J. A. “Drew” Hamilton, Jr., Ph.D.

Director, Distributed Analytics & Security Institute
Director, Center for Cyber Innovation
Professor, Computer Science & Engineering

CCI
Post Office Box 9627
Mississippi State, MS 39762

Voice: (662) 325-2294
Fax: (662) 325-7692
hamilton@cci.msstate.edu

Outline (Designing, Performing, and Analyzing Security Testing) 12%

- Assessment and test strategies
- Security process data (e.g. management and operational controls)
- Security control testing
- Test outputs (e.g. automated, manual)
- Security architecture vulnerabilities

Assessment and test strategies

Dr. C.W. Perr, Sandia Labs

Reference: Shon Harris

Security Software

- Antivirus/Antimalware
- Intrusion Detection/Intrusion Prevention Systems
- Remote Access Software (VPNs)
- Web Proxies
- Vulnerability Management Software
- Authentication Servers
- Routers
- Firewalls
- Network Access Control (NAC) /
  Network Access Protection (NAP)

Software Testing Strategies

- Black Box Testing vs. White Box Testing
- Dynamic Testing vs. Static Testing
- Manual Testing vs. Automated Testing
- ISC2 Software Testing Tenets
  - The expected test outcome is predefined
  - A good test case has a high probability of exposing an error
  - A successful test is one that finds an error
  - Testing is independent of coding
  - Both application (user) and software (programming) expertise are employed
  - Testers use different tools from coders
  - Examining only the usual case is insufficient
  - Test documentation permits its reuse and an independent confirmation of the pass/fail status of a test outcome during a subsequent review.

Test Strategies

- A backdoor is a program that is installed by an attacker to enable them to come back into the computer at a later date without having to supply login credentials or go through any type of authorization process
  - Such behaviors can often be detected by host-based intrusion detection systems

Test Strategies

- **Goals of a vulnerability testing assessment**
  - **Evaluate the true security posture of an environment (minimize false positives)**
  - **Identify as many vulnerabilities as possible with honest evaluations and prioritization of each**
  - **Test how systems react to certain circumstances and attacks, to learn not only what the known vulnerabilities are (given a specific operating environment), but also how the unique elements of the environment might be abused (such as SQL injection attacks, buffer overflows, and process design flaws that facilitate social engineering)**

Test Strategies

- **Highlighted caution:** **Before carrying out vulnerability testing, a written agreement from management is required!**
  - **This protects the tester against prosecution for doing his job, and ensures there are no misunderstandings by providing in writing what the tester should – and should not – do.**

Test Strategies

- Personnel testing: includes reviewing employee tasks and thus identifying vulnerabilities in the standard practices and procedures that employees are instructed to follow, demonstrating social engineering attacks and the value of training users to detect and resist such attacks, and reviewing employee policies and procedures to ensure those security risks that cannot be reduced through physical and logical controls are met with the final control category (Administrative)

Test Strategies

- **Physical testing: includes reviewing facility and perimeter protection mechanisms.**
  - **For example do the doors automatically close and an alarm sound if the door is open too long?**
  - **Are interior protection mechanisms of server rooms, wiring closets, sensitive systems, and assets appropriate?**
  - **Is dumpster diving a threat? What of protection mechanisms for manmade, natural, or technical threats?**
  - **Is there a fire suppression system?**
  - **Are sensitive electronics kept above raised floors so they survive a minor flood?**

Test Strategies

- Systems and network testing: perhaps what most people think of when discussing information security vulnerability testing. For efficiency, an automated scanning product identifies known system vulnerabilities, and some may (if management has signed off on the performance impact and the risk of disruption) attempt to exploit vulnerabilities

Test Strategies

- **Penetration Testing: the process of simulating attacks on a network and its systems at the request of the owner or senior management**
  - **Measures an organization's level of resistance to an attack and uncovers weaknesses within their environment**
  - **Foundation is established by a vulnerability scan**

Test Strategies

- Highlighted note: A “Get Out of Jail Free Card” is a document you can present to someone who thinks you are up to something malicious, when in fact you are carrying out an approved test.
- There have been many situations in which an individual (or a team) was carrying out a penetration test and was approached by a security guard or someone who thought this person was in the wrong place at the wrong time

Test Strategies

The process steps of a penetration test:

1. Discovery: Footprinting and information gathering
2. Enumeration: Port scans and resource identification
3. Vulnerability mapping: Identifying vulnerabilities
4. Exploitation: Gaining unauthorized access
5. Reporting: Documentation and suggestions to management

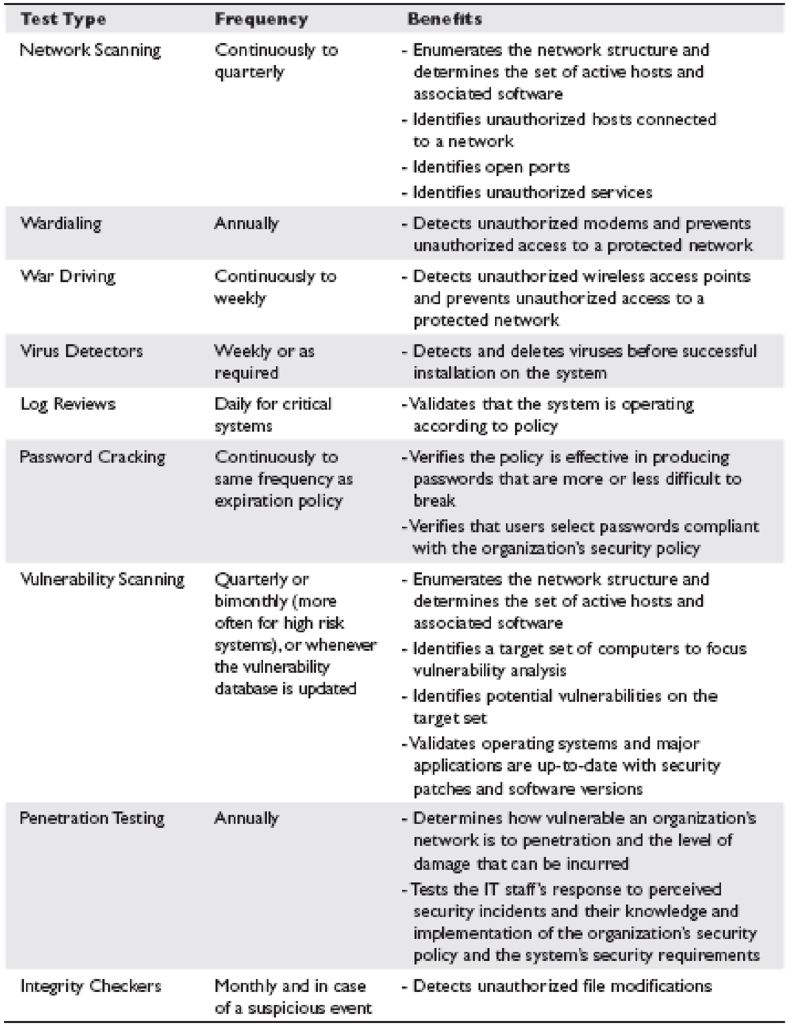
Threats to Operations Security

- Types of tests
  - Zero knowledge v. partial knowledge (advance knowledge of the tester)
  - Blind, double-blind, or targeted (use of public knowledge or targeted knowledge, and whether the staff is aware)

Threats to Operations Security

- **Vulnerability targets**
  - Kernel flaws: fixed by patching
  - Buffer overflows: fixed by defensive programming and developer education
  - Symbolic links: fixed by requiring scripts to ensure use of fully qualified paths
  - File descriptor attacks: fixed by defensive programming and developer education
  - Race conditions: fixed by defensive programming and developer education
  - File and directory permissions: fixed by use of file integrity checkers

Test Strategies



Test Type	Frequency	Benefits
Network Scanning	Continuously to quarterly	- Enumerates the network structure and determines the set of active hosts and associated software - Identifies unauthorized hosts connected to a network - Identifies open ports - Identifies unauthorized services
Wardialing	Annually	- Detects unauthorized modems and prevents unauthorized access to a protected network
War Driving	Continuously to weekly	- Detects unauthorized wireless access points and prevents unauthorized access to a protected network
Virus Detectors	Weekly or as required	- Detects and deletes viruses before successful installation on the system
Log Reviews	Daily for critical systems	- Validates that the system is operating according to policy
Password Cracking	Continuously to same frequency as expiration policy	- Verifies the policy is effective in producing passwords that are more or less difficult to break - Verifies that users select passwords compliant with the organization's security policy
Vulnerability Scanning	Quarterly or bimonthly (more often for high risk systems), or whenever the vulnerability database is updated	- Enumerates the network structure and determines the set of active hosts and associated software - Identifies a target set of computers to focus vulnerability analysis - Identifies potential vulnerabilities on the target set - Validates operating systems and major applications are up-to-date with security patches and software versions
Penetration Testing	Annually	- Determines how vulnerable an organization's network is to penetration and the level of damage that can be incurred - Tests the IT staff's response to perceived security incidents and their knowledge and implementation of the organization's security policy and the system's security requirements
Integrity Checkers	Monthly and in case of a suspicious event	- Detects unauthorized file modifications

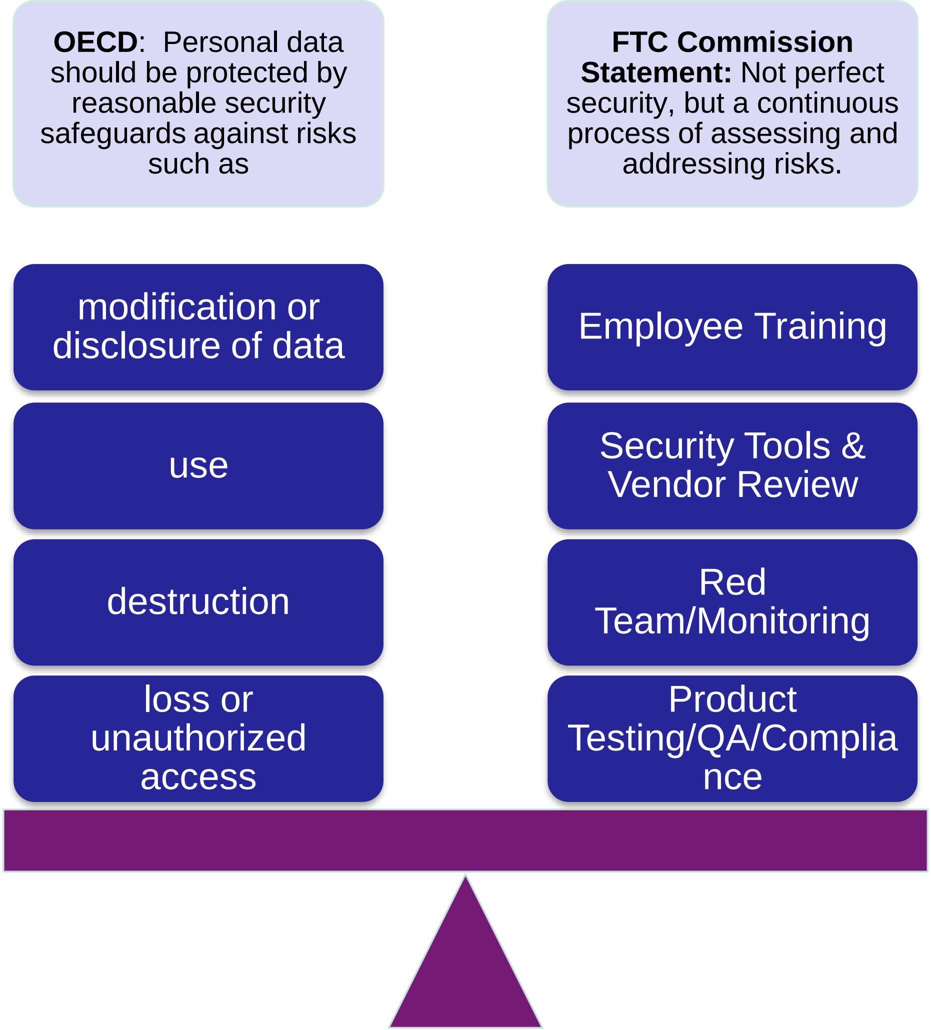
Table 12-3 Example Testing Schedules for Each Operations and Security Department

Security process data (e.g. management and operational controls)

Reference: Association of Corporate Counsel

Reference: CPSC 4670, UTC

Security Standard: “reasonable security”



OECD: Personal data should be protected by reasonable security safeguards against risks such as

- modification or disclosure of data
- use
- destruction
- loss or unauthorized access

FTC Commission Statement: Not perfect security, but a continuous process of assessing and addressing risks.

