Plan, Do, Check, Act

Julia H. Allen

November 2006

ABSTRACT: This article describes a tried and true approach to security improvement that can be effectively used during deployment and operations. It identifies prerequisites that must be in place to sustain a desired state of security. It provides a set of minimum requirements for security hygiene and several security implementation frameworks that can be used in concert with the other articles in this content area.

INTRODUCTION

This article

- describes a general approach to security sustainment and improvement that can be applied to any system, from an individual practice or control up to a full-blown information security architecture and management system
- describes prerequisites that must be in place to support an effective, sustainable security effort. It presents a table of minimum requirements for basic security hygiene to serve as the foundation for any subsequent effort
- introduces several implementation frameworks that can be used to get started

The Plan-Do-Check-Act approach described here can be used to deploy and operate the categories of practices described in the other articles in this content area.

One reasonable way to determine how to deploy and operate a secure, software-intensive system is to ask the following questions:

- How do I decide what to do and in what order?
- How do I do it?
- How do I know if what I did worked?
- How do I decide what to do next?

These four questions can be directly mapped to W. Edwards Deming's Plan, Do, Check, Act (PDCA) approach. Effective methods for improvement and management of change typically use some variation of this approach.

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

Phone: 412-268-5800
Toll-free: 1-888-201-4479

www.sei.cmu.edu

ISO/IEC 27001[1]

ISO/IEC 27001 [ISO 05b]:

- **Plan**: Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
- **Do**: Implement and operate the ISMS policy, controls, processes, and procedures.
- **Check**: Assess and, where applicable, measure process performance against ISMS policy, objectives, and practical experience and report the results to management for review.
- **Act**: Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

This approach can be used during deployment and operations to install a single security practice or control, a new secure software testing procedure, a new security technology, a patch or any other software change, or to securely configure a new server. The approach is general purpose and can be applied in a spiral, iterative fashion for successive levels of improvement and incrementally increasing scope.

PLAN: HOW DO I DECIDE WHAT TO DO AND IN WHAT ORDER?

W. Edwards Deming states "It is not enough to do your best; you must know what to do and then do your best." In large part, deployment and operations is about managing change, whether intentional or unintentional (including change caused by a security breach). To achieve effective and sustainable success and efficient use of resources, several prerequisites need to be in place before any changes are made to an operational system. This includes changes that could affect the software's or system's security posture or state.

The following prerequisites must be in place for an effective, sustainable security effort:

- management commitment to security

---

[1] ISO 27001 builds upon the security practices and controls identified in ISO 27002 (also known as ISO 17799). These include information systems acquisition, development, and maintenance.

- security policy
- security risk assessment results
- security strategy and plan
- security measures

Management Commitment to Security

Organizational leaders, including board directors, business executives, chief information officers, and managers of corporate audit, security, legal, line-of-business, privacy, and supply chain, all must play a role in making and reinforcing the business case for effective security. Trust, reputation, brand, stakeholder value, and customer retention are at stake if security management is performed poorly. Attentive organizations are much more competent in using security to mitigate risk if their leaders treat it as essential to the business and are aware and knowledgeable about security issues.

It is difficult, if not impossible, to sustain security improvement and move it into everyday organizational culture and practice without senior management commitment and ongoing reinforcement.

Security Policy

Clear, concise policies serve to enact the intent of the organization and help fulfill organizational objectives. A policy typically outlines specific requirements and rules that must be met, including appropriate behavior and consequences for unacceptable behavior.

A security policy specifies [Guel 01]

- its intended purpose
- its scope
- related roles and responsibilities

Categories of security policies include

- acceptable use (for users, system administrators, security personnel, and outside parties)
- remote access
- information protection
- perimeter protection
- host security
- application security
- configuration management

- change management (patch management)
- virus protection
- identity management (provisioning, use of passwords, other means of authentication)
- requirements for all devices with network access

Security Risk Assessment Results

You need to identify the organization's most critical assets and where those assets are most at risk in order to help select and prioritize security practices to implement during deployment and operations.

