuits to shared use of data networking via VoIP has begun. If your organization has not yet deployed it, it is probably being considered. Nonetheless, some of your business partners have deployed which may introduce risks if you share information with them. VOIP consists of a set of communication protocols that can be easily attacked. Recently, an example of this was demonstrated when someone demonstrated a successful remote eavesdropping attack against [Cisco's Unified IP VOIP solution](#).

Instant Messaging

The use of Instant Messaging (IM) continues to grow on mobile phones, PDAs and corporate networks. IM technology can significantly increase the security risks from attacks and social engineering that tricks users into disclosing sensitive information.

Security and Privacy Requirements

When Federal government agencies engage vendors and commercial service providers to provide a service or capability that involves transmission, storage or processing of Government information, agencies must ensure these providers comply with FISMA and NIST. With the recent guidance from OMB, vendors and commercial service providers should expect increased security requirements in contracts and task orders.

Federal Information Security Management Act (FISMA)

The E-Government Act (Public Law 107-347) of 2002, Title III Federal Information Security Management Act (FISMA) recognized the importance of information security to the economic and national security interests of the United States. FISMA requires federal agencies to develop, document, and implement an information security program for the information and information systems that support the operations and assets of the agency, including those provided or managed by a contractor.

FISMA requires the National Institutes of Standards and Technology (NIST) to develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets. The objective of FISMA and the NIST standards is to provide the means for agencies to accomplish their stated missions with security commensurate with risk.

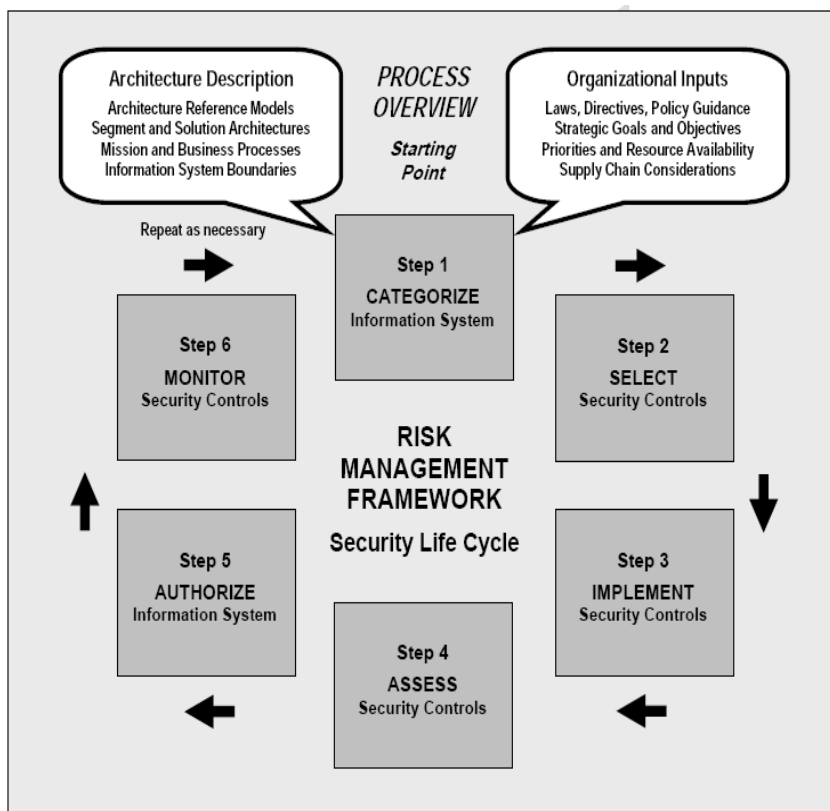
FISMA, together with NIST standards and guidance from the Office of Management and Budget (OMB), form a framework for developing and maturing an information security program. The framework spans program development, definition of controls and their assessment, the resulting certification and accreditation of system. The framework also supports the ongoing management and monitoring of processes and controls, continual assessment of threats and the ongoing management of risk and change.

The ultimate objective² 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 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.