- Employee Training
- Security Tools & Vendor Review
- Red Team/Monitoring
- Product Testing/QA/Complia nce

California AG 2016 Data Breach Report

CA Statute: Requires businesses to use "reasonable security procedures and practices… to protect personal information from unauthorized access, destruction, use, modification, or disclosure."

The 20 Controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all of the Controls that apply to an organization's environment constitutes a lack of reasonable security.

Full List of 20 Controls

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Security configurations for Hardware and Software on Mobile Devices, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browsing Protection
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capability
11. Secure configurations for Network Devices such as Firewalls, Routers, and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Security Standard: “reasonable security”

Few examples of “reasonable security” failures from Enforcement Actions:

PRODUCT TESTING/QA/RISK ASSESSMENT/COMPLIANCE

- Code Review
- Design Review
- Test Product against Choice Mechanisms (*Asutek Computer*)
- Security Audits/investigations (Microsoft)
- Monitor compliance (*CVS*)

RED TEAM TESTING/REGULAR MONITORING

- Pen Testing
- Bug Bounty Program or Process to investigate vulnerability research (*Asutek Computer*)
- Widely known security flaws (*Lookout*)
- Network scanning (*EPN*)
- Anti-virus (*Lifelock*)
- Security warning process (*TJX*)

SECURITY TOOLS

- Use SSL/encryption to protect information (*Credit Karma; Fandango*)
- Password policies and regular required password changes (*Lifelock/Twitter/Reed Elsevier*)
- Access/Identity Management (*CBR/Accretive Health*)

VENDOR REVIEW

- Should make sure vendors implement reasonable security (*GMR Transcription/Credit Karma*)

TRAINING

- Train employees adequately on infosec and privacy (*Upromise/HTC/Tower Records*)
- Incident response training and plan (*EPN*)

In 2014, FTC reached 50 enforcement actions – so number continues to grow.

“Good Computing Practices”
10 Safeguards for Users

1. User ID or Log-In Name (aka. User Access Controls)
2. Passwords
3. Workstation Security
4. Portable Device Security
5. Data Management, e.g., back-up, archive, restore.
6. Remote Access
7. Recycling Electronic Media & Computers
8. E-Mail
9. Safe Internet Use
10. Reporting Security Incidents / Breach

Safeguard - #1: Unique User Log-In / User Access Controls

- **Access Controls:**
  - Users are assigned a unique "User ID" for log-in purposes
  - Each individual user's access to PII system(s) is appropriate and authorized
  - Access is "role-based", e.g., access is limited to the minimum information needed to do your job
  - Unauthorized access to PII by former employees is prevented by terminating access
  - User access to information systems is logged and audited for inappropriate access or use.

Safeguard - #2: Password Protection

Passwords will be assigned to you for most data systems to comply with the security rule, but when necessary here are guidelines for choosing a password:

- Don't use a word that can easily be found in a dictionary — English or otherwise.
- Use at least eight characters (letters, numbers, symbols)
- Don't share your password — protect it the same as you would the key to your residence. After all, it is a "key" to your identity.
- Don't let your Web browser remember your passwords. Public or shared computers allow others access to your password.

Safeguard - #3: Workstation Security

- "Workstations" include any electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions.
- Physical Security measures include:
  - Disaster Controls
    - Protect workstations from natural and environmental hazards, such as heat, liquids, water leaks and flooding, disruption of power, conditions exceeding equipment limits.
  - Device & Media Controls:
    - Auto Log-Off or Automatic Screen Savers

Safeguard - #4: Security for Portable Devices & Laptops with PII

- **Implement the workstation physical security measures listed in Safeguard #3, including this Check List:**
  - **Use an Internet Firewall**
  - **Use up-to-date Anti-virus software**
  - **Install computer software updates, e.g., Microsoft patches**
  - **Encrypt and password protect portable devices, e.g. USB memory stick**
  - **Lock-it up!, e.g., Lock office or file cabinet, cable**
  - **Automatic log-off from programs is possible**
  - **Use password protected screen savers**
  - **Back-up critical data and software programs**
  - **De-identify PII or delete PII from memory stick or PDA**
  - **Disable wireless or use VPN**

Safeguard - #5: Data Management & Security

- Data backup and storage
  - Backup original data files with PII and other essential data and software programs frequently based on data criticality, e.g., daily, weekly, monthly.
  - Consider encrypting back-up disks
  - Permanent copies of PII should not be stored for archival purposes on portable device, such as laptop computers, PDAs and memory sticks.
  - If necessary, temporary copies could be used on portable devices, only when:
    - The storage is limited to the duration of the necessary use; <u>and</u>
    - If protective measures, such as encryption, are used to safeguard the confidentiality, integrity and availability of the data in the event of theft or loss.
- Transferring and downloading data
  - Encryption is an important tool for protection of PII in transit across unsecured networks and communication systems
- Data disposal
  - Destroy PII data which is no longer needed (professional overwrite)

Safeguard - #6: Remote Access

- Need to consider authentication such as Radius
- Can adopt Virtual Private Network to encrypt communication in transit
- Use access control to authorize users
- Audit behavior of remote users

Safeguard - #7: E-Mail Security

- Email is like a "postcard".
  - Email may potentially be viewed in transit by many individuals, since it may pass through several switches enroute to its final destination or never arrive at all!
- Although the risks to a single piece of email are small given the volume of email traffic, emails containing PII need a higher level of security.

7-1 Should You Open the E-mail Attachment?

If it's suspicious, don't open it!

What is suspicious?

- Not work-related
- Attachments not expected
- Attachments with a suspicious file extension (*.exe, *.vbs, *.bin, *.com, or *.pif)
- Web link
- Unusual topic lines; "Your car?"; "Oh!" ; "Nice Pic!"; "Family Update!"; "Very Funny!"

7-2. E-Mail Security – Risk Areas

1. **Spamming.** Unsolicited bulk e-mail, including commercial solicitations, advertisements, chain letters, pyramid schemes, and fraudulent offers.
   - Do not reply to spam messages. Do not spread spam.
   - Do not forward chain letters. It's the same as spamming!
   - Do not open or reply to suspicious e-mails.
2. **Phishing Scams.** E-Mail pretending to be from trusted names, such as Citibank or Paypal or Amazon, but directing recipients to rogue sites. A reputable company will never ask you to send your password through e-mail.
3. **Spyware.** Spyware is adware which can slow computer processing down; hijack web browsers; spy on key strokes and cripple computers

7-3. Instant Messaging (IM) - Risks

- Instant messaging (IM) and Instant Relay Chat (IRC) or chat rooms create ways to communicate or chat in “real-time” over the Internet.
- Exercise extreme caution when using Instant Messaging on Computers:
  - Maintain up-to-date virus protection and firewalls, since IM may leave networks vulnerable to viruses, spam and open to attackers / hackers.
  - Do not reveal personal details while in a Chat Room
  - Be aware that this area of the Internet is not private and subject to scrutiny

Safeguard - #8: Internet Use

- **Be careful about providing personal, sensitive or confidential information to an Internet site or to web-based surveys that are not from trusted sources.**
- **Personal information posted to web-pages may not be protected from unauthorized use.**
- **Even unlinked web pages can be found by search engines**
- **Some web sites try to place small files ("cookies") on your computer that might help others track the web pages you access**

Remember: **The Internet is not private!** Access to any site on the Internet could be traced to your name and location.

Safeguard - #9: Report Security Incidents

- Users are responsible for:
  - Report and respond to security incidents and security breaches.
  - Know what to do in the event of a security breach or incident related to ePHI and/or Personal Information.
- Security Incident defined:
  - "The attempted or successful improper instance of unauthorized access to, or use of information, or misuse of information, disclosure, modification, or destruction of information or interference with system operations in an information system.“ [45 CFR 164.304]

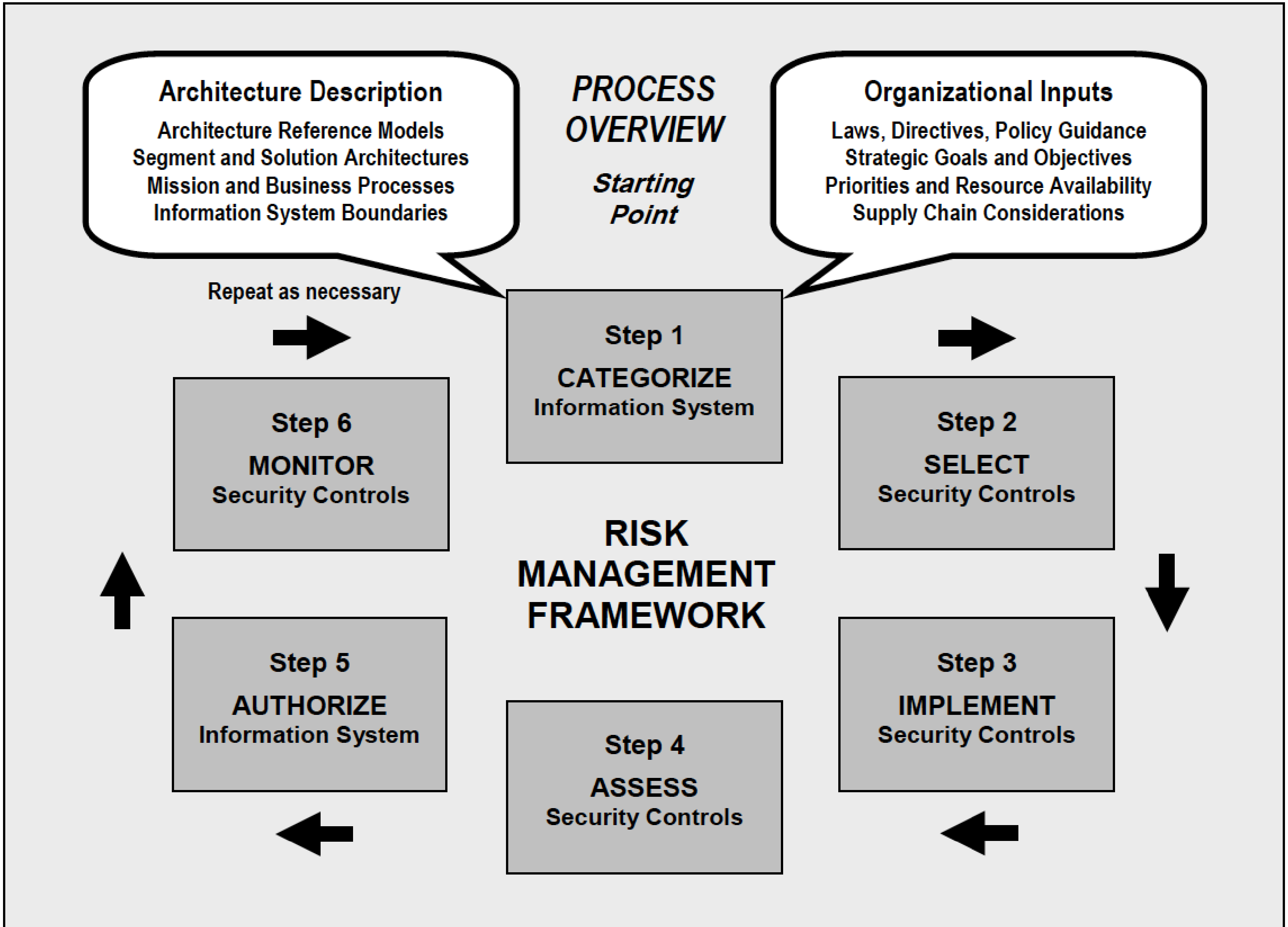
Safeguard-#10: User Responsibility to Adhere to Information Security Policies

- CIO or CISO may use the following language in their trainings
- "Users of electronic information resources are responsible for complying with all policies, procedures and standards relating to information security."
- "Workforce members who violate policies regarding privacy / security of confidential, restricted and/or PII are subject to further corrective and disciplinary actions according to existing policies."
- "Actions taken could include:
  - Termination of employment
  - Possible further legal action
  - Violation of local, State and Federal laws may carry additional consequences of prosecution under the law, costs of litigation, payment of damages, (or both); or all.
  - Knowing, malicious intent → Penalties, fines, jail!"