The sources identified in Table 1 describe risk assessment methods and practices that reliably produce useful results. It is important to note that risk assessment must be performed on a periodic basis (such as annually), as the risk and threat landscape is constantly changing. A high-priority risk today (and the security controls necessary to mitigate it) may be overtaken by an even higher priority risk tomorrow. (See also Risk-Centered Practices.)

Security Strategy and Plan

As with any project, a strategy and plan are necessary to successfully deploy and operate systems and software to meet security requirements and sustain a desired security posture. Security strategies and plans can be integrated into organizational strategic and operational plans (ideally) or they can be written as standalone documents.

Security plans describe and specify the following topics from Table 1:

Program/project management (see also the BSI Project Management content area)

- Standard operating procedures and processes
- Security budget
- Security tasks
- Security roles and responsibilities
- Security staff competencies
- Definition of what constitutes acceptable performance

Security Measures

A popular expression is "what gets measured, gets done." Some form of security measures is necessary to determine if deployed security practices are meeting

security requirements and how well they are doing so. Metrics, in part, serve to enact policies, plans, and strategies and to indicate progress (or not) toward mitigating security risks.

Having well-defined measures in place and regularly reported serves to direct the organization's attention based on the results. Visible measures positively influence human behavior by invoking the desire to succeed and compare favorably with one's peers. (See also the BSI Measurement content area.)

The extent to which each of the prerequisites described above is in place depends on the organization's view of security's role in meeting business objectives, including the need to mitigate security risks to critical business assets (information, processes, services, applications, and infrastructure).

Indicators for Determining the Presence of Prerequisites

Table 1 (included at the end of this article) provides indicators for each prerequisite to help determine its presence (or absence). Suggested sources for detailed practices are also listed. These describe, at varying levels, how to implement each prerequisite.

DO: HOW DO I DO IT?

If the prerequisites in Table 1 are absent or are not sufficient to determine which practices to deploy and in what order, then the best choice is to start tackling them in order, recognizing that addressing all of them to the degree required will take time. Many of the sources listed in Table 1 provide additional guidance on how to do this.

Minimum Essential Security Practices

Unless security is a critical requirement for deploying and operating a system, most organizations first encounter the need for greater security when they experience common types of infections such as viruses, worms, and spyware, many of which result from opening email attachments or visiting infected web sites. There is ample, current state-of-practice guidance describing how to mitigate against events of this type, including the use[2] of antivirus and antispyware soft-

2 Use includes defining and deploying procedures to ensure that antivirus software is regularly updated with signatures for newly detected events and that virus scans are conducted on a frequent basis

ware. Most organizations find that deploying such software is necessary but not sufficient to protect against the increasing proliferation and evolution of malicious software-based attacks and the exploitation of software vulnerabilities.

Other technology practices, such as deploying firewalls and intrusion detection systems at the perimeter of the network and protecting critical subnetworks and servers, are implemented to better secure the operational environment. Testing and installing vendor patches as they are released is essential. Vulnerability scanning and assessment is often used to detect and patch existing vulnerabilities before they can be exploited by new attack scripts.

These commonly deployed security practices, along with several others, are sometimes referred to as the minimum required for basic security hygiene. While tackling the prerequisites noted above, a useful parallel action is ensuring the presence of the minimum essential security practices listed below and then deploying those that are missing or insufficient. This list of practices derives in large part from the Payment Card Industry (PCI) Data Security Standard [PCI 08]. Table 2 (included at the end of this article) provides additional details and sources that expand these practices.

- Build and maintain a secure network.
  - Install and maintain a firewall configuration to protect data.
  - Do not use vendor-supplied defaults for system passwords and other security parameters.
  - Maintain an inventory of all devices, software, and services on the network.
- Protect sensitive data.
  - Protect stored data.
  - Encrypt transmission of sensitive data across open, public networks.
- Maintain a vulnerability management program.
  - Use and regularly update antivirus software or programs. Guard against all forms of malicious code.
  - Develop and maintain secure systems and applications.
- Implement strong access control measures.

---

across all system components, both physically resident and remotely connected (laptops and mobile devices, workstations, servers, routers, etc.).