FISMA requires each federal agency to develop and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency, **including those provided or managed by another agency, contractor, or other source.**

The agency's program must include:

- Periodic assessments of risk;
- 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;
- Plans for providing adequate information security for networks, facilities, information systems, or groups of information systems;
- Security awareness training;
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security;



² NIST Special Publication 800-39 Managing Risk from Information Systems - An Organizational Perspective, April 2008

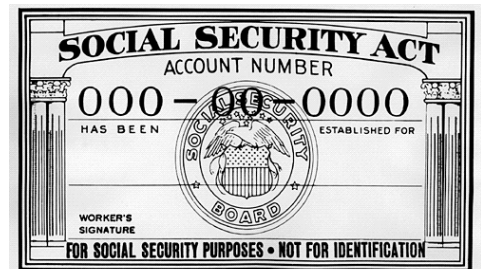
- A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies
- Procedures for detecting, reporting, and responding to security incidents; and
- Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the organization.

Privacy Act and Personally Identifiable Information (PII)

The Privacy Act of 1974 established safeguards for privacy of records of citizens through the creation of procedural and substantive rights to personal data. The Act requires government agencies to provide an individual with access to records that are maintained by the agency that contain the personal information on the requesting individual. The Act further requires agencies to follow principles, called "fair information practices," when gathering and handling personal data. The Privacy Act places restrictions on how agencies can share an individual's data with other people and agencies.

Section 208 of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C.) directed OMB to issue guidance to agencies for implementing the privacy provisions of the E-Government Act. The E-Government Act requires federal agencies to conduct Privacy Impact Assessments (PIA) before developing or procuring information technology or initiating any new collections of Personally Identifiable Information (PII)³. When information in identifiable form is gathered by any system or application, then the requirement to conduct a PIA applies regardless of the individuals involved whether they are members of the public, government personnel, or government contractors and consultants.

Executive Order 13402 charged the Identity Theft Task Force with developing a comprehensive strategic plan for steps the federal government can take to combat identity theft, and recommending actions which can be taken by the public and private sectors. On April 23, 2007 the Task Force submitted its report to the President, titled "Combating Identity Theft: A Strategic Plan." This report is available at www.idtheft.gov. In response to this report, the Office of Management and Budget issued memo [07-16 "Safeguarding Against and Responding to the Breach of Personally Identifiable Information"](#). This memorandum required agencies to develop and implement a breach notification policy within 120. Subsequent the issue of this memo, OMB now asks agency CIOs to certify in their FISMA annual reports that their agency has implemented the four requirements of this memo:



- 1) A breach notification policy (Attachment 3 of M-07-16)
- 2) An implementation plan to eliminate unnecessary use of Social Security Numbers (SSN) (Attachment 1 of M-07-16)
- 3) An implementation plan and progress update on review and reduction of holdings of personally identifiable information (PII) (Attachment 1 of M-07-16)
- 4) Policy outlining rules of behavior and identifying consequences and corrective actions available for failure to follow these rules (Attachment 4 of M-07-16)

³ Information in identifiable form is defined in Section 208(d) of the e-Government Act as "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." Information "permitting the physical or online contacting of a specific individual" (see section 208(b)(1)(A)(ii)(II)) is the same as "information in identifiable form."

Your agency policy and implementation must extend to business partners and contractors that process your agency's information that contains PII whether in electronic or non-digital format.

Office of Management and Budget (OMB) Memorandums

Security of Contracted or Outsourced Systems

OMB guidance requires federal agencies to ensure FISMA and the associated NIST risk management framework is extended to **both internal as well as external or contracted systems and services**. In [OMB Memo 06-20 "FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management"](#), OMB requires agencies to ensure contracted services, systems and operations comply with FISMA and NIST security in an "equivalent" manner. In this guidance, OMB also requires each agency Office of Inspector General (OIG) to annually review a subset of each agency's contracted systems. OMB provided examples of situations that meet its criteria:



- 1) Service providers -- this encompasses typical outsourcing of system or network operations, telecommunications services, or other managed services (including those provided by another agency).
- 2) Contractor support -- this encompasses on or offsite contractor technical or other support staff.
- 3) Government Owned, Contractor Operated (GOCO) -- For the purposes of FISMA, GOCO facilities are agency components and their security requirements are identical to those of the managing Federal agency in all respects. Security requirements must be included in the terms of the contract.
- 4) Laboratories and research facilities -- For the purposes of FISMA, laboratories and research facilities are agency components and their security requirements are identical to those of the managing Federal agency in all respects. Security requirements must be included in the terms of the contract or other similar agreement.
- 5) Management and Operating Contracts – For the purposes of FISMA, management and operating contracts include contracts for the operation, maintenance, or support of a Government-owned or-controlled research, development, special production, or testing establishment.