NIST 800-137 RMF & Controls

- ***Categorize***
  - the information system and the information processed, stored, and transmitted by that system based on an impact analysis.
- ***Select***
  - an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.
- ***Implement***
  - the security controls and describe how the controls are employed within the information system and its environment of operation.
- ***Assess***
  - the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- ***Authorize***
  - information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.
- ***Monitor***
  - the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

NIST 800-137 RMF



Architecture Description

Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries

PROCESS OVERVIEW

Starting Point

Organizational Inputs

Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations

Repeat as necessary

Step 1
CATEGORIZE
Information System

Step 2
SELECT
Security Controls

Step 3
IMPLEMENT
Security Controls

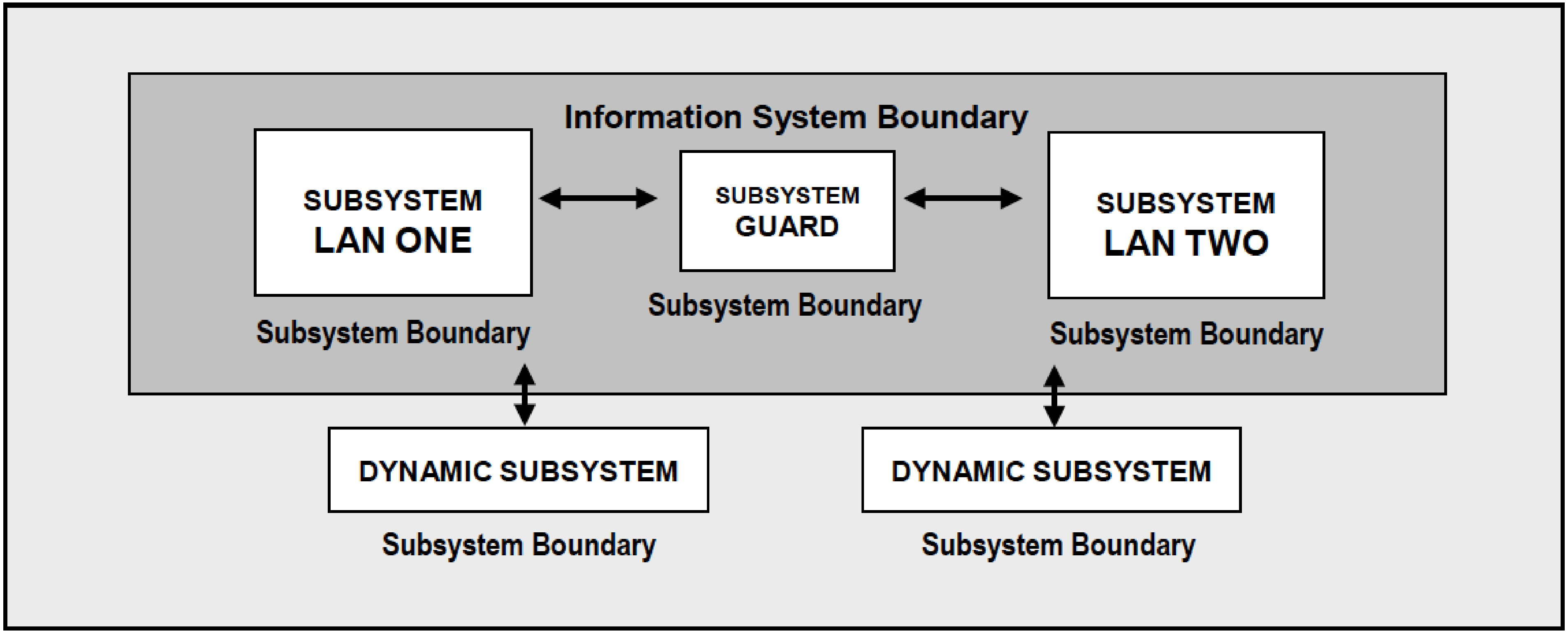
Step 4
ASSESS
Security Controls

Step 5
AUTHORIZE
Information System

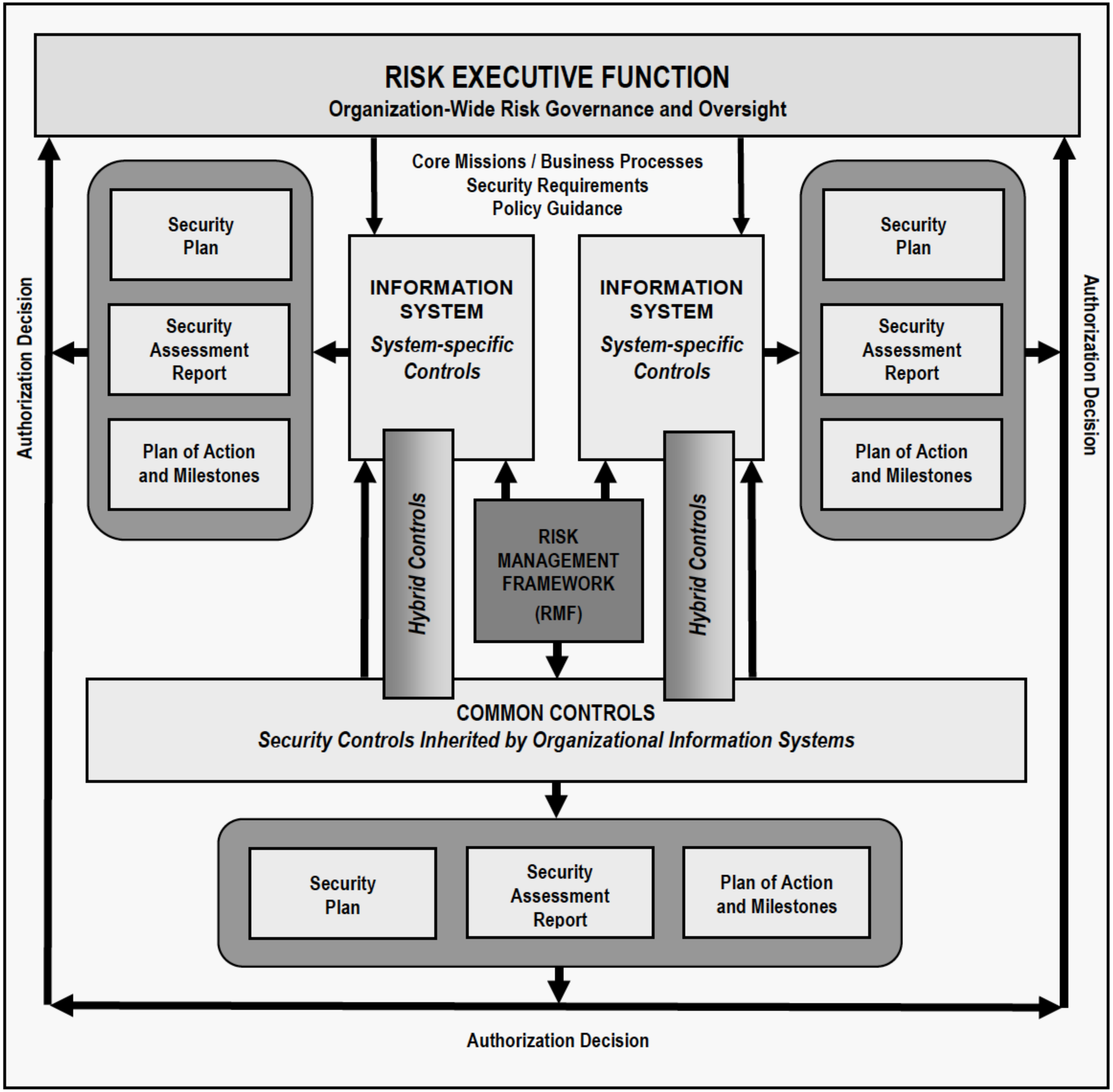
Step 6
MONITOR
Security Controls

RISK MANAGEMENT FRAMEWORK

Decomposition of a Complex IS



Security Control Allocation



RISK EXECUTIVE FUNCTION

Organization-Wide Risk Governance and Oversight

Core Missions / Business Processes
Security Requirements
Policy Guidance

Security Plan

Security Assessment Report

Plan of Action and Milestones

INFORMATION SYSTEM

System-specific Controls

INFORMATION SYSTEM

System-specific Controls

Security Plan

Security Assessment Report

Plan of Action and Milestones

Authorization Decision

Authorization Decision

Hybrid Controls

RISK MANAGEMENT FRAMEWORK (RMF)

Hybrid Controls

COMMON CONTROLS

Security Controls Inherited by Organizational Information Systems

Security Plan

Security Assessment Report

Plan of Action and Milestones

Authorization Decision

Security control testing

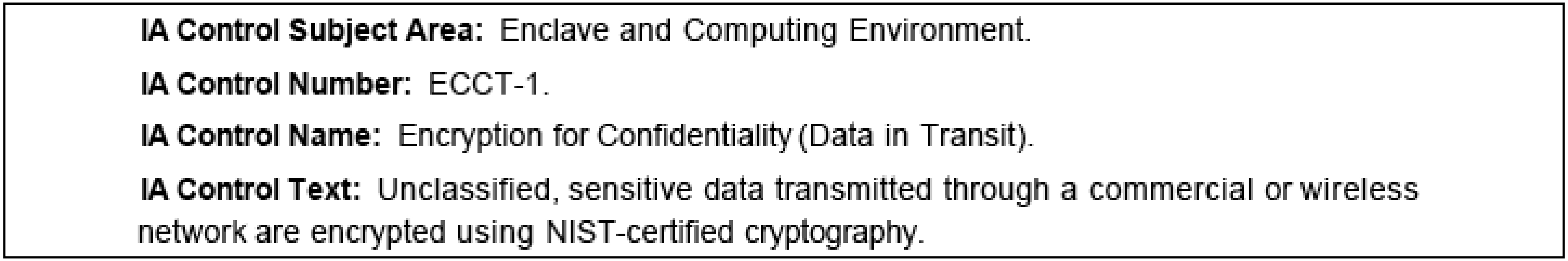
Dr. Drew Hamilton

ISC2 continuum of controls relative to the timeline of a security incident

- Directive
  - Controls designed to specify acceptable rules of behavior within an organization
- Deterrent
  - Controls designed to discourage people from violating security
- Preventive
  - Controls implemented to prevent a security incident or information breach
- Compensating
  - Controls implemented to substitute for the loss of primary controls and mitigate risk down to an acceptable level
- Detective
  - Controls designed to signal a warning when a security control has been breached
- Corrective
  - Controls implemented to remedy circumstance, mitigate damage, or restore controls
- Recovery
  - Controls implemented to restore conditions to normal after a security incident

IA Controls (Enclosure 4, DoDI 8500.2)

- **IA Control Subject Area. One of eight groups indicating the major subject or focus area to which an individual IA Control is assigned. (Next Slide)**
- **IA Control Number. A unique identifier comprised of four letters, a dash, and a number. The first two letters are an abbreviation for the subject area name and the second two letters are an abbreviation for the individual IA Control name. The number represents a level of robustness in ascending order that is relative to each IA Control. (Next Slide)**
- **IA Control Name. A brief title phrase that describes the individual IA Control.**
- **IA Control Text. One or more sentences that describe the IA condition or state that the IA Control is intended to achieve.**



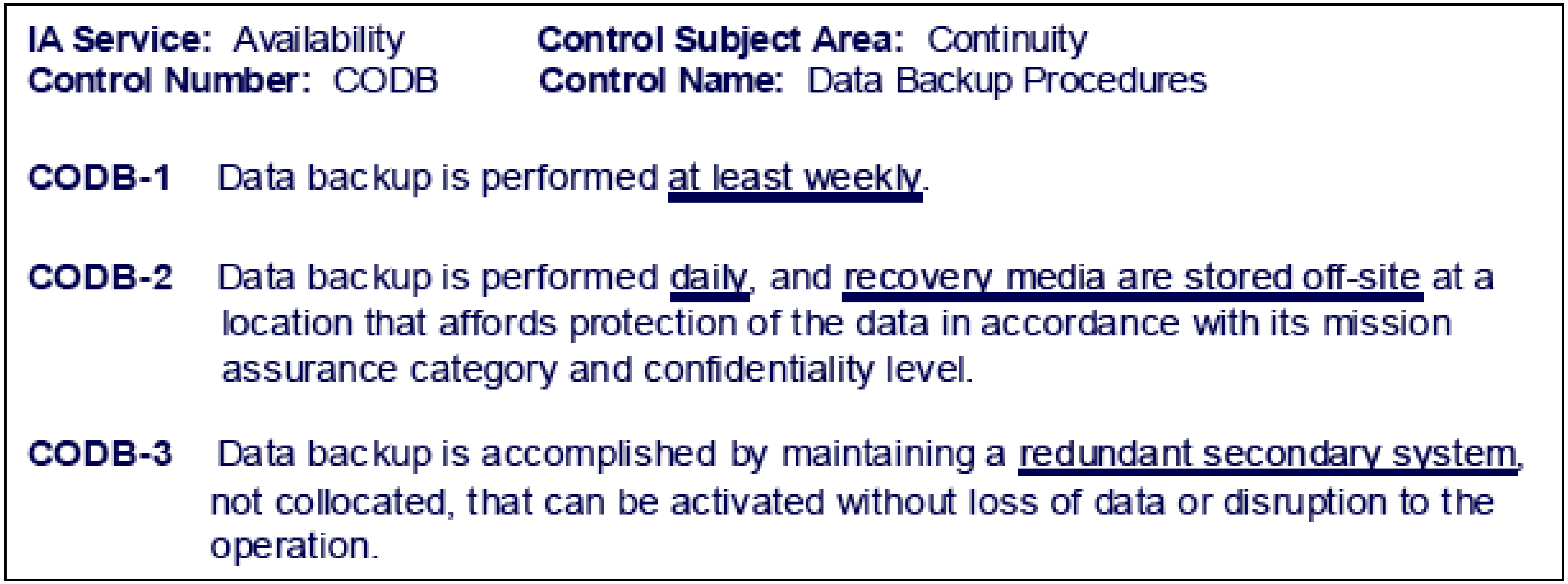
IA Control Subject Area: Enclave and Computing Environment.

