NIST Special Publication 800-53

Practical Application of the Minimum Baseline Security Controls

Graydon S. McKee IV – CISSP, GSEC

A Framework for All Seasons

- With the finalization of Federal Information Processing Standard (FIPS) Publication 200: Minimum Security Requirements for Federal Information and Information Systems, the application of NIST SP 800-53 became mandatory for Federal Information Systems.

- While aimed at the Federal Government, the framework created by NIST in response to the Computer Security Act of 1987 and the Federal Information Security Management Act of 2002, is applicable in many different industries and environments both inside and outside the U.S. Federal Government.

A Framework for All Seasons

- Many of the NIST SP 800-53 Security Controls correspond with the required controls of:
  - ISO 17799
  - HIPAA
  - Sarbanes-Oxley
  - Gramm-Leach-Bliley
- The flexibility of the NIST Framework and the security control crossover allows environments subject to many different requirements to address them all within a single methodology.

A Framework for All Seasons

- This presentation will showcase the practical application of select NIST SP 800-53 controls, the issues faced with the actual implementation, and how these controls correspond to the requirements of:
  - ISO 17799,
  - HIPAA,
  - Sarbanes-Oxley, and
  - Gramm-Leach-Bliley.

The Benefits of NIST SP 800-53

- NIST SP 800-53 facilitates a consistent, comparable and repeatable approach for specifying security controls;
- Provides recommendations on a minimum set of security controls for Information Systems;
- Promotes a dynamic, extensible catalog of security controls to meet the demands of ever-changing technologies and requirements;
- Creates a foundation for the development of assessment methodologies and procedures for measuring security control effectiveness

Source: NIST SP 800-53A

What is a Security Control exactly?

- As defined by NIST SP 800-53:

"…the management, operational, and technical safeguards or countermeasures prescribed for an information system to adequately protect the confidentiality, integrity, and availability of the system and the information it contains."

- NIST SP 800-53 provides a baseline of controls based upon the system's FIPS199 / NIST SP 800-60 System Security Categorization

The Security Control Selection Process

- Selection of security controls needs to be part of an organization-wide or system-specific security program
- Remember the goal of security control selection is to reduce the information systems risk level to acceptable levels and is not about being compliant with any particular regulation.

If we are doing a good job securing our systems, we will, in turn, be compliant with the applicable regulations.

The Security Control Selection Process

- The Activities related to managing organizational risk and the selection of Security Controls are:

  - **Categorization of the Information System**
    - **(FIPS 199/NIST SP 800-60)**
  - **Selection of the initial set of controls**
    - **(NIST SP 800-53)**
  - **Adjustment of the controls based upon a risk assessment and local conditions (requirements, threats, cost, etc)**
    - **(NIST SP 800-53)**
  - **Documentation of the agreed upon set of controls**
    - **(NIST SP 800-18/SP 800-37)**

The Security Control Selection Process

- Implementation of the controls
  - (NIST SP 800-53 / SP 800-53A)
- Assessment of the implemented controls
  - (NIST SP 800-30 / SP 800-53A)
- Re-Determination of Risk
  - (FIPS 199 / NIST SP 800-30 / SP 800-60)
- Authorization to Operate the Information System with selected controls
  - (NIST SP 800-37)
- Monitoring and continuous assessment of the selected controls.
  - (NIST SP 800-37)

Security Control Classes

- **Managerial**—Security controls that focus on the management of risk and the management of information system security (example: Risk Assessment)
- **Operational**—Security controls that primarily are implemented and executed by people (example: Personnel Security)
- **Technical**—Security controls that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. (example: Audit and Accountability)

Control Families

Managerial

- **Certification, Accreditation, and Security Assessments (CA)**
- **Planning (PL)**
- **Risk Assessment (RA)**
- **System and Services Acquisition (SA)**

Technical

- **Access Control (AC)**
- **Audit and Accountability (AU)**
- **Identification and Authentication (IA)**
- **System and Communications Protection (SC)**