  - Restrict access to data by business need-to-know.
  - Assign a unique ID to each person with computer access.
  - Restrict physical access to sensitive data.
- Regularly monitor and test networks.
  - Track and monitor all access to network resources and sensitive data.
  - Regularly test security systems and processes.
- Maintain an information security policy.
- Develop, deploy, and periodically refresh some level of security awareness and training.
- Determine and implement a means for measuring practice effectiveness.
- Ensure that third-party providers deploy adequate security practices (at least this minimum essential set).

CHECK: HOW DO I KNOW IF WHAT I DID WORKED?

This question is answered by monitoring, measuring, reviewing, assessing, and evaluating system and software security performance against some pre-established list or standard such as those suggested in the tables at the end of this article. Doing this on a regular and periodic basis and as part of normal day-to-day operations is vital.

The **Check phase**

- involves at least daily monitoring of system logs, firewall logs, intrusion detection logs, and other security alert mechanisms
- includes regularly collecting, analyzing, and reporting on designated security measures (refer to the BSI Measurement content area)
- may include conducting and reviewing the results of vulnerability assessments, penetration tests, security risk assessments, IT audits, and processes designed to demonstrate compliance with regulations and standards

The most critical aspect of the Check phase is to define in advance what constitutes success and acceptable performance and then ensure that practices are in place to collect and report against these criteria to those in a position to act on the results.

ACT: HOW DO I DECIDE WHAT TO DO NEXT?

The Act phase involves determining how best to sustain the current security state of systems and software while also accommodating changes and improvements. Actions should be informed by security policy, objectives, strategies, plans, assessment results from the Check phase, and analysis of security events.

Acting often starts as a reactive task, identifying critical, near-term corrective actions that need to be taken immediately. As the system and software security state becomes more stable, staff can concentrate on more proactive and preventive measures as the next order of business. Risk-centered practices that produce reliable risk assessment results are one of the most effective methods for determining what to do next.

IMPLEMENTATION FRAMEWORKS

This section introduces several implementation frameworks that can be used to deploy and operate systems and software in a secure manner, building on the practices described above.

Security Knowledge in Practice (SKiP[SM])

One organizing framework for categorizing and deploying security practices is Security Knowledge in Practice (SKiP) (Figure 1) [Rogers 02], [Allen 01]:

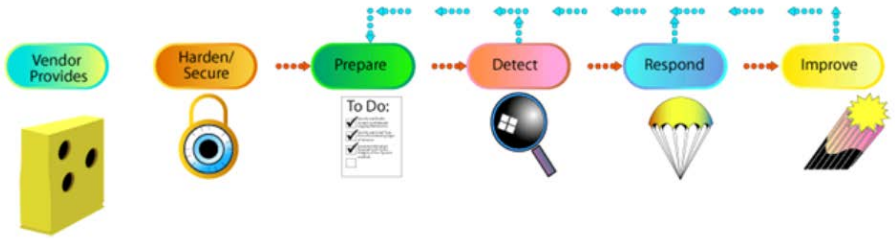

Figure 1. Security Knowledge in Practice

SKiP is a useful organizing structure for

- systems running mission-critical applications
- network infrastructure, including routers, hubs, and switches
- subsystems or subnetworks such as those providing email services, web content production and delivery services, and perimeter protection services
- a network architecture and topology
- systems containing sensitive or proprietary information such as mission logistics, customer data, and financial projections

- systems containing customer- or Internet-facing applications, including web applications

Each element and step in Figure 1 is described below.

"Vendor Provides" Element

One of the more difficult issues in effectively deploying and operating systems from a technology-centered practice perspective is allocating responsibility when the system relies heavily on a combination of vendor-supplied and other supplier components, as represented by the Vendor Provides element in Figure 1 (refer also to the Assembly and Integration content area). Most often, systems and software provided by vendors are general purpose; that is, they are fully featured with most of the software enabled for ease of use. They are meant to satisfy a wide range of customer needs and requirements. Such systems frequently contain