IA Control Number: ECCT-1.

IA Control Name: Encryption for Confidentiality (Data in Transit).

IA Control Text: Unclassified, sensitive data transmitted through a commercial or wireless network are encrypted using NIST-certified cryptography.

Another IA Control Example



IA Service: Availability **Control Subject Area:** Continuity
Control Number: CODB **Control Name:** Data Backup Procedures

CODB-1 Data backup is performed at least weekly.

CODB-2 Data backup is performed daily, and recovery media are stored off-site at a location that affords protection of the data in accordance with its mission assurance category and confidentiality level.

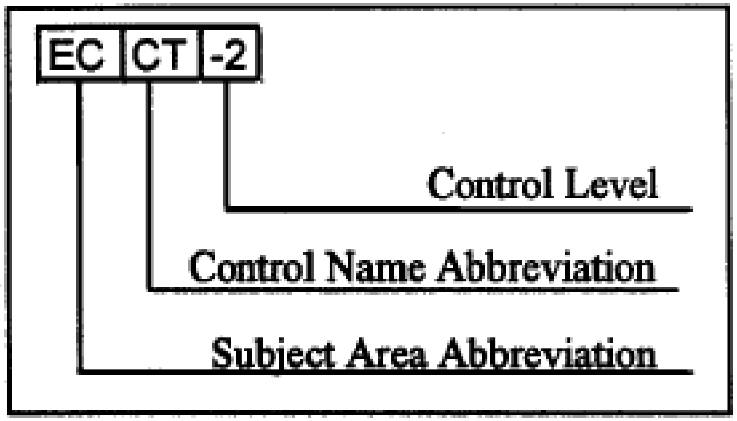
CODB-3 Data backup is accomplished by maintaining a redundant secondary system, not collocated, that can be activated without loss of data or disruption to the operation.

IA Control Subject Areas

Enclosure 4, DoDI 8500.2

Abbreviation	Subject Area Name	Number of Controls in Subject Area
DC	Security Design & Configuration	31
IA	Identification and Authentication	9
EC	Enclave and Computing Environment	48
EB	Enclave Boundary Defense	8
PE	Physical and Environmental	27
PR	Personnel	7
CO	Continuity	24
VI	Vulnerability and Incident Management	3

- **In the example to the right --> the control level is two (2), which means there is a related IA Control, ECCT-1, that provides less robustness. There may also be an IA Control, ECCT-3, that provides greater robustness.**


EC CT -2

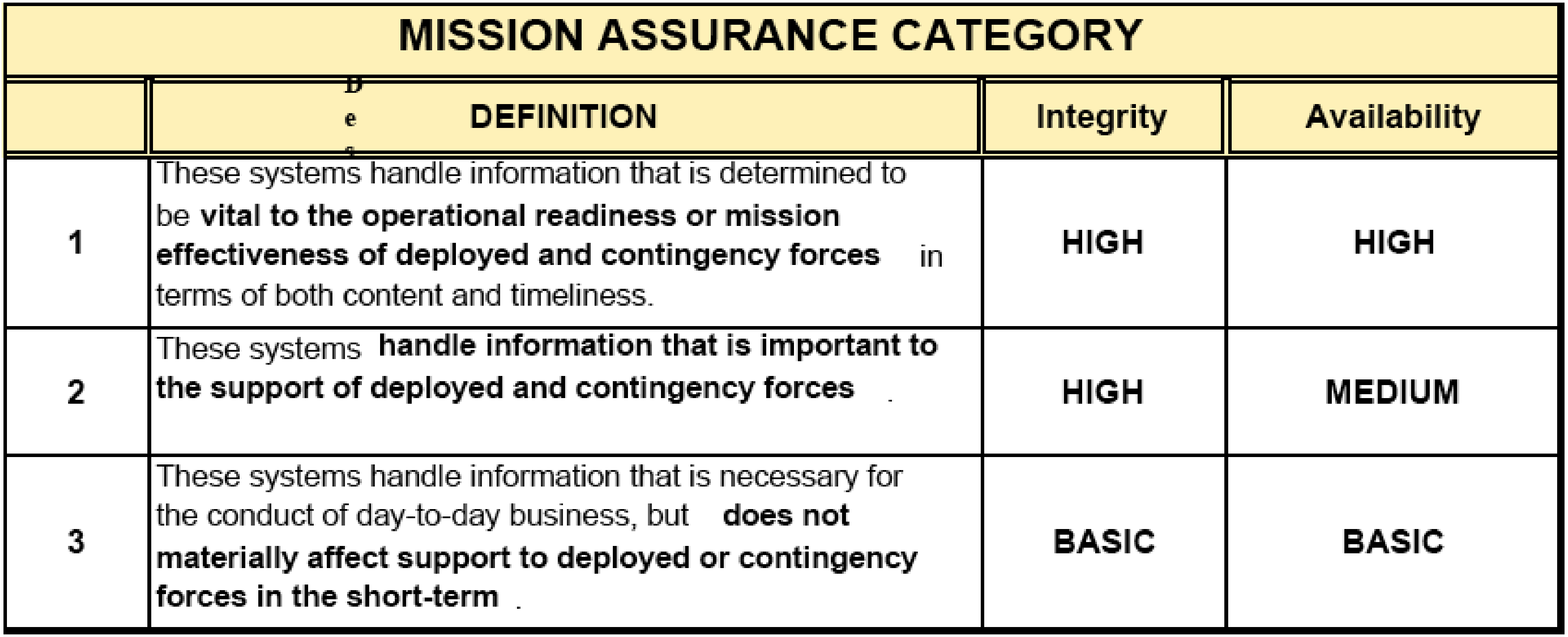
Control Level

Control Name Abbreviation

Subject Area Abbreviation

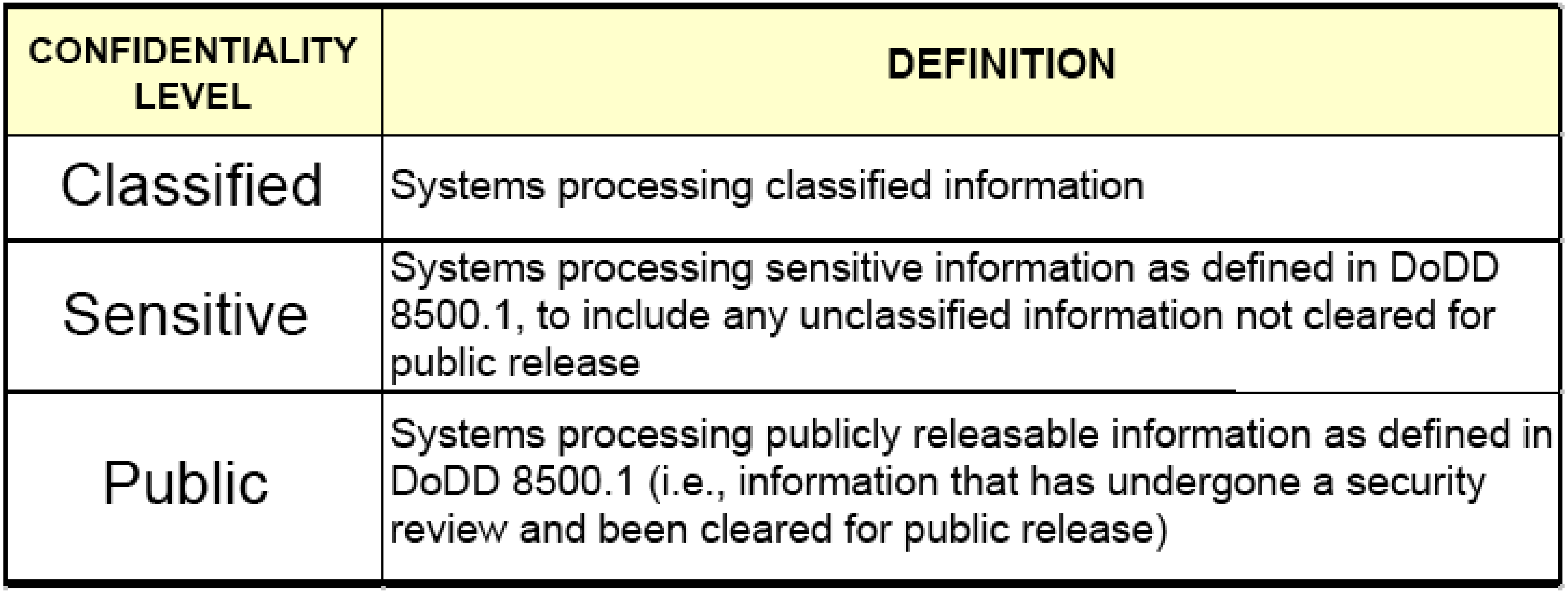
Mission Assurance Category Summary
DoDI 8500.2 Enclosure 3

- The baseline sets of IA controls are pre-defined based on the determination of the Mission Assurance Category (MAC) and Confidentiality Levels as specified in the formal requirements documentation or by the info owner.
- IA Controls addressing availability, confidentiality, integrity, authentication and non-repudiation requirements are keyed to the system's MAC based on the importance of the information to the mission, particularly the warfighters' combat mission, and on the sensitivity or classification of the information.



MISSION ASSURANCE CATEGORY			
	DEFINITION	Integrity	Availability
1	These systems handle information that is determined to be **vital to the operational readiness or mission effectiveness of deployed and contingency forces** in terms of both content and timeliness.	HIGH	HIGH
2	These systems **handle information that is important to the support of deployed and contingency forces** .	HIGH	MEDIUM
3	These systems handle information that is necessary for the conduct of day-to-day business, but **does not materially affect support to deployed or contingency forces in the short-term** .	BASIC	BASIC

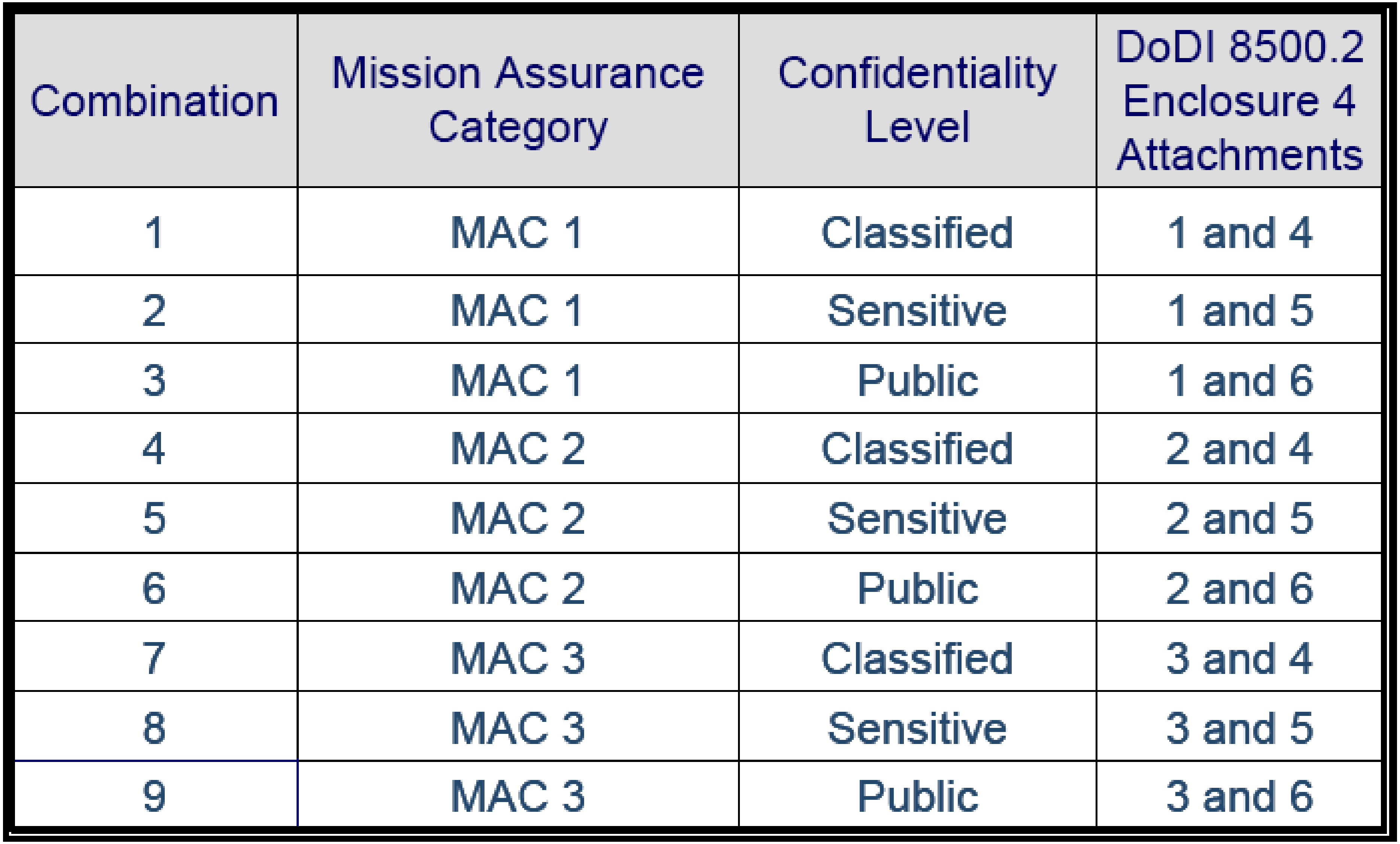
Mission Assurance Category Levels for IA Controls