Therefore, agencies that obtain services via contract which involve agency information or connect to agency systems must ensure these services incorporate applicable security requirements and that they are assessed per FISMA established standards.

Protection of Sensitive and Personally Identifiable Information

In response to a series of security breaches involving sensitive information, OMB issued memo [M-06-16 "Protection of Sensitive Agency Information"](#) which provided additional guidance to agencies regarding protection of Personally Identifiable Information (PII). This memo required all federal agencies to:

- Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive. This spans PDAs, laptops, USB storage devices, and backup media;



- Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;
- Use a “time-out” function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity; and
- Log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required.

Standard Security Configuration Baselines

In August 2008, OMB issued [Memorandum M-08-01](#) which summarized earlier memos on the topic of implementation of commonly accepted security configurations for Windows operating systems. This memo directed all agencies to adopt the Federal Desktop Core Configuration (FDCC) security configurations for Windows XP and Vista. This was the first step in an effort to reduce persistent security vulnerabilities in the federal government through eliminating mis-configurations, deploying hardened configurations and driving commercial product vendors to ship software that operates in these hardened configurations. If your agency outsources IT, you need to be sure your providers have met this new standard or have identified deviations and are managing the process of remediation. It is anticipated that OMB will issue similar guidance for server operating systems and networking devices.

Trusted Internet Connections (TIC) Initiative

Thorough analysis performed by US-CERT, the Department of Homeland Security and the Intelligence Community, the Federal government has determined that most Federal government agency internet connections and hosted websites do not implement the necessary security technology and practices necessary to protect its networks. This realization along with security events of the past years compelled the Office of Management and Budget to create the Trusted Internet Connection (TIC) initiative with the goal of consolidating government internet connections to access points that meet new stringent standards.

In April 2008, OMB issued [M-08-16 “Guidance for Trusted Internet Connection Statement of Capability Form \(SOC\)”](#). Through this initiative, OMB seeks to consolidate and optimize individual external connections, including internet points of presence currently in use by the federal government. For approved internet access points, a series of security capabilities are required to thwart attacks, provide increased security situational awareness, and improve the federal government’s incident response capability. Agencies that manage their own internet connections today, must either apply and be approved to become a Trusted Internet Connection Access Provider (TICAP) or the agency must convert its service to a provider that is approved by OMB as a TICAP⁴. This impacts general internet access for an agency as well as hosted services. Agencies that are not approved to continue their present internet service must review available options, follow future guidelines from OMB and transition to new approved internet services.

CURRENT AND TARGET CONNECTIONS (AGENCY REPORTED)
◆ Existing Connections (Jan 2008) = 4300+
◆ Existing Connections (May 2008) = 2758
◆ Target Connections = <100

⁴ http://www.whitehouse.gov/omb/egov/documents/2008_TIC_SOC_EvaluationReport.pdf

Current Situation

Federal Government Information and Services at Risk

The Identity Theft Task Force recently reported⁵ the result of its analysis of recent security events across the Federal government. The task force found that there were a number of common weaknesses which increased risk that sensitive information and government operations could be compromised. These risks pertain to both government-owned and operated information technology as well as services and solutions contracted by the Federal government.

1. Security and privacy training is inadequate and poorly aligned with the different roles and responsibilities of various personnel.
2. Contracts and data sharing agreements between agencies and entities operating on behalf of the agency do not describe the procedures for appropriately processing and adequately safeguarding information.
3. Information inventories inaccurately describe the types and uses of government information, and the locations where it is stored, processed or transmitted, including personally identifiable information.
4. Information is not appropriately scheduled, archived, or destroyed.
5. Suspicious activities and incidents are not identified and reported in a timely manner.
6. Audit trails documenting how information is processed are not appropriately created or reviewed.
7. Inadequate physical security controls where information is collected, created, processed or maintained.
8. Information security controls are not adequate.
9. Inadequate protection of information accessed or processed remotely.
10. Agencies acquire information technology and information security products without incorporating appropriate security and privacy standards and guidelines.