Operational

- **Awareness and Training (AT)**
- **Configuration Management (CM)**
- **Contingency Planning (CP)**
- **Incident Response (IR)**
- **Maintenance (MA)**
- **Media Protection (MP)**
- **Physical and Environmental Protection (PE)**
- **Personnel Security (PS)**
- **System and Information Integrity (SI)**

Managerial Controls: Risk Assessment

- **RA-1 Risk Assessment Policy and Procedure**
  - A formal documented policy and corresponding procedures that address requirements, roles and responsibilities (among other things)
- **RA-2 Security Categorization**
  - Ensures that the information within the system is assessed in accordance with the worst case potential impact the organization will feel should it become compromised, altered, or unavailable. This ties the system into the overall mission of the organization.
- **RA-3 Risk Assessment**
  - Ensures that the organization assesses the risks to the system to a level of detail commiserate with the worst case potential impact (see RA-2)
- **RA-4 Risk Assessment Update**
  - Ensures the Risk Assessment is updated regularly or whenever a significant change has occurred to the system.
- **RA-5 Vulnerability Scanning**
  - Ensures the organization incorporates technical vulnerability scanning on a regular and consistent basis. The results are to be incorporated into a change/configuration management process.

Case Study
Risk Assessment : Implementation

Department of Justice : Asset Forfeiture Management Staff (AFMS)
Consolidated Asset Tracking System (CATS)

- **Background**
  - One of the many tasks for AFMS involves the development, maintenance and oversight of the DOJ Asset Forfeiture Program's property management information system.
  - The system is designed to track, throughout the forfeiture life-cycle, assets seized by federal law enforcement agencies.
  - Currently there are approximately 1450 workstations deployed at more than 700 sites across the continental US, Alaska, Hawaii, Guam, and various islands in the Caribbean, serving over 1500 trained users.

Case Study
Risk Assessment : Implementation
Department of Justice : Asset Forfeiture Management Staff (AFMS)
Consolidated Asset Tracking System (CATS)

- **Background (Continued)**
  - **CATS supports the day-to-day operations for seized and forfeited assets for the following agencies:**
    - Asset Forfeiture Management Staff, DOJ
    - Criminal Division, DOJ
    - Drug Enforcement Administration, DOJ
    - Federal Bureau of Investigation, DOJ
    - US Attorneys Office, DOJ
    - US Marshals Service, DOJ
    - Food and Drug Administration
    - US Postal Inspection Service
  - **CATS is accessible only from within the DOJ WAN.**

Case Study
Risk Assessment : Implementation

Department of Justice : Asset Forfeiture Management Staff (AFMS)
Consolidated Asset Tracking System (CATS)

- **The Task:**
  - Establish a comprehensive Risk Management program that integrates security into the system development life-cycle and allows for a proactive approach to security.
- **The Issues:**
  - Limited funding
  - Development staff not accustomed to considering information security concerns
    - Security was an afterthought and an added expense.
  - Operations staff was resistant to any sort of “interference” into their work.
  - Program Management felt that information security was an “unfunded mandate” and a mere paperwork exercise.

Case Study
Risk Assessment : Implementation

Department of Justice : Asset Forfeiture Management Staff (AFMS)
Consolidated Asset Tracking System (CATS)

- **Outside Factors:**
  - Federal Information Security Management Act of 2002 (FISMA)
  - Increased Internal and External Audits focused on Security
  - Funding began to be tied to audit findings.
- **The Solution:**
  - Increased Federal Focus on Information Security called for measurement of a program's security maturity through the Certification and Accreditation process.
  - Risk began to be tied to the mission and the impact to that mission
  - Education of the Development and Operations staff focused on using security to become proactive as opposed to reactive
  - Risk Management began to be seen as a mission enabler rather than a obstacle to be avoided.
  - The key was enacting not only the letter of FISMA but the spirit of FISMA.