CONFIDENTIALITY LEVEL	DEFINITION
Classified	Systems processing classified information
Sensitive	Systems processing sensitive information as defined in DoDD 8500.1, to include any unclassified information not cleared for public release
Public	Systems processing publicly releasable information as defined in DoDD 8500.1 (i.e., information that has undergone a security review and been cleared for public release)

- **IA Controls addressing confidentiality requirements are based on the sensitivity or classification of the information.**
- **There are three MAC levels and three confidentiality levels with each level representing increasingly stringent information assurance requirements.**

Determining Baseline IA Controls



Combination	Mission Assurance Category	Confidentiality Level	DoDI 8500.2 Enclosure 4 Attachments
1	MAC 1	Classified	1 and 4
2	MAC 1	Sensitive	1 and 5
3	MAC 1	Public	1 and 6
4	MAC 2	Classified	2 and 4
5	MAC 2	Sensitive	2 and 5
6	MAC 2	Public	2 and 6
7	MAC 3	Classified	3 and 4
8	MAC 3	Sensitive	3 and 5
9	MAC 3	Public	3 and 6

NIST SP 800-53r4

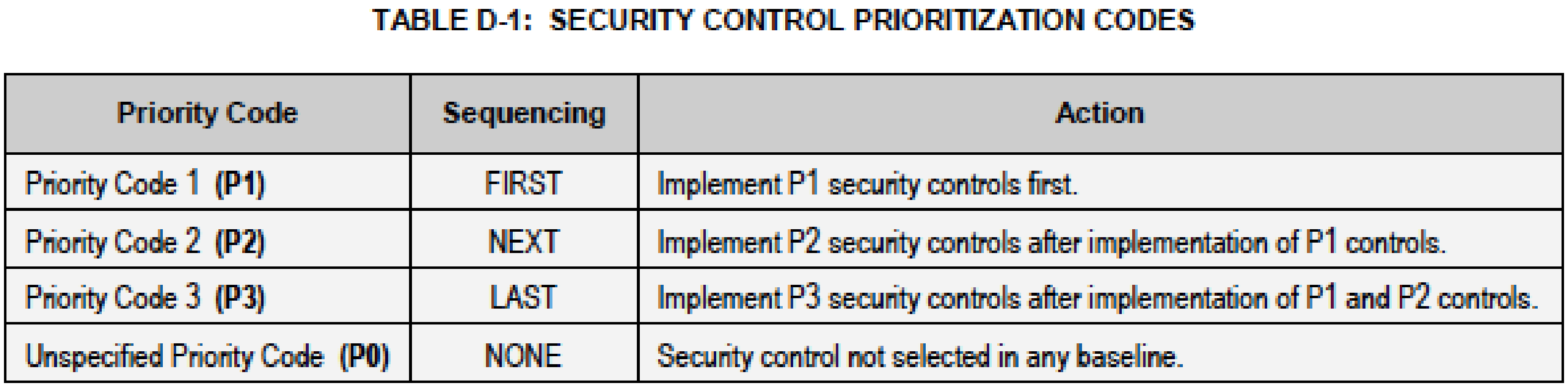


TABLE D-1: SECURITY CONTROL PRIORITIZATION CODES

Priority Code	Sequencing	Action
Priority Code 1 **(P1)**	FIRST	Implement P1 security controls first.
Priority Code 2 **(P2)**	NEXT	Implement P2 security controls after implementation of P1 controls.
Priority Code 3 **(P3)**	LAST	Implement P3 security controls after implementation of P1 and P2 controls.
Unspecified Priority Code **(P0)**	NONE	Security control not selected in any baseline.

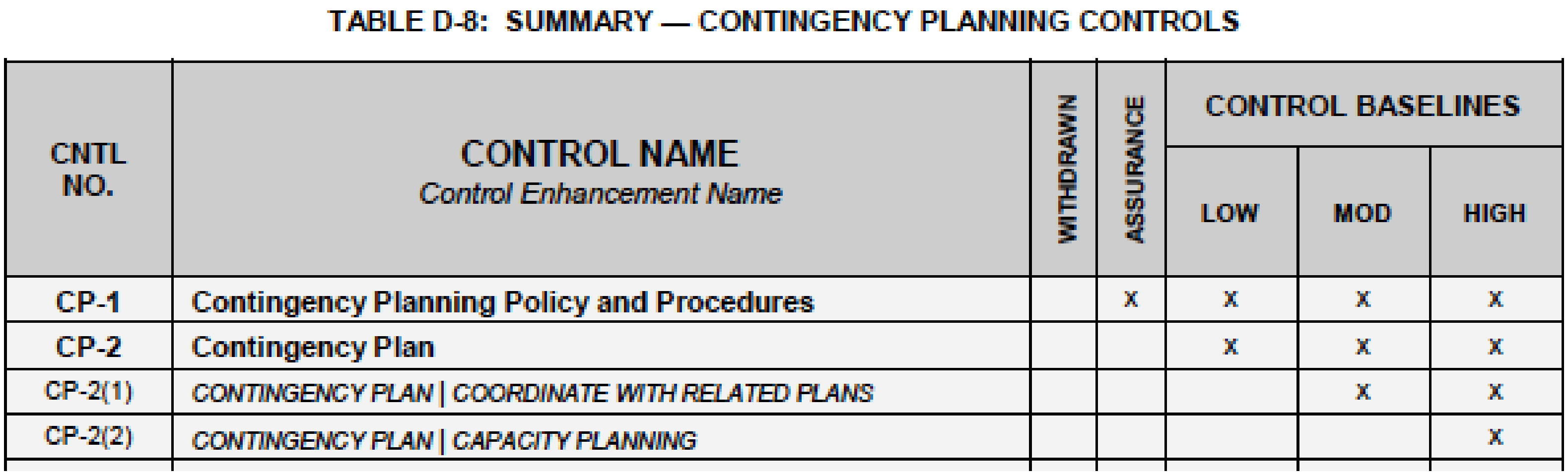


TABLE D-8: SUMMARY — CONTINGENCY PLANNING CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CP-1	**Contingency Planning Policy and Procedures**		x	x	x	x
CP-2	**Contingency Plan**			x	x	x
CP-2(1)	*CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS*				x	x
CP-2(2)	*CONTINGENCY PLAN | CAPACITY PLANNING*					x

NIST SP 800-53r4

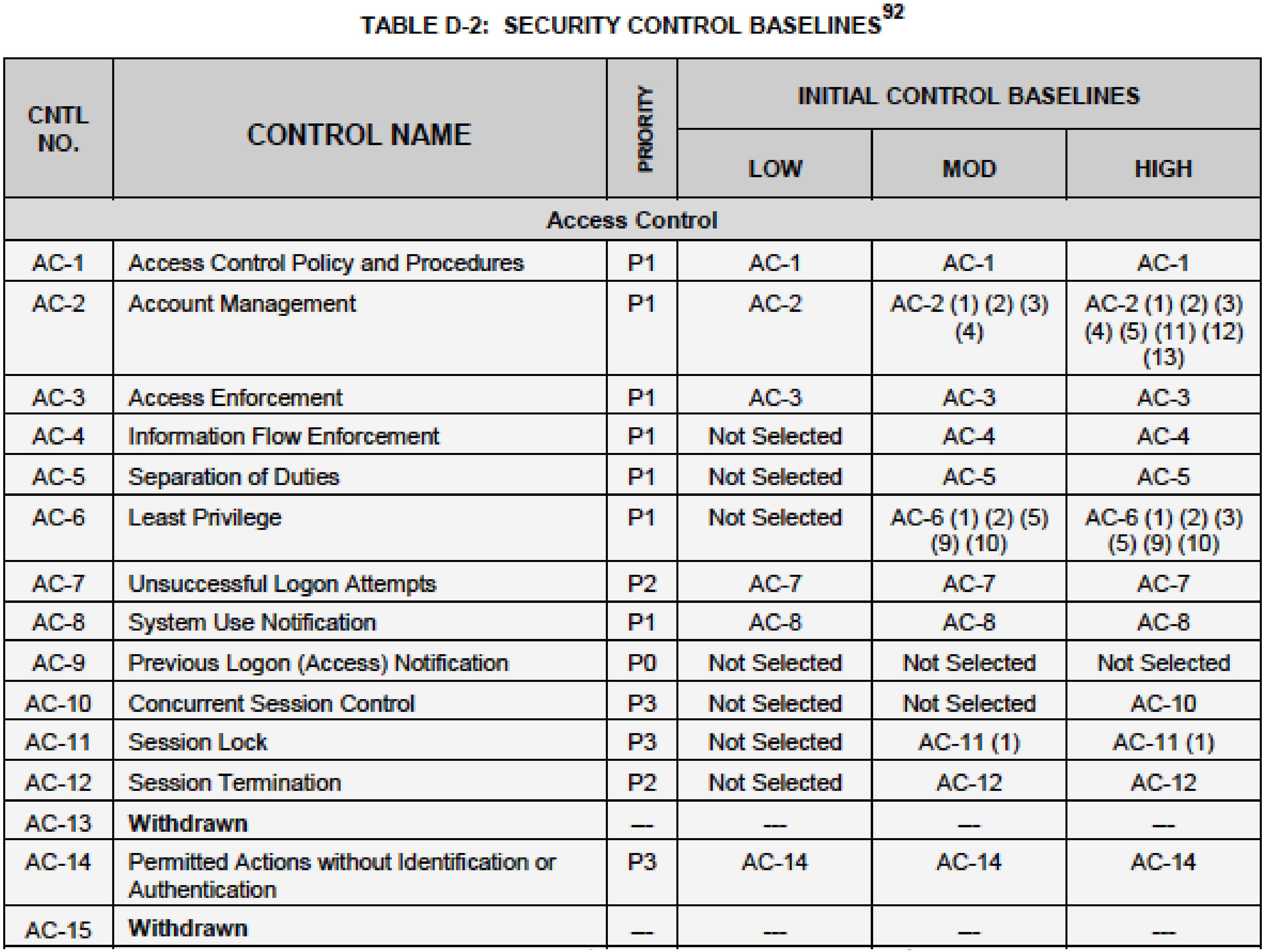


TABLE D-2: SECURITY CONTROL BASELINES[92]

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Access Control					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P3	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	P2	Not Selected	AC-12	AC-12
AC-13	**Withdrawn**	---	---	---	---
AC-14	Permitted Actions without Identification or Authentication	P3	AC-14	AC-14	AC-14
AC-15	**Withdrawn**	---	---	---	---

Industry

ISO/IEC 27001:2005, Information Technology – Security Techniques – Security Management System – Requirements