Industry Security Frameworks Not Equivalent with FISMA

Currently, the OMB requires equivalent security in any contracted or outsourced operations, systems or services. NIST has stated a future objective to work with industry and global standards organizations in an effort to map these frameworks. Once completed, agencies and corporations can leverage the frameworks they have implemented, tested and have had audited to demonstrate compliance with Federal, OMB and NIST requirements. However, until that mapping is approved and issued by NIST, agencies must seek demonstration of compliance with Federal requirements. Organizations that have adopted Cobit, ITIL and/or ISO 17799 have many of the security requirements of the Federal government addressed. However, these organizations will need to demonstrate equivalence with NIST standards. Provided below is a brief overview of related industry and global IT management frameworks which address aspects of the requirements of FISMA, OMB and NIST.

⁵ <http://csrc.nist.gov/pcig/document/Common-Risks-Impeding-Adequate-Protection-Govt-Info.pdf>

Cobit⁶

The Control Objectives for Information and related Technology (COBIT) is a set of best practices for information technology (IT) management created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1992. COBIT specifies a set of generally accepted measures, indicators, processes and best practices for maximizing the benefits derived through the use of IT. It established best practices for appropriate IT governance and control to include security. Cobit has been adopted by many companies and is used by IT auditors to determine risk.

ITIL⁷

The Information Technology Infrastructure Library (ITIL) is a set of best practices for managing information technology (IT) infrastructure, development, and operations. Many organizations in the public and private sectors have begun to adopt ITIL best practices and its comprehensive checklists, tasks and procedures that can be tailored to the organization. The ITIL Security Management describes information security management for an organization. ITIL Security Management is based ISO/IEC 17799. ISACA has produced a [mapping between Cobit and ITIL version 3](#).

ISO 17799, 27001 and 27002⁸

ISO/IEC 27001 / 27002 and its predecessor ISO 17799 are best practices for information security management. Like NIST, information security is defined in the context of Confidentiality, Integrity Availability. Organizations can be certified for implementation of these ISO standards by independent, accredited organizations.

NIST included a mapping of ISO 17799 to its SP 800-53 control standard, however has not formally endorsed any equivalence or similar guidance that would permit agencies to accept ISO 17799 as equivalent with FISMA and NIST SP 800-53.

Security and Privacy Requirements Not Incorporated in Contracts

Security policy, standards and processes have been rapidly changing due to threats and security exposures. This has made it difficult for CIOs to ensure their agency has guidance in place and the necessary security professionals available to ensure contracts contain the necessary security and privacy requirements. Once issued, it is frequently extremely difficult for agencies to obtain the information necessary to evaluate security associated with the contract. Often times, the cost to add the security requirements after award is prohibitive.

Lack of Monitoring or Inability to Determine Performance and Compliance

For many agencies, their contracted and outsourced services and solutions may contain service level agreements (SLA) and measure contract performance in a wide variety of areas. However, frequently, agency personnel find they are unable to complete FISMA performance measurements or unable to respond to data calls from OMB because they are unable to obtain the information required regarding its

⁶ <http://www.isaca.org>

⁷ <http://www.itil-officialsite.com/>

⁸ <http://www.iso.org/>

contracts. This ranges from security control testing, security awareness training, and incident handling and reporting.

Relying Solely on a SAS 70 Audit as a Measure of Compliance

Government agencies that rely on the results of SAS 70 audits as a means to measure security and demonstrate compliance will find that audit does not measure many of the areas required by FISMA, NIST and OMB. SECURE|IT prepared a Whitepaper that provides an analysis of the critical aspects of the Federal government security requirements and standards along with that which is typically examined through a SAS 70 Type II audit

Security Checklist

The purpose of the checklist is a high level guide to assess the overall security and privacy status associated with a contracted IT service or outsourced business processing. The objective of checklist is to assist program managers, security officers, system owners and contracting officer representatives to identify areas of increased security risk and areas not in compliance with national and agency policy and standards. The key areas examined in this checklist include:

1. IT, Physical and Personnel Security Policy
2. Organization / Contract General Provisions
3. System, Data and Device Inventory
4. System Certification and Accreditation
5. Contingency Planning
6. Continuous Monitoring / Risk Management
7. Weakness Management
8. Incident Handling and Response
9. Security Configuration Management
10. Security Training

IT, Physical and Personnel Security Policy

For each, determine if the contract specifies requirements and appropriately references national and agency-specific policy for each factor.