- services that are unneeded and often insecurely configured
- little to no protection on access to data objects such as files and directories
- vulnerabilities that intruders can use to break into systems
- ease-of-use features often provided at the expense of security
- latent errors that may emerge when components are combined in unexpected ways, resulting in unknown impact to the system's overall security posture

It is important to assign accountability for configuring the hundreds of security parameters in the average operating system product, especially taking into account the various and widely used combinations of operating systems, middleware, and applications software. It is up to purchasers of software applications to insist on the demonstration of full functionality of the application on hardened operating-system and middleware platforms. The need to "soften" the software status of the platform (with respect to security) to achieve application functionality is all too common. Community work in developing, implementing, and enforcing the use of effective consensus benchmarks[3] for securely configuring broadly used software products is providing demonstrable results.

---

[3] Such work is being done by the Center for Internet Security [CIS 08].

Harden/Secure Step

The Harden/Secure step strengthens a system against known attacks by eliminating vulnerabilities and other weaknesses commonly used by intruders. Practices include retaining only those services and features necessary to meet system requirements, removing or disabling those that are not necessary, and replacing those that are known to be insecure. Patch selection, installation, and prerelease testing occur here. Object access controls (such as default passwords) are eliminated, updated, and restricted based on role and need to know. Tools necessary for secure administration (such as antivirus, antispyware, vulnerability assessment, and software/system/network monitoring) are installed and tested. The practices performed during this step may change over time to address new attacks and vulnerabilities.

Prepare Step

An essential concept underlying the Prepare step is that undiscovered vulnerabilities exist. This requires an administrator to be able to recognize when previously unknown vulnerabilities start to be exploited. Practices to characterize normal system behavior are included here, such as capturing a trusted baseline state for all files and directories and periodically comparing the current state with the securely stored, trusted state to detect suspicious or unexpected behavior. Prepare also includes the configuration and installation of intrusion detection technology and other data collection mechanisms, such as firewall and log analysis tools, that are responsible for reporting suspicious or out-of-tolerance behavior.

Detect Step

The Detect step includes practices that determine whether an event has occurred and whether it is sufficiently noteworthy to require further investigation. Practices in this step include

- an initial analysis of reports from security tools installed during the Prepare step
- ongoing vulnerability assessment
- regular penetration testing. For further details, refer to the Penetration Testing content area on the BSI site.

Respond Step

The Respond step includes practices to analyze a security incident, including

- protecting necessary evidence
- containing the damage caused

- returning systems to normal operation (often while continuing to investigate the incident)
- increasing monitoring activity to mitigate against further damage and recurrence
- communicating with affected parties

Improve Step

The Improve step includes the following practices:

- conducting an incident postmortem review
- identifying and installing necessary improvements
- updating policies, procedures, and processes reflecting the improvements
- capturing business-case information on the costs incurred for future return-on-investment analyses

Additional Frameworks

Organizing Framework for Incident Management

An organizing framework for incident management is described in the BSI Incident Management content area and in Defining Incident Management Processes for CSIRTs (Computer Security Incident Response Teams) [Alberts 04]. This framework describes the following five high-level capabilities and their supporting processes:

- Prepare/Sustain/Improve (Prepare) – establish, sustain, and improve the CSIRT
- Protect Infrastructure (Protect) – make changes in the infrastructure to protect systems or mitigate an ongoing computer security event
- Detect Events (Detect) – recognize and report events when they occur and look for indicators that might identify future events/incidents
- Triage Events (Triage) – categorize, correlate, prioritize, and assign events to someone for further investigation and possible response
- Respond – plan, coordinate, and carry out effective response to incidents

IDEAL[SM] Model

The Software Engineering Institute's IDEAL model for software process improvement can be easily adapted for security practice deployment and has been tailored for information security governance [CGTF 04].

Visible Ops and Visible Ops Security

Work performed in collaboration with the IT Process Institute and the Institute of Internal Auditors has provided access to a community of practitioners who operate large, complex, highly secure, highly available operational systems. Practitioners responsible for deploying and operating such systems accomplish this, in part, by embedding well-defined security controls into mature IT operational processes such as change management (which includes patch management), configuration management, and release management.