CONTROL CATEGORY	SUB-CATEGORY OF CONTROLS
Security Policy	Information security policy
Organization of Information Security	Internal organization; External parties
Asset Management	Responsibility for assets; Information classification
Human Resource Security	Prior to employment; During employment; Termination or change of employment
Physical and Environmental Security	Secure areas; Equipment security
Communications and Operations Management	Operational procedures and responsibilities; Third party service delivery management; System planning and acceptance; Protection against malicious and mobile code; Back-up; Network security management; Media handling; Exchange of information; Electronic commerce services; Monitoring
Access Control	Business requirement for access control; User access management; User responsibilities; Network access control; Operating system access control; Application and information access control; Mobile computing and teleworking
Information Systems Acquisition, Development, and Maintenance	Security requirements of information systems; Correct processing in applications; Cryptographic controls; Security of system files; Security in development and support processes; Technical vulnerability management
Information Security Incident Management	Reporting information security events and weaknesses; Management of information security incidents and improvements
Business Continuity Management	Information security aspects of business continuity management
Compliance	Compliance with legal requirements; Compliance with security policies and standards, and technical compliance; Information system audit considerations

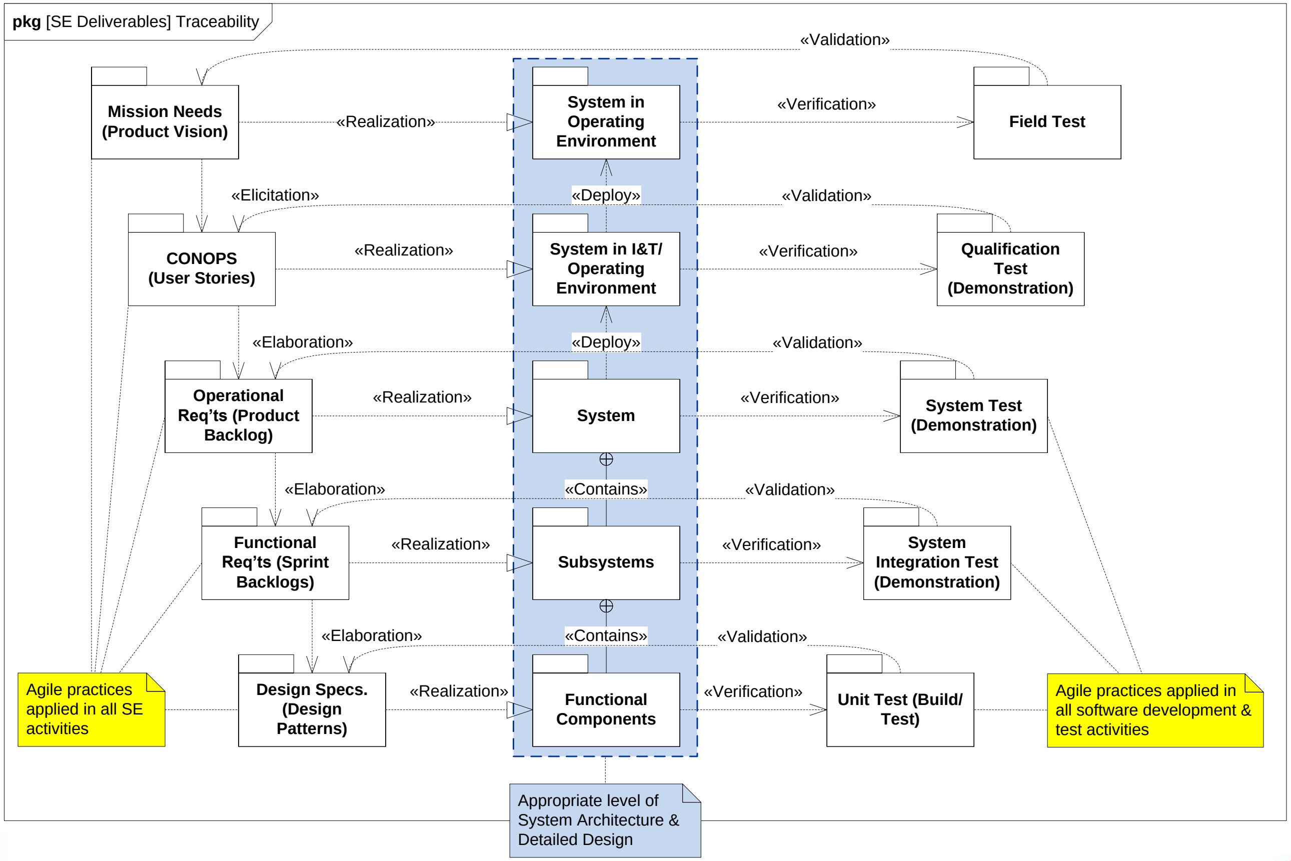
Industry

Payment Card Industry – Data Security Standard (PCI-DSS), *Requirements and Security Assessment Procedures*,

Assessment Procedures	Requirements
Build and Maintain a Secure Network	Req. 1: Install and maintain a firewall configuration to protect cardholder data. Req. 2: Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	Req. 3: Protect stored cardholder data. Req. 4: Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	Req. 5: Use and regularly update anti-virus software or programs. Req. 6: Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	Req. 7: Restrict access to cardholder data by business need to know. Req. 8: Assign a unique ID to each person with computer access. Req. 9: Restrict physical access to cardholder data.
Regular Monitor and Test Network	Req. 10: Track and monitor all access to network resources and cardholder data. Req. 11: Regular test security systems and processes.
Maintain an Information Security Policy	Req. 12: Maintain a policy that addresses information security for all personnel.

Everything must be traceable

- **Verification: "The process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase."**
- **Validation: "Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled."**



pkg [SE Deliverables] Traceability

Mission Needs (Product Vision) «Realization» **System in Operating Environment** «Verification» **Field Test**

«Validation»

«Elicitation»

«Deploy»

CONOPS (User Stories) «Realization» **System in I&T/ Operating Environment** «Verification» **Qualification Test (Demonstration)**

«Validation»

«Elaboration»

«Deploy»

Operational Req'ts (Product Backlog) «Realization» **System** «Verification» **System Test (Demonstration)**

«Validation»

«Elaboration»

«Contains»

Functional Req'ts (Sprint Backlogs) «Realization» **Subsystems** «Verification» **System Integration Test (Demonstration)**

«Validation»

«Elaboration»

«Contains»

Design Specs. (Design Patterns) «Realization» **Functional Components** «Verification» **Unit Test (Build/ Test)**

«Validation»

Agile practices applied in all SE activities

Agile practices applied in all software development & test activities

Appropriate level of System Architecture & Detailed Design

Reference: ISO/IEC/IEEE 24765:2010, *Systems and Software Engineering - Vocabulary*, 1st Ed. December 15, 2010.

Test outputs (e.g. automated, manual)

Reference: Youki Kadobayashi, NICT Japan

Capacity building with ITU-T cybersecurity standards

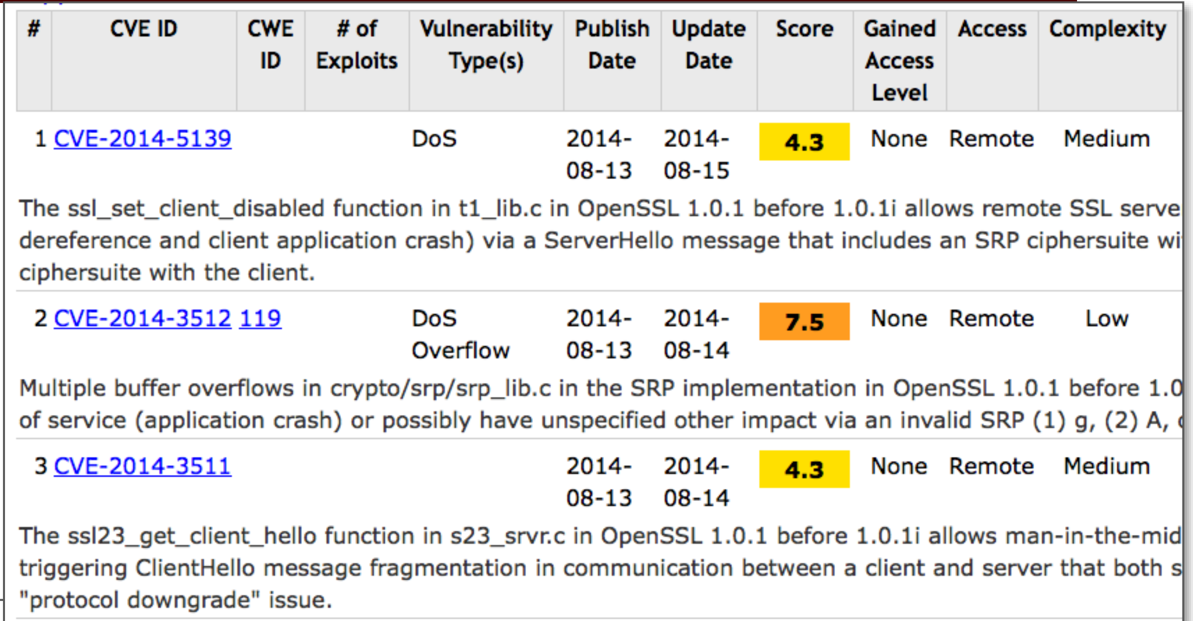
- Existing process-oriented standards, as well as checklist standards, should be complemented with detailed knowledge-base of cybersecurity, because:
  - Cyber-risks are highly volatile
  - Chain reactions are typical – difficult to estimate the risk without considering technical detail
  - You’ll need to communicate the detail
- ITU-T provides knowledge-base standards

Knowledge base of vulnerabilities

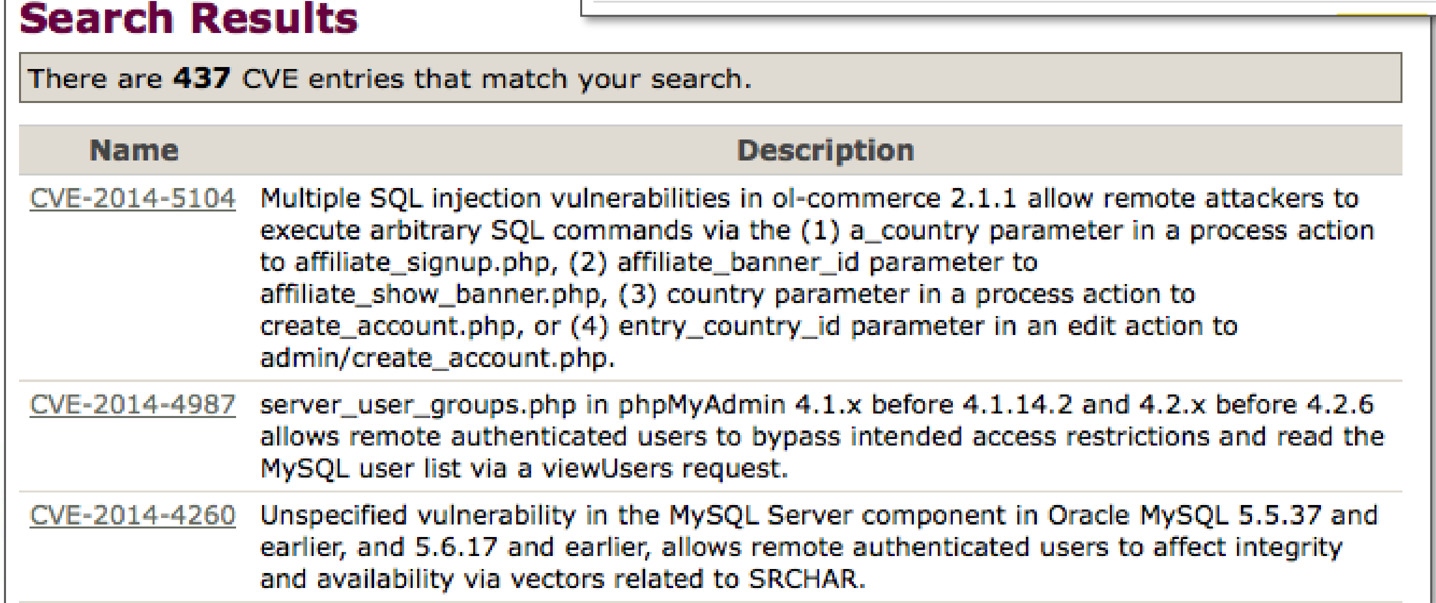
- **CVE: Common Vulnerability Enumeration**
  - A structured means to exchange information on security vulnerabilities and exposures and provides a common identifier for publicly-known problems.
  - http://cve.mitre.org/
  - Standardized as ITU-T Recommendation X.1520
  - National databases:
    - U.S. NIST NVD
    - Japan JVN
  - R. Martin, "Managing Vulnerabilities in Networked Systems", IEEE Computer, 34(11), Nov 2001.