Factor	Assessment	Weaknesses / Non-Compliance
System Development Life Cycle		
System Inventory		
Contingency Planning		
Continuous Monitoring / Risk Management		
Plan of Action and Milestones Management		
Incident Handling and Response		
Security Configuration Management		
Security Training		
Information Privacy		

Factor	Assessment	Weaknesses / Non-Compliance
Certification and Accreditation		
Media Protection		
Voice Communication		
Data / Wireless Communication		
Portable Devices		
Access Control		
Network Security		
Internet Communication Security		
Encryption		
Personnel Security		
IT Physical Security		
Agency Specific Requirements		

Organizational / General Contract Provisions

These areas typically need to be addressed in all contracts that involve access, handling, processing or transportation of Federal government sensitive information.

Factor	Assessment	Weaknesses / Non-Compliance
Does the contract identify the System Owner, Certification Agent and Authorizing Official? Are the roles and responsibilities of these roles defined in the contract or in referenced security policy?		
Does the contract identify an Information Systems Security Officer? Are the roles and responsibilities defined in the contract or in referenced security policy? Is separation of duties addressed in these responsibilities?		
Is the company required to notify your agency when it uses subcontractors?		
Does the contract require the company to have a policy and process for ensuring security and privacy requirements of your agency contract is properly specified to its contractors?		
Does your contract prevent the company from subcontracting with businesses located outside of the United States?		
Does the contract include appropriate personnel security policy from OPM and that which is specific to your agency?		

Factor	Assessment	Weaknesses / Non-Compliance
Does your contract require execution of Non-Disclosure Agreements, Acceptable Use and appropriate Code of Ethics?		
Agency Specific Requirements		

System, Data and Device Inventory and Asset Management

For contracts that include the provision of or use of a contractor system or application, the following checklist applies:

Factor	Assessment	Weaknesses / Non-Compliance
Has the agency determined its security impact level per FIPS PUB 199 based on the data involved and mission or support function? Were these values specified in the contract? If not currently available, does the contract have provision for its determination?		
Does the system/application meet E-authentication criteria? If so, has it been validated at the required assurance level in accordance with the NIST Special Publication 800-63, "Electronic Authentication Guidelines"?		
Does the contract involve processing of Federal government financial information subject to FISCAM? If so, is FISCAM incorporated into the contract?		
Does the contract provide guidance regarding system interconnection or interface of the contractor's system with others that are outside of the contractor's control?		
Is there an interconnection security agreement or similar agreement that defines and governs security policy and controls associated with this connection included as part of this contract?		
Agency Specific Requirements		

All contracts that involve handling or access to Federal government information should address the following areas:

Factor	Assessment	Weaknesses / Non-Compliance
Does the contract involve processing of sensitive (SBU), For Official Use Only (FOUO) or other government sensitive information? If so, are the data types identified and the appropriate security policy specified?		

Factor	Assessment	Weaknesses / Non-Compliance
Does the contract require processing of information subject to the Privacy Act or is deemed Personally Identifiable Information (PII)? If so, are the data types identified and the appropriate security policy specified?		
Is the organization required to uniquely identify portable devices and provide a means to track them with serial number, user and location?		
Does the contract specify that portable devices must be encrypted with FIPS 140-2 encryption if connected to the systems that contain your agency information?		
Agency Specific Requirements		

System Certification and Accreditation

The System C&A checklist is applicable to contracts where the company is providing a computer system or application that contains your agency’s information.

Factor	Assessment	Weaknesses / Non-Compliance
Is a System Security Plan (SSP) required? If so, must it conform to NIST SP 800-18?		
Does the contract specify who in the organization is responsible for the system? Does that individual have the necessary authority to manage change and security risk on this system?		
Does the contract specify the baseline security requirements of NIST SP 800-53 controls? Does the contract include your agency parameters for the controls?		
Does your agency have security policy and controls that are supplemental to NIST SP 800-53? These are referred to as agency-specific. If so, are they described in the contract?		
Has your agency defined assessment procedures for its agency-specific security policies and controls? If so are they specified in the contract? If you agency has not defined assessment procedures, is it up to the contractor to determine appropriate assessment procedures?		
Does the contract require the organization to perform system security certification and accreditation in accordance with NIST SP 800-37? If not, you provide guidance on acceptable forms which are equivalent to NIST SP 800-37?		