The Visible Ops [ITPI 04] and Visible Ops Security [ITPI 08] methods describe this concept in detail, identifying the steps necessary to get an IT infrastructure that is out of control under control. This method takes into account technical, management, performance, monitoring, and audit practices for both operations and security. Visible Ops and Visible Ops Security are described in more detail in Integrating Security and IT and Prioritizing IT Controls for Effective, Measurable Security.

Chemical Sector Cyber Security Program

The American Chemistry Council's Chemical Information Technology Council (ChemITC)TM Chemical Sector Cyber Security Program describes a comprehensive Plan-Do-Check-Act cyber security management system that addresses securing manufacturing and control systems, IT, and the value chain for chemical-sector organizations. It includes "a collection of self-assessment questions and examples of how chemical companies are implementing cyber security practices" [CSCSP 06].

CONCLUSION

This article described a general approach to ensuring adequate security during deployment and operations of software-intensive systems. It recommended using a Plan-Do-Check-Act improvement cycle supported by essential prerequisites and practices necessary for security hygiene and provided several example implementation frameworks. The tables below provide a range of sources providing further guidance on how to go about this.

The Plan-Do-Check-Act approach described here can be used to deploy and operate the categories of practices described in the other articles in this content area.

Table 1: Indicators for Determining the Presence of Prerequisites

Table 1 provides indicators for each prerequisite to help determine its presence (or absence). Suggested sources for detailed practices are also listed. These describe, at varying levels, how to implement each prerequisite. The sources include other Build Security In content areas. Each source is fully cited on its first occurrence and summarized thereafter.

Table 1. Prerequisites for deploying and operating secure systems and software

Prerequisites	Indicators	Practice Sources
Management commitment to security	Sponsorship and oversight are visible, ongoing, active; leader roles and responsibilities are assigned, accepted, enacted, enforced	• Build Security In (BSI) Governance & Management, Acquisition, System Strategies, Business Case Models, Secure Software Development Life Cycle Process content areas • ISO 27002 (17799) *Code of practice for information security management* [ISO 05a] • ISO 27001 *Information security management systems* [ISO 05b] • NIST SP 800-100 Information Security Handbook [Bowen 06]
Security policy	Sponsored, developed, concise, implementable, documented, trained, enforced, reviewed, improved, reported on	• ISO 27002 [ISO 05a] • ISO 27001 [ISO 05b] • "Compliance Management," CERT Information Assurance Defense-in-Depth Curriculum [May 06] • "Report of the Best Practices and Metrics Teams," Appendix D [CISWG 04] • SANS Security Policy Project • CERT Podcast "Making Information Security Policy Happen" [CERT 08]
Security risk assessment results	Reviewed, acted on, periodically updated; asset-based; guided by security requirements, business objectives, and critical business services, processes, and assets	• BSI Architectural Risk Analysis, Risk Management, SDLC Process, Requirements Engineering content areas; D&O Article 2

		• "Risk Management," CERT Defense-in-Depth [May 06] • ISO 27005 Information Security Risk Management [ISO 08] • BS 7799-3 *Information security risk management* [BSI 06] • OCTAVE®[4] (CERT's Operationally Critical Threat, Assets, and Vulnerability Evaluation℠) • OCTAVE Allegro [Caralli 07] • NIST 800-100 [Bowen 06] • "Managing Enterprise Security Risk with NIST Standards" [Ross 07a] • "Managing Enterprise Risk in Today's World of Sophisticated Threats" [Ross 06] • FIPS 199 *Security Categorization of Federal Information and Information Systems* [NIST 04] • FIPS 200 *Minimum Security Requirements for Federal Information and Information Systems* [NIST 06] • NIST 800-53 *Recommended Security Controls for Federal Information Systems* [Ross 07b] • ISO 27001 [ISO 05b]
Security strategy and plan	Developed, reviewed, updated, reported on; ensures that security requirements and policy are met, security assurance accomplished, risks mitigated; reflects continuous review and improvement of security program	• NIST 800-18 *Guide for Developing Security Plans for Federal Information Systems* [Swanson 06] • BSI System Strategies, SDLC Process, Principles content areas

[4] OCTAVE is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University. Operationally Critical Threat, Asset, and Vulnerability Evaluation is a service mark of Carnegie Mellon University.