Case Study
Risk Assessment : Implementation

Department of Justice : Asset Forfeiture Management Staff (AFMS)
Consolidated Asset Tracking System (CATS)

- **The Result:**
  - Program wide shift towards a comprehensive Risk Management methodology.
  - Increased education for all elements on secure development and operations practices.
  - Implementation of a formalized change and configuration management program that incorporates risk into the decision making process.
  - Implementation of a multi-tiered architecture complete with intrusion detection and vulnerability scanning capability.
  - Program Management now has reliable data from which to build the “business case” for security control enhancements.

Managerial Controls: Risk Assessment

- **ISO 17799 Cross Walk[1]:**
  - **4.2 Organizational Security**
    - Third-Party Access: To maintain the security of information assets accessed by third parties
  - **4.3 Asset Classification and Control**
    - Outsourcing: To maintain the security of information when information processing is outsourced to another organization.
  - **5.2 Asset Classification and Control**
    - Information Classification: Information should be classified to indicate the need, priorities, and degree of protection
  - **5.1 Asset Classification and Control**
    - Accountability for assets: All major information assets should be accounted for and have a nominated owner

1 – Based on the Bindview® Regulatory Cross Reference Guide

Managerial Controls: Risk Assessment

- **HIPAA Cross Walk[1]:**
  - **Security Standard:**
    - **a) 1. Risk Analysis (R)**
    - **b) 1. Written Contract or Other Arrangement (R)**
  - **Physical Standard:**
    - **d) 2. Device and Media Controls – Accountability (A)**
- **Sarbanes-Oxley Cross Walk[1]:**
  - **Internal Environment:**
    - **Management's Philosophy and Operating Style**
    - **Commitment to Competence**
    - **Human Resource Policies and Practices**
  - **Risk Assessment:**
    - **Likelihood and Impact**
  - **Control Activities:**
    - **General Controls**
  - **Information and Communication Monitoring Event Identification:**
    - **Event Categories**

1 – Based on the Bindview® Regulatory Cross Reference Guide

Managerial Controls: Risk Assessment

- **Gramm-Leach-Bliley Cross Walk[1]:**
  - **Security Process:**
    - **Roles and Responsibilities**
  - **Service Provider Oversight:**
    - **SAS 70 Reports**
  - **Security Testing:**
    - **Outsourced Systems**
  - **Information Security Risk Assessment:**
    - **Information Gathering**
    - **Analyze Information**
    - **Prioritize Responses**

1 – Based on the Bindview® Regulatory Cross Reference Guide

Operational Controls: Contingency Planning

- CP-1 Contingency Planning Policy and Procedures
- CP-2 Contingency Plan
- CP-3 Contingency Training
- CP-4 Contingency Plan Testing
- CP-5 Contingency Plan Update
- CP-6 Alternate Storage Sites
- CP-7 Alternate Processing Sites
- CP-8 Telecommunication Services
- CP-9 Information System Backup
- CP-10 Information System Recovery and Reconstitution

Case Study
Contingency Planning : Implementation

U.S. Department of Transportation (DOT), Research and Special Programs Administration , Office of Emergency Transportation

- Background
  - The Office Of Intelligence, Security, And Emergency Response (OET), in the Office of the Secretary (OST) of the Department of Transportation (DOT), performs coordinated crisis management functions for multimodal transportation emergencies, including:
    - **natural disasters;**
    - **technological incidents / accidents;**
    - **labor strikes;**
    - **security situations, such as domestic criminal acts or international terrorist acts;**
    - **national defense mobilization.**

* NOTE – The Research and Special Programs Administration is now the Office of Intelligence, Security, and Emergency Response.

Case Study
Contingency Planning: Implementation

U.S. Department of Transportation (DOT), Research and Special Programs Administration*, Office of Emergency Transportation

- The Task
  - The DOT needed assistance performing and analyzing a full scale Continuity of Operations Plan Exercise
  - The DOT needed assistance establishing a department wide IT Contingency Plan that incorporated a common support infrastructure as well as support each subcomponents needs regardless of their unique environments
- The Issues
  - The level of Contingency Planning maturity varied widely throughout the DOT
  - Each subcomponent had a unique infrastructure
  - The DOT also needed to incorporate outside agencies in its plans.