Factor	Assessment	Weaknesses / Non-Compliance
Does the certification letter summarize risks and provide recommendations to the Authorizing Official?		
Is the Accreditation Letter signed by the Authorizing Official and does it reference the Plan of Action and Milestones?		
Does the Plan of Action and Milestones accurately report the outstanding, non-accepted risks as well as the risks accepted by the AO?		
Does the POA&M identify POC, resources and corrective action / milestones?		
Agency Specific Requirements		

Contingency Planning

The Contingency Planning checklist is applicable to contracts where the company is providing a computer system or application that contains your agency’s information or the company is performing an outsourced business processing service.

Factor	Assessment	Weaknesses / Non-Compliance
Is the organization required to have Contingency Plan for the system and/or business process associated with the contract? Is Contingency Plan consistent with NIST SP 800-34?		
Are recovery time objectives established for the system and essential business functions that support the contracted services or business processing?		
Does the contract require testing of contingency and recovery capabilities at least annually?		
Agency Specific Requirements		

Continuous Monitoring / Risk Management

The Continuous Monitoring / Risk Management checklist is applicable to contracts where the company is providing a computer system or application that contains your agency’s information or the company is performing an outsourced business processing service.

Factor	Assessment	Weaknesses / Non-Compliance
--------	------------	-----------------------------

Factor	Assessment	Weaknesses / Non-Compliance
Does the contract specify compliance with continuous monitoring of security controls NIST SP 800-53 per NIST SP 800-37?		
Does the contract require the organization to provide evidence of control testing in accordance with the system FIPS PUB 199 impact level (not to exceed 12 months)?		
Does the contract require assessments to be performed in accordance with NIST SP 800-53A?		
Does the contract require the organization to update a report of all known weaknesses and corresponding Plan of Action and Milestones (POA&M) at least quarterly?		
Does your contract permit your agency to perform onsite inspections?		
Agency Specific Requirements		

Weakness Management

The Weakness Management checklist is applicable to contracts where the company is providing a computer system or application that contains your agency’s information or the company is performing an outsourced business processing service.

Factor	Assessment	Weaknesses / Non-Compliance
Does the contract require the organization to manage known weaknesses in a process consistent with the NIST and OMB defined Plan of Action and Milestones (POA&M)?		
Does the contract require the organization to perform security vulnerability assessments, penetration testing and security configuration compliance scans to identify weaknesses?		
Does the individual responsible for the contract have the authority to set priorities and approve resources associated with remediating weaknesses?		
Agency Specific Requirements		

Incident Handling and Response

The Incident Management checklist is applicable to contracts where the company is providing a computer system or application that contains your agency’s information or the company is performing an outsourced business processing service.

Factor	Assessment	Weaknesses / Non-Compliance
Does the contract require the organization to have a formal incident handling and response capability to serve as the first tier of incident response and the investigative and reporting body for its organization?		
Does the contract require the organization to track incidents?		
Is the organization required to report significant computer security incidents to your organization and the US-CERT in accordance with US-CERT reporting procedures?		
Is the organization required to report minor incidents in a monthly incident report to your organization and US-CERT?		
Does the contract require the organization to handle and report incidents involving PII?		
Does the contract specify how the organization is to respond if there is a breach of PII?		
Agency Specific Requirements		

Security Configuration Management

The Security Configuration Management checklist is applicable to contracts that involve:

- A computer system or application that contains your agency’s information
- A managed service for user workstations, network or application servers

Factor	Assessment	Weaknesses / Non-Compliance
Does the contract specify policy and standards for security configuration standards that include FDCC and other NIST standards http://checklists.nist.gov?		
Does the contract require the organization to use a NIST Security Content Automation Protocol (SCAP) approved tool to determine Federal Desktop Core Configuration (FDCC) deviations?		
Does the contract specify how the contractor must demonstrate compliance with other than FDCC when SCAP baselines are not available?		

Factor	Assessment	Weaknesses / Non-Compliance
Is the organization required to check for deviations monthly producing a compliance report?		
Agency Specific Requirements		

Security Training

Applicable to all contracts the enable access to Federal government information.