		• ISO 27001 [ISO 05b] • ISO 27005 [ISO 08] • NIST 800-100 [Bowen 06] • NIST 800-64 *Security Considerations in the Information Systems Development Life Cycle* [Kissel 08] • NIST 800-53, Planning (PL) [Ross 07b]
Program/project management	Executes strategy and plan; security is considered a project like any other business or IT project; ensures adequate security of all newly installed and updated software, and its security-compatibility with existing software/systems; manages all partners and other third parties having network and information access and providing software/ systems	• NIST 800-100 [Bowen 06] • ISO 27001 [ISO 05b]
Standard operating procedures and processes	Developed, measurable, trained, enforced, reviewed, updated, used as basis for traceability to legal requirements, standards, guidelines, and other practice frameworks	• ISO 27001 [ISO 05b] • BSI <a href="/sdlc>SDLC Process content area
Security budget	Sustained; regarded as a cost of doing business, not discretionary	• BSI Business Case Models content area • ISO 27001 [ISO 05b]
Security roles, responsibilities (security staff, users)	Defined, assigned, trained, enforced, enacted; serve as basis for authentication, authorization, access control, and basis for performance evaluation, as appropriate	• BSI Training & Awareness content area • ISO 27001 [ISO 05b] • ISO 13335-2 *Managing and planning IT Security* [ISO 97] • FIPS 200 *Minimum Security Requirements for Federal Information and Information Systems AT* [NIST 06]
Competent security staff	Trained, aware, competent, available when needed based on priorities	• BSI Training & Awareness content area • ISO 27001 [ISO 05b] • FIPS 200 AT [NIST 06]
Security measures	Defined, collected, analyzed, reviewed,	• BSI Measurement content

	reported on, acted on, updated; traceable to security plan and risk assessment results	area • "Report of the Best Practices and Metrics Teams" [CISWG 04] • CERT Defense-in-Depth [May 06] • NIST 800-53 [Ross 07b] • NIST 800-55 *Performance Measurement Guide for Information Security* [Chew 08] • NIST 800-100 [Bowen 06]

Table 2: Minimum Essential Security Practices Required for Security Hygiene

This table includes sources that identify the designated practices as necessary for security hygiene. Several provide implementation guidance. Each source is fully cited on its first occurrence and abbreviated thereafter.

Table 2. Minimum essential security practices required for security hygiene

Practice	Subpractice	Practice Sources
Build and maintain a secure network.	Install and maintain a firewall configuration to protect data.	• Payment Card Industry (PCI) Data Security Standard[5] [PCI 08] • FIPS 200 *Minimum Security Requirements for Federal Information and Information Systems* SC [NIST 06][6]

---

5 See also Wikipedia's Payment Card Industry entry for additional references [Wikipedia-PCI 08] and [Conner 06] for top-level guidance on how to implement the PCI standard.

6 FIPS 200 uses the following two-letter designators for security-related practice areas. These are used in this table to provide more direct traceability: AC (access control), AT (awareness and training), AU (audit and accountability), CA (certification, accreditation, and security assessments), CM (configuration management), CP (contingency planning), IA (identification and authentication), IR (incident response), MA (maintenance), MP (media protection), PE (physical and environmental protection), PL (planning), PS (personnel security), RA (risk assessment), SA (system and services acquisition), SC (system and communication protection), and SI (system and information integrity).