Example: vulnerabilities of widely used software for data protection purposes

CVE entries for OpenSSL



#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity
1	CVE-2014-5139			DoS	2014-08-13	2014-08-15	4.3	None	Remote	Medium
	The ssl_set_client_disabled function in t1_lib.c in OpenSSL 1.0.1 before 1.0.1i allows remote SSL serve dereference and client application crash) via a ServerHello message that includes an SRP ciphersuite wi ciphersuite with the client.									
2	CVE-2014-3512	119		DoS Overflow	2014-08-13	2014-08-14	7.5	None	Remote	Low
	Multiple buffer overflows in crypto/srp/srp_lib.c in the SRP implementation in OpenSSL 1.0.1 before 1.0 of service (application crash) or possibly have unspecified other impact via an invalid SRP (1) g, (2) A,									
3	CVE-2014-3511				2014-08-13	2014-08-14	4.3	None	Remote	Medium
	The ssl23_get_client_hello function in s23_srvr.c in OpenSSL 1.0.1 before 1.0.1i allows man-in-the-mid triggering ClientHello message fragmentation in communication between a client and server that both s "protocol downgrade" issue.									



Search Results

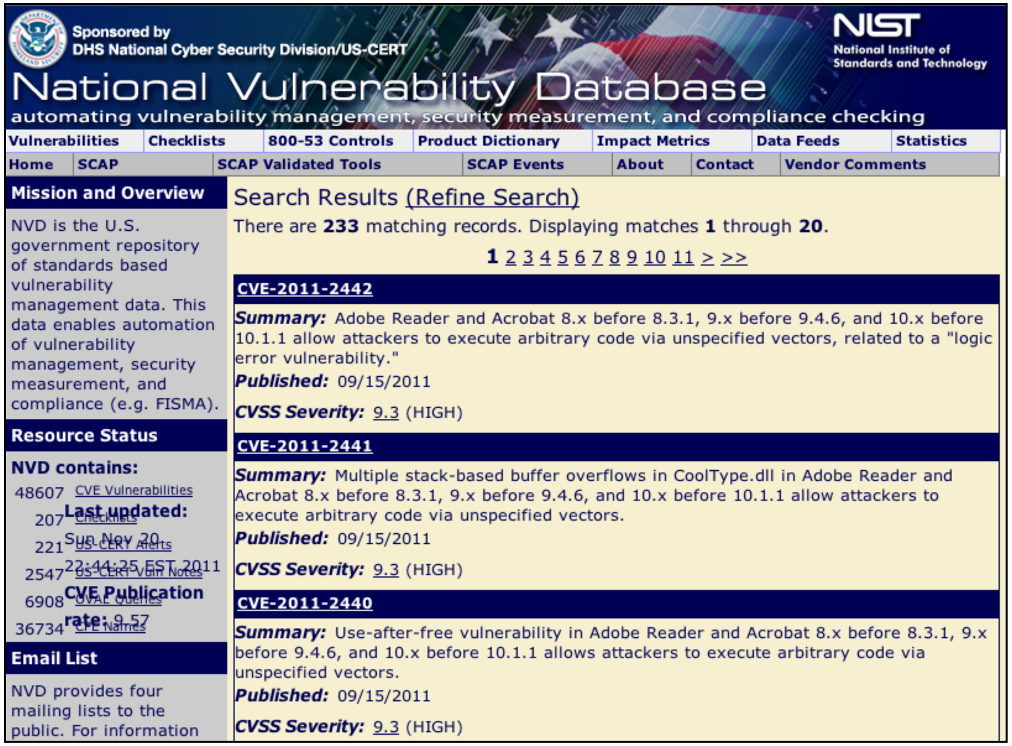
There are **437** CVE entries that match your search.

Name	Description
CVE-2014-5104	Multiple SQL injection vulnerabilities in ol-commerce 2.1.1 allow remote attackers to execute arbitrary SQL commands via the (1) a_country parameter in a process action to affiliate_signup.php, (2) affiliate_banner_id parameter to affiliate_show_banner.php, (3) country parameter in a process action to create_account.php, or (4) entry_country_id parameter in an edit action to admin/create_account.php.
CVE-2014-4987	server_user_groups.php in phpMyAdmin 4.1.x before 4.1.14.2 and 4.2.x before 4.2.6 allows remote authenticated users to bypass intended access restrictions and read the MySQL user list via a viewUsers request.
CVE-2014-4260	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.37 and earlier, and 5.6.17 and earlier, allows remote authenticated users to affect integrity and availability via vectors related to SRCHAR.

CVE entries for MySQL

Ongoing Proliferation of CVE

- **143 CVE-compatible products and services**



Sponsored by
DHS National Cyber Security Division/US-CERT
NIST
National Institute of Standards and Technology
National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking
Vulnerabilities | Checklists | 800-53 Controls | Product Dictionary | Impact Metrics | Data Feeds | Statistics
Home | SCAP | SCAP Validated Tools | SCAP Events | About | Contact | Vendor Comments

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

48607	CVE Vulnerabilities
207	Checklists
221	US-CERT Alerts
2547	US-CERT Vuln Notes
6908	OVAL Queries
36734	CPE Names

Last updated: Sun Nov 20 22:44:25 EST 2011

CVE Publication rate: 9.57

Email List

NVD provides four mailing lists to the public. For information

Search Results (Refine Search)

There are **233** matching records. Displaying matches **1** through **20**.

1 2 3 4 5 6 7 8 9 10 11 > >>

CVE-2011-2442

Summary: Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allow attackers to execute arbitrary code via unspecified vectors, related to a "logic error vulnerability."

Published: 09/15/2011

CVSS Severity: 9.3 (HIGH)

CVE-2011-2441

Summary: Multiple stack-based buffer overflows in CoolType.dll in Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allow attackers to execute arbitrary code via unspecified vectors.

Published: 09/15/2011

CVSS Severity: 9.3 (HIGH)

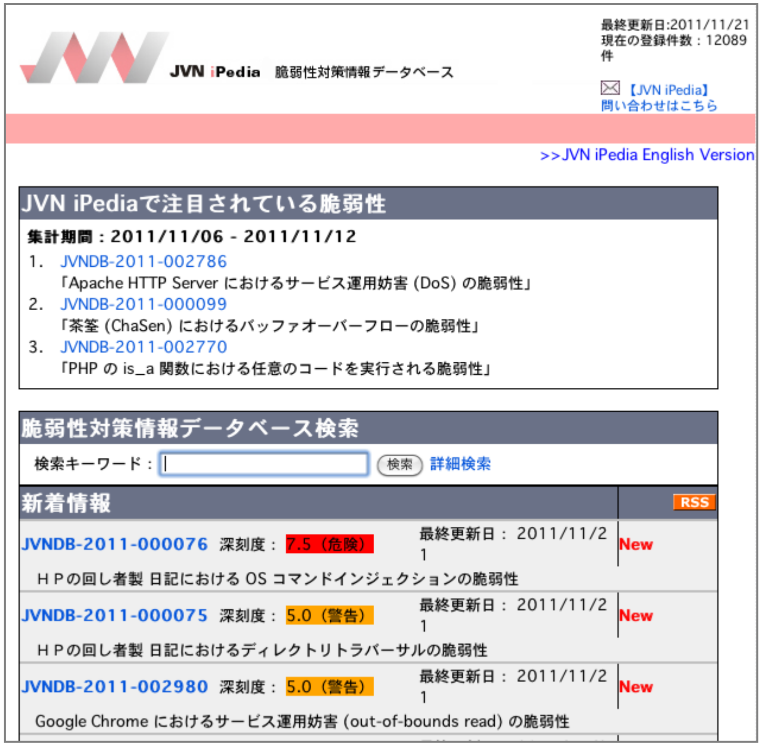
CVE-2011-2440

Summary: Use-after-free vulnerability in Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allows attackers to execute arbitrary code via unspecified vectors.

Published: 09/15/2011

CVSS Severity: 9.3 (HIGH)

U.S. NIST NVD



JVN iPedia 脆弱性対策情報データベース
【JVN iPedia】
問い合わせはこちら
>>JVN iPedia English Version

最終更新日:2011/11/21
現在の登録件数：12089件

JVN iPediaで注目されている脆弱性

集計期間：2011/11/06 - 2011/11/12

1. JVNDB-2011-002786
「Apache HTTP Server におけるサービス運用妨害 (DoS) の脆弱性」
2. JVNDB-2011-000099
「茶筌 (ChaSen) におけるバッファオーバーフローの脆弱性」
3. JVNDB-2011-002770
「PHP の is_a 関数における任意のコードを実行される脆弱性」

脆弱性対策情報データベース検索

検索キーワード：

新着情報

JVNDB-2011-000076 深刻度：7.5（危険） 最終更新日：2011/11/21 New
ＨＰの回し者製 日記における OS コマンドインジェクションの脆弱性

JVNDB-2011-000075 深刻度：5.0（警告） 最終更新日：2011/11/21 New
ＨＰの回し者製 日記におけるディレクトリトラバーサルの脆弱性

JVNDB-2011-002980 深刻度：5.0（警告） 最終更新日：2011/11/21 New
Google Chrome におけるサービス運用妨害 (out-of-bounds read) の脆弱性

Japan IPA JVN

CPE: common naming of IT assets

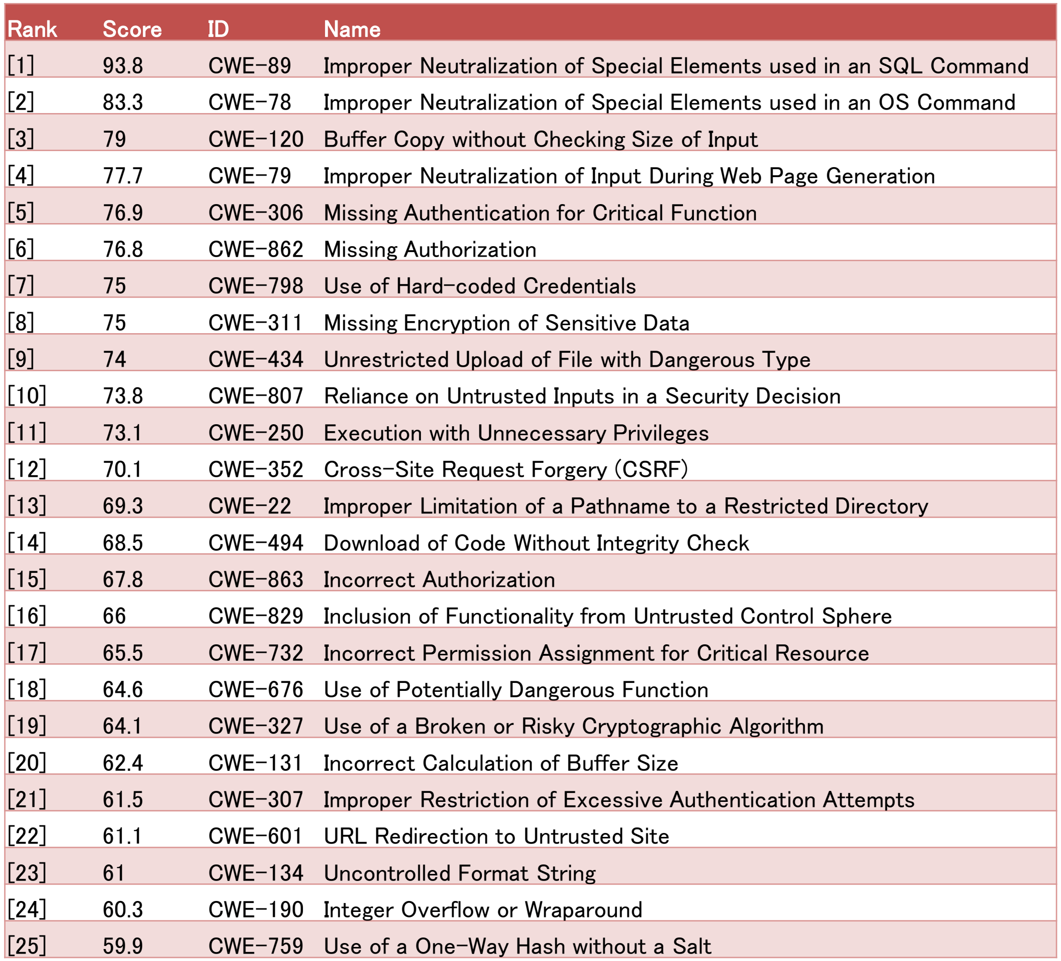
- CPE: Common Platform Enumeration
  - A structured method of describing and identifying classes of applications, operating systems, and hardware devices present among an enterprise's computing assets.
- URI for IT assets, primarily software
- Standardized as ITU-T Recommendation X.1528
  - `cpe:/o:microsoft:windows_2003`
  - `cpe:/a:adobe:reader:8.1`

Taxonomy of vulnerabilities

- **CWE: Common Weakness Enumeration**
  - **Group same kind of vulnerabilities into a weakness, and give it a distinct number**
  - **Provides common names for publicly known problems in the commercial or open source software**
  - **Intended for security tools and services that can find weaknesses in source code and operational systems**
  - **Helps better understand and manage software weaknesses related to architecture and design**
  - **http://cwe.mitre.org/**
  - **Standardized as ITU-T Recommendation X.1524**