* NOTE – The Research and Special Programs Administration is now the Office of Intelligence, Security, and Emergency Response.

Case Study
Contingency Planning : Implementation

U.S. Department of Transportation (DOT), Research and Special Programs Administration , Office of Emergency Transportation

- The Solution
  - Support for the DOT Continuity of Operations (COOP) Exercise function included:
    - **The drafting of the Exercise Design;**
    - **The coordination of Exercise Design with DOT agencies;**
    - **The development of an Exercise Plan;**
    - **The coordination of Exercise Master Scenario of Events Lists (MSELS) with DOT agencies;**
    - **The development of the final Exercise Plan, Exercise Scenario, and Exercise MSELS;**
    - **The implementation of the Preparation Exercise (PREPEX); and**
    - **Coordination of the Hot Wash and PREPEX feedback into an After Action Report (AAR).**

Case Study
Contingency Planning : Implementation

U.S. Department of Transportation (DOT), Research and Special Programs Administration , Office of Emergency Transportation

- The Solution (Continued)
  - Coordinated DOT IT assets and personnel responsible for critical IT support to DOT Level III COOP Sites and the DOT DR Alternate Facility in an effort to identify and build IT infrastructure support strategies in support to the DOT COOP Program.
    - This effort analyzed each DOT Agency IT COOP support infrastructure to determine commonalities for developing a standard DOT COOP support approach.
    - The analysis and resulting strategies were designed to support the DOT IT Infrastructure with regards to Networks, Servers, Desktop, and Email critical support environments.
- The Result
  - The DOT was able to align it's policy and procedures across it's various subcomponents.
  - The DOT was able to ensure that critical staff were properly trained.

Case Study
Contingency Planning : Implementation

U.S. Department of Transportation (DOT), Research and Special Programs Administration , Office of Emergency Transportation

- The Result
  - Mechanisms were put in place to ensure that proper testing and plan updates were being performed.
  - Testing included the alternate storage and processing sites as well as telecommunication services and backup methodology.
  - Critical systems were tested to ensure proper recovery and reconstitution as required by the plan.

Operational Controls: Contingency Planning

- **ISO 17799 Cross Walk[1]:**
  - **8.4 Communications and Operations Management**
    - **Housekeeping:**
      - **Routine procedures for implementing the back-up strategy**
  - **11.1 Business Continuity Management**
    - **Aspects of Business Continuity Management:**
      - **To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters**
- **HIPAA Cross Walk[1]:**
  - **Security Standard:**
    - **a) 7. Disaster Recovery Plan (R)**
    - **a) 7. Testing and Revision Procedures (A)**
    - **a) 7. Applications and Data Criticality Analysis (A)**
    - **a) 7. Data Backup Plan (R)**
    - **a) 7. Emergency Mode Operation Plan (R)**

1 – Based on the Bindview® Regulatory Cross Reference Guide

Operational Controls: Contingency Planning

- **HIPAA Cross Walk[1] (Continued):**
  - **Physical Standard:**
    - **a) 2. Contingency Operations (R)**
    - **a) 2. Data Backup and Storage (A)**
- **Sarbanes-Oxley Cross Walk[1]:**
  - **Event Identification:**
    - **Event interdependencies**
  - **Risk Response:**
    - **Identify Risk Responses**
    - **Select Responses**
  - **Control Activities:**
    - **General Controls**

1 – Based on the Bindview® Regulatory Cross Reference Guide

Operational Controls: Contingency Planning

- **Sarbanes-Oxley Cross Walk[1]:**
  - **Information and Communication Monitoring Event Identification:**
    - **Event interdependencies**
  - **Monitoring**
- **Gramm-Leach-Bliley Cross Walk[1]:**
  - **Business Continuity Considerations**

1 – Based on the Bindview® Regulatory Cross Reference Guide

Technical Controls:

- **IA-1 Identification and Authentication Policy and Procedures**
- **IA-2 User Identification and Authentication**
- **IA-3 Device Identification and Authentication**
- **IA-4 Identifier Management**
- **IA-5 Authenticator Management**
- **IA-6 Authenticator Feedback**
- **IA-7 Cryptographic Module Authentication**

Case Study
Identification and Authentication : Implementation
Credit Suisse Group

- Background
  - Credit Suisse is a leading global bank headquartered in Zurich, Switzerland.
  - It focuses on serving its clients in three business lines:
    - Investment Banking,
    - Private Banking, and
    - Asset Management
  - The Credit Suisse Group required a multi-tiered approach to implementing an Identification and Authentication solution that would meet their current and future needs
  - This example was chosen to illustrate how the NIST Framework can be applied outside the U.S. Federal Government and to private institutions.

Case Study
Identification and Authentication : Implementation
Credit Suisse Group

- The Task:
  - Evolving out of a need to implement a global enterprise directory system and access control for host systems, Credit Suisse Group (CSG) determined that they needed a global Public Key Infrastructure (PKI).
  - CSG needed to be able to encrypt their communications (including secure e-mail) and conduct transactions with customers using electronic signatures.
  - CSG was also concerned with the need to meet the growing number of regulations in the countries which they conduct business worldwide.

Case Study
Identification and Authentication : Implementation
Credit Suisse Group

- The Issues:
  - CSG is active in over 50 countries world wide and employs approximately 63,000 individuals from over 100 different nationalities.
  - CSG's clients range from governments, institutions and corporations to private individuals.
  - CSG's product and service offerings are subject to multiple laws and regulations across the globe therefore any solution implemented must be sufficient to meet or exceed any one regulatory requirement.

Case Study
Identification and Authentication : Implementation
Credit Suisse Group

- The Solution:
  - **The design of the PKI implementation needed to ensure that it was adaptable to future trends.**
    - **Standards (including those from NIST), market trends, and emerging technology were examined.**
  - **The architecture needed to ensure that proper number and placement of Certificate Authorities (CA) and directories were determined.**
    - **Registration and CA functions were separated so that differing levels of control were achievable.**
    - **Interoperability of different products was ensured**
  - **Policy and Procedure needed to be enacted to reflect the global issues surrounding the implementation and operation of the solution.**

Case Study
Identification and Authentication : Implementation
Credit Suisse Group

- The Result:
  - **A formal documented policy (with corresponding procedures) was established that addressed the purpose, scope, roles, responsibilities, regulatory compliance, and coordination among organizational entities was established.**
  - **Multifactor authentication was implemented to not only meet regulatory requirements but in order to ensure sufficient protection for CSG's resources**
  - **A multi-tiered administration system was established that enforces separation of duties and ensures unique identification and authentication of CSG employees and clients.**

Case Study
Identification and Authentication : Implementation
Credit Suisse Group

- The Result:
  - **The solution:**
    - **Validates certificates by constructing a certification path to an accepted trust anchor;**
    - **Establishes user control of the corresponding private key; and**
    - **Maps the authenticated identity to the user account.**
    - **Ensures that the use of cryptography is compliant with all applicable regulations and guidelines required by the countries in which CSG operates.**

Technical Controls: Identification and Authentication

- **ISO 17799 Cross Walk[1]:**
  - **9.1 Access Control**
    - **Business Requirement for Access Control: Access control policies and rules**
  - **9.2 Access Control**
    - **User Access Management: Formal procedures to control the allocation of access rights to information systems and services**
  - **9.3 Access Control**
    - **User Responsibilities: User awareness, particularly with the use of passwords and the security of equipment**
  - **9.4 Access Control**
    - **Network Access Control: Ensure that appropriate authentication mechanisms for users and equipment are in place**