		• "Report of the Best Practices and Metrics Teams," Appendix C [CISWG 04] • "The 60 Minute Network Security Guide" [NSA 06] • BSI Principles and Guidelines content areas •
	Do not use vendor-supplied defaults for system passwords and other security parameters.	• PCI Standard [PCI 08] • FIPS 200 CM [NIST 06] • Center for Internet Security (CIS) Benchmarks[7] • NSA Security Configuration Guides
	Maintain an inventory of all devices, software, and services on the network.	• FIPS 200 CM [NIST 06] • 60 Minute Guide [NSA 06]
Protect sensitive data.	Protect stored data.	• PCI Standard [PCI 08] • FIPS 200 SI [NIST 06]
	Encrypt transmission of sensitive data across open, public networks.	• PCI Standard [PCI 08]
Maintain a vulnerability management program.	Use and regularly update antivirus software or programs. Guard against all forms of malicious code.	• PCI Standard [PCI 08]

[7] The Center for Internet Security's configuration benchmarks represent consensus among technical security experts from user organizations and software vendors. The benchmarks support "high level standards that deal with the "Why, Who, When, and Where" aspects of IT security by detailing "How" to secure an ever widening array of workstations, servers, network devices, and software applications in terms of technology specific controls."

		• FIPS 200 SI [NIST 06] • CISWG, Appendix C [CISWG 04] • 60 Minute Guide [NSA 06]
	Develop and maintain secure systems and applications. This includes secure configuration management, change management, and patch management.[8]	• PCI Standard [PCI 08] • FIPS 200 CA, CM, MA, SI [NIST 06] • CIS Benchmarks • NSA Security Configuration Guides • CISWG, Appendix C [CISWG 04] • 60 Minute Guide [NSA 06]
Implement strong access control measures.	Restrict access to data by business need to know.	• PCI Standard [PCI 08] • FIPS 200 AC, CA, MP [NIST 06] • CISWG, Appendix C [CISWG 04] • 60 Minute Guide [NSA 06]
	Assign a unique ID to each person with computer access.	• PCI Standard [PCI 08] • FIPS 200 IA [NIST 06] • CISWG, Appendix C [CISWG 04] • 60 Minute Guide [NSA 06]

[8] The next set of lower level practices in [PCI 08] includes 6.3.1 Test all security patches and configuration changes before deployment; 6.3.2 Separate development/test and production environments; 6.3.3 Ensure separation of duties between development/test personnel and production personnel; 6.3.4 Do not use production data for testing or development; 6.3.5 Remove test data and accounts before production systems become active; 6.3.6 Remove custom application accounts, user IDs, and passwords before applications become active; 6.3.7 Review custom code prior to release to production to identify vulnerabilities. Web applications are subject to additional controls (6.6).

	Restrict physical access to sensitive data.	• PCI Standard [PCI 08] • FIPS 200 PE [NIST 06] • CISWG, Appendix C [CISWG 04]
Regularly monitor and test networks.	Track and monitor all access to network resources and sensitive data.	• PCI Standard [PCI 08] • FIPS 200 AU, CA [NIST 06] • CISWG, Appendix C [CISWG 04] • 60 Minute Guide [NSA 06]
	Regularly test security systems and processes.	• PCI Standard [PCI 08] • FIPS 200 CA [NIST 06] • CISWG, Appendix C [CISWG 04] • 60 Minute Guide [NSA 06]
	Detect, respond to, and track security events and incidents.	• FIPS 200 CP, IR [NIST 06] • CISWG, Appendix C [CISWG 04] • 60 Minute Guide [NSA 06]
Maintain an information security policy. (See also Table 1.)	For employees and contractors. Policy includes topics such as acceptable use, roles/responsibilities, employee screening, incident response, access control, data backup and recovery, third party access, sanctions for non-compliance; include policy statements that require minimum essential practices included in this table.	• PCI Standard [PCI 08] • FIPS 200 PL, PS, SA [NIST 06] • CISWG, Appendix C [CISWG 04] • 60 Minute Guide [NSA 06]
Develop, deploy, and periodically refresh some level of security awareness and training. (See also Table 1.)		• FIPS 200 AT [NIST 06] • CISWG, Appendix C [CISWG 04]

Determine and implement a means for measuring practice effectiveness. (See also Table 1.)		• ISO 27001 [ISO 05b] • CISWG, Appendix C [CISWG 04] • FIPS 200 CA [NIST 06]
Ensure that third party providers deploy adequate security practices (at least this minimum essential set).	Includes outside parties with network access and those to whom applications and services have been outsourced	• FIPS 200 SA [NIST 06] • 60 Minute Guide [NSA 06]

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM-0001120