CWE top 25
http://cwe.mitre.org/top25/

- **Prioritized list of dangerous software errors**
  - **Intended to minimize software vulnerability and data breach**
  - **Any software for data protection needs serious consideration of these failure modes, among others**
  - **Useful for:**
    - **Procurement**
    - **Development, etc.**

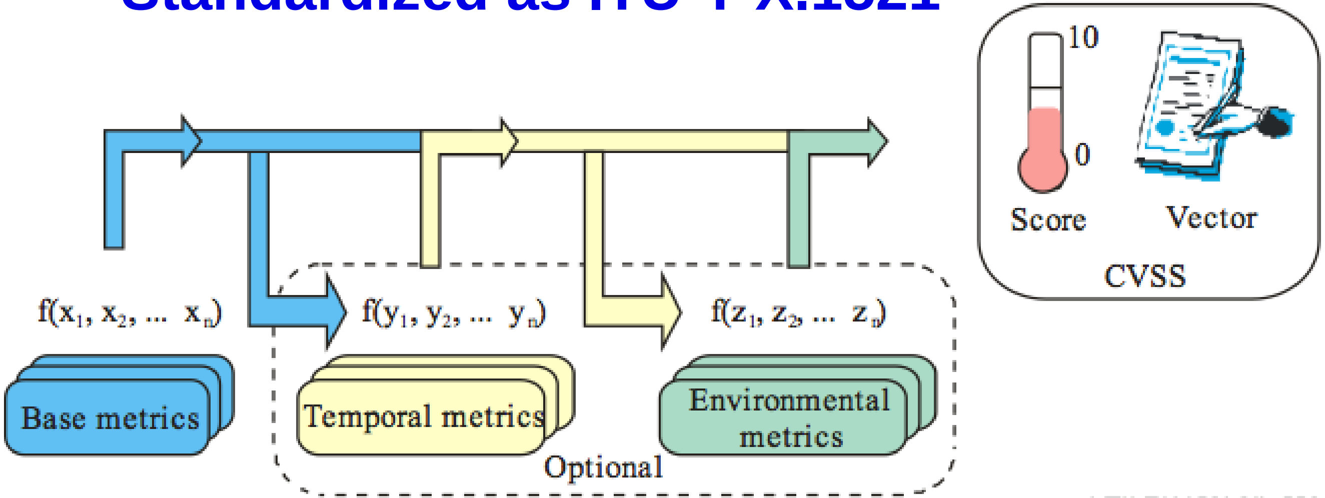


Rank	Score	ID	Name
[1]	93.8	CWE-89	Improper Neutralization of Special Elements used in an SQL Command
[2]	83.3	CWE-78	Improper Neutralization of Special Elements used in an OS Command
[3]	79	CWE-120	Buffer Copy without Checking Size of Input
[4]	77.7	CWE-79	Improper Neutralization of Input During Web Page Generation
[5]	76.9	CWE-306	Missing Authentication for Critical Function
[6]	76.8	CWE-862	Missing Authorization
[7]	75	CWE-798	Use of Hard-coded Credentials
[8]	75	CWE-311	Missing Encryption of Sensitive Data
[9]	74	CWE-434	Unrestricted Upload of File with Dangerous Type
[10]	73.8	CWE-807	Reliance on Untrusted Inputs in a Security Decision
[11]	73.1	CWE-250	Execution with Unnecessary Privileges
[12]	70.1	CWE-352	Cross-Site Request Forgery (CSRF)
[13]	69.3	CWE-22	Improper Limitation of a Pathname to a Restricted Directory
[14]	68.5	CWE-494	Download of Code Without Integrity Check
[15]	67.8	CWE-863	Incorrect Authorization
[16]	66	CWE-829	Inclusion of Functionality from Untrusted Control Sphere
[17]	65.5	CWE-732	Incorrect Permission Assignment for Critical Resource
[18]	64.6	CWE-676	Use of Potentially Dangerous Function
[19]	64.1	CWE-327	Use of a Broken or Risky Cryptographic Algorithm
[20]	62.4	CWE-131	Incorrect Calculation of Buffer Size
[21]	61.5	CWE-307	Improper Restriction of Excessive Authentication Attempts
[22]	61.1	CWE-601	URL Redirection to Untrusted Site
[23]	61	CWE-134	Uncontrolled Format String
[24]	60.3	CWE-190	Integer Overflow or Wraparound
[25]	59.9	CWE-759	Use of a One-Way Hash without a Salt

Quantification of vulnerabilities

facilitates prioritization during vulnerability management

- CVSS: common vulnerability scoring system
  - Base metrics: constant over time and across user environments
  - Temporal metrics: reflects vulnerability landscape
  - Environmental metrics: reflects user environments
  - http://www.first.org/cvss/
  - Standardized as ITU-T X.1521



proposed ITU-T X.1521 (11)_F02

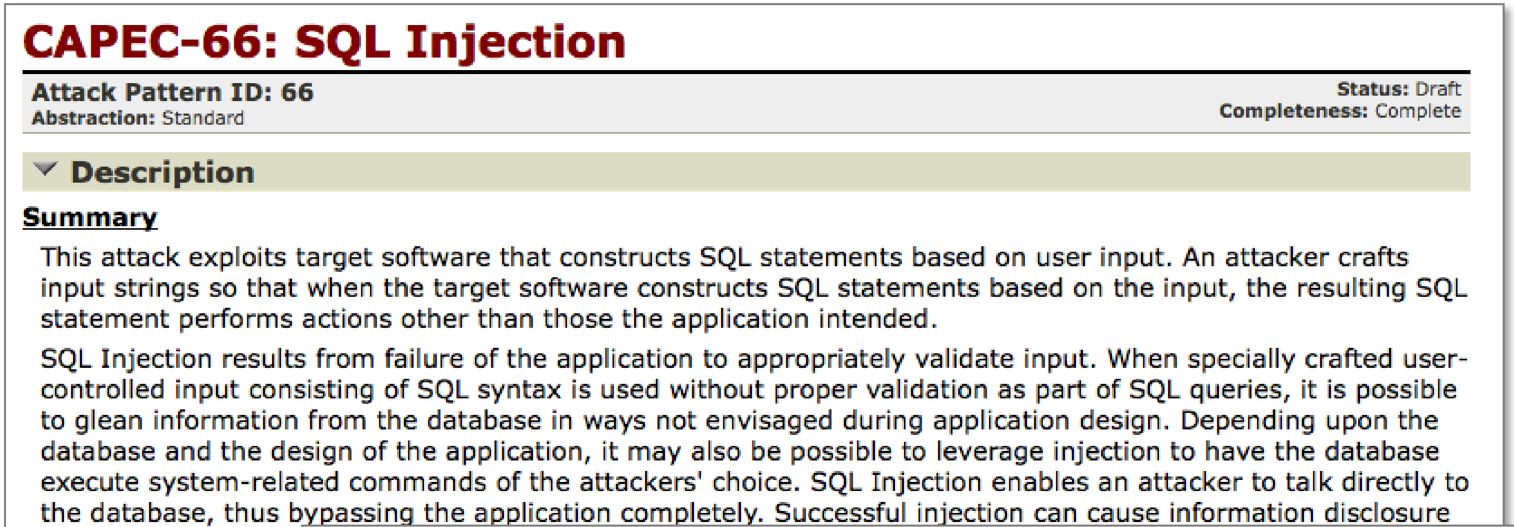
Knowledge base of attack patterns

- **CAPEC: Common Attack Pattern Enumeration and Classification**
  - **Dictionary of attack patterns, solutions & mitigations**
  - **Facilitates communication of incidents, issues, as well as validation techniques and mitigation strategies**

  - **http://capec.mitre.org/**
  - **Standardized as ITU-T Recommendation X.1544**

CAPEC example: SQL injection

Summary, how it works, solutions and mitigations



CAPEC-66: SQL Injection

Attack Pattern ID: 66
Abstraction: Standard

Status: Draft
Completeness: Complete

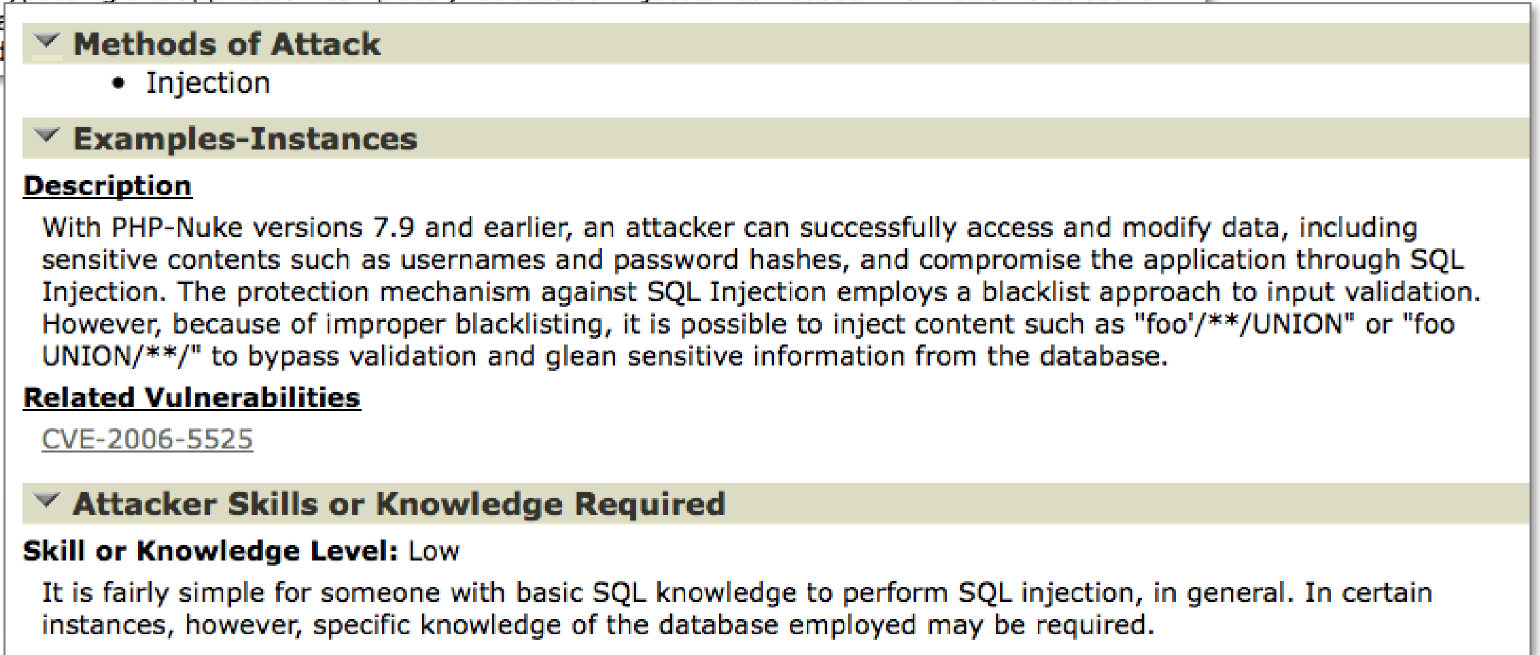
Description

Summary

This attack exploits target software that constructs SQL statements based on user input. An attacker crafts input strings so that when the target software constructs SQL statements based on the input, the resulting SQL statement performs actions other than those the application intended.

SQL Injection results from failure of the application to appropriately validate input. When specially crafted user-controlled input consisting of SQL syntax is used without proper validation as part of SQL queries, it is possible to glean information from the database in ways not envisaged during application design. Depending upon the database and the design of the application, it may also be possible to leverage injection to have the database execute system-related commands of the attackers' choice. SQL Injection enables an attacker to talk directly to the database, thus bypassing the application completely. Successful injection can cause information disclosure as well as ability to a

information from a d



Methods of Attack

- Injection

Examples-Instances

Description

With PHP-Nuke versions 7.9 and earlier, an attacker can successfully access and modify data, including sensitive contents such as usernames and password hashes, and compromise the application through SQL Injection. The protection mechanism against SQL Injection employs a blacklist approach to input validation. However, because of improper blacklisting, it is possible to inject content such as "foo'/**/UNION" or "foo UNION/**/" to bypass validation and glean sensitive information from the database.

Related Vulnerabilities

CVE-2006-5525

Attacker Skills or Knowledge Required

Skill or Knowledge Level: Low

It is fairly simple for someone with basic SQL knowledge to perform SQL injection, in general. In certain instances, however, specific knowledge of the database employed may be required.

Vulnerability assessment