1 – Based on the Bindview® Regulatory Cross Reference Guide

Technical Controls: Identification and Authentication

- **ISO 17799 Cross Walk[1]:**
  - **9.5 Access Control**
    - **Operating System Access Control: Security at the operating system level to control access. Methods include: ensure quality passwords, user authentication, and the recording of successful and failed system accesses**
  - **9.6 Access Control**
    - **Application Access Control: Security to restrict access within application systems**
  - **9.7 Access Control**
    - **Monitoring System Access and Use: Systems should be monitored to detect deviations from access control policy and provide evidence in case of security incidents**
  - **9.8 Access Control**
    - **Mobile Computing and Teleworking: To ensure information security when using mobile computing and teleworking facilities**

1 – Based on the Bindview® Regulatory Cross Reference Guide

Technical Controls: Identification and Authentication

- **HIPAA Cross Walk[1]:**
  - **Security Standard:**
    - **a) 3. Termination Procedures (A)**
    - **a) 4. Access Authorization (A)**
    - **a) 4. Access Establishment and Modification (A)**
    - **a) 5. Password Management (A)**
    - **a) 5. Log-In Monitoring (A)**
    - **a) 1. Information System Activity Review (R)**
    - **b) 8. Audit Controls (R)**
  - **Technical Standard :**
    - **a) 2. Unique User Identification (R)**
    - **c) 2. Mechanism to Authenticate Electronic Protected Health Information (A)**
    - **d) Person or Entity Authentication (R)**
    - **a) 2. Automatic Logoff (A)**
    - **d) Person or Entity Authentication (R)**
  - **Physical Standard:**
    - **b) Workstation Use (R)**
    - **c) Workstation Security**

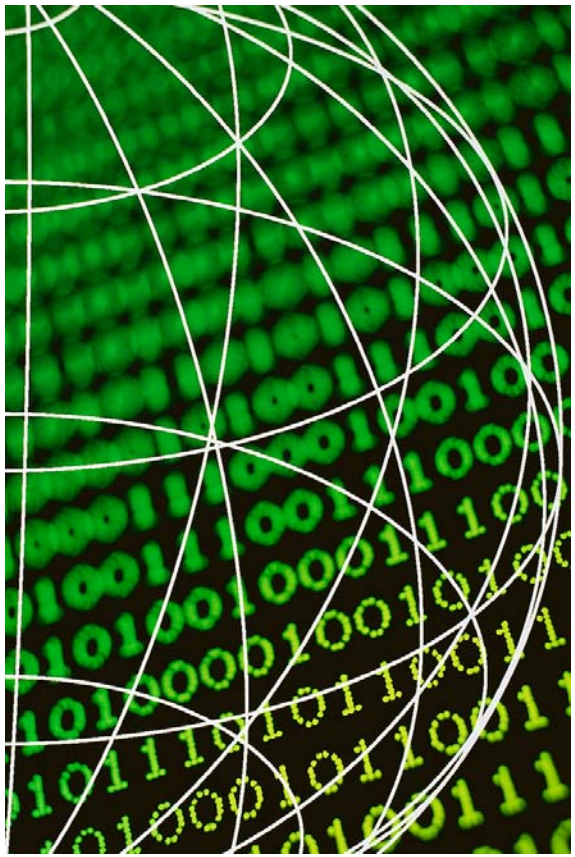
1 – Based on the Bindview® Regulatory Cross Reference Guide

Technical Controls: Identification and Authentication

- **Sarbanes-Oxley Cross Walk[1]:**
  - **Internal Environment:**
    - **Human Resource Policies and Practices**
  - **Control Activities:**
    - **General Controls**
  - **Monitoring**
- **Gramm-Leach-Bliley Cross Walk[1]:**
  - **Logical and Administrative Access Control:**
    - **Access Rights Administration**
    - **Authentication**
    - **Network Access**
    - **Operating System Access**
    - **Application Access**
    - **Remote Access**
  - **Personnel Security:**
    - **Training**
  - **Monitoring**
  - **Logging and Data Collection**

1 – Based on the Bindview® Regulatory Cross Reference Guide

Conclusion



- **As we have illustrated, the application of the NIST Framework and security controls can be applied across many different types of environments.**
- **The NIST Security Controls found in Special Publication 800-53 are just as applicable and beneficial outside the federal government.**

Questions?