Factor	Assessment	Weaknesses / Non-Compliance
Is the organization required to track all employees with access to your agency information?		
Does the contract specify a minimum standard for security awareness that addresses all areas of security awareness contained in the OMB Information Systems Security Line of Business awareness course?		
Does the contract require security and privacy awareness training that informs users of responsibilities associated with access to PII and ramifications if it is not properly handled?		
Does the contract require reporting of completion of awareness training at least annually? Does the contract define acceptable forms of evidence of completion of awareness training?		
Does the contract require the organization to identify personnel in security professional roles or those personnel with significant security management responsibilities?		
Does the contract require the organization to report training completed annually for security professionals and personnel in significant security management roles involved in the contract?		
Agency Specific Requirements		

Conclusions

Federal government program managers must review their current IT and outsourcing contracts to determine if adequate security is implemented, monitored and managed. If necessary, program managers should obtain the necessary security expertise to perform this assessment and provide information and advice to modify current contracts and acquisition plans to ensure security has been effectively incorporated. Agencies that rely on SAS 70 audit reports from their vendors as a measure of security performance and compliance must recognize a SAS 70 audit can provide valuable insight into a company's services, but alone does not meet the requirements of a Federal government security and privacy requirements.

Next Steps

Determine your Current Situation, Gaps and Security Risk

SecureIT can review the current security in place associated with contracted services and present the assessment in a gap analysis report which is presented in terms of risk to your agency. Additionally, SecureIT provides independent assessment, measurement and monitoring services to provide Government agencies independent assessment of security performance, assess impacts, manage change and risks.

Update Contracts and Acquisitions to Address Security Requirements

SecureIT can assist your program offices to efficiently incorporate the appropriate security requirements into existing contracts and future acquisitions. Working with your contracting officers, COTRs and Program Managers, your team can incorporate the proper security requirements and identify security performance measures appropriate for your business need. This will enable your organization to monitor security performance and compliance of the provider.

Obtain Independent Assessment and Monitoring

Develop and implement an independent assessment and monitoring solution that are appropriate for your contracts. Take advantage of your agency's existing resources and that of your contracted services and supplement with independent assessment and monitoring for security and performance. SecureIT can assist in developing a solution that is appropriate based on risk and compliance. SecureIT can also provide the independent security assessment and monitoring deemed appropriate and provide the information required to demonstrate effective risk management and compliance with security requirements.

Update your Agency-wide Cyber Security Program

FISMA requires each federal agency to develop, document, and implement an agency-wide information security program to provide security for the information and information systems that support the operations and assets of the agency. The security program must provide comprehensive, uniform IT security policies and standards for the protection of agency assets. The agency must ensure that national policies and standards are appropriately incorporated and adapt them to the agency's



specific circumstances, defining additional standards when necessary. The program must span the following areas:

- Capital Planning and Investment Control (CPIC) for the security program security and to ensure security is integrated into agency investments
- Security oversight, compliance, and reporting
- System inventory management
- Information security / classification and policy for sharing
- Critical Infrastructure Protection (CIP)
- Computer Security Incident Response Capability (CSIRC)
- Plans of Actions and Milestones (POA&M)
- Security Configuration Management (CM)
- Trusted Internet Connections (TIC)
- Security Enterprise Architecture (EA)
- Integrating security into acquisitions and agreements with business partners
- All control areas specified in NIST Special Publication 800-53

The program must be documented and define the agency's information technology security management structure and responsible individuals assigning responsibilities and specific minimum information security controls for all agency systems. The Chief Information Officer (CIO), supported by the Chief Information Security Officer (CISO) must keep pace with advances in technology and policy evolution continually updating the agency cyber security program, training, and technology to mitigate threats and vulnerabilities and adopt national policies and standards.

About SecureIT

SecureIT helps private and public sector clients manage technology risks and create value through effective practices in IT security. SecureIT provides services and solutions in the areas of Cybersecurity, Information Assurance, Governance & Compliance, IT Audit, and Security Training. SecureIT designs enterprise security programs, implements best practices and assesses technology implementation for security risk. Professionals with industry knowledge and technical expertise devise strategies and solutions to reduce risk, increase efficiency and overcome the challenges of compliance. Located in Reston, VA, SecureIT serves clients in the Federal government including; DISA, HHS, DOJ, Treasury, Commerce, USAID, Education, DHS, and IMF as well as the private sector with clients such as Freddie Mac, CSC, FINRA, and E*TRADE.

For more information, call 703.464.7010, email info@secureit.com or visit www.secureit.com

Notice

Copyright © 2008, SecureIT Consulting Group Inc. All rights reserved.

The SECURE|IT logo, and all page headers, footers and icons are trademarks or registered trademarks of SecureIT Consulting Group.

Other company names or products mentioned are or may be trademarks of their respective owners. Information in this document is subject to change without notice.

For the latest information, visit www.secureit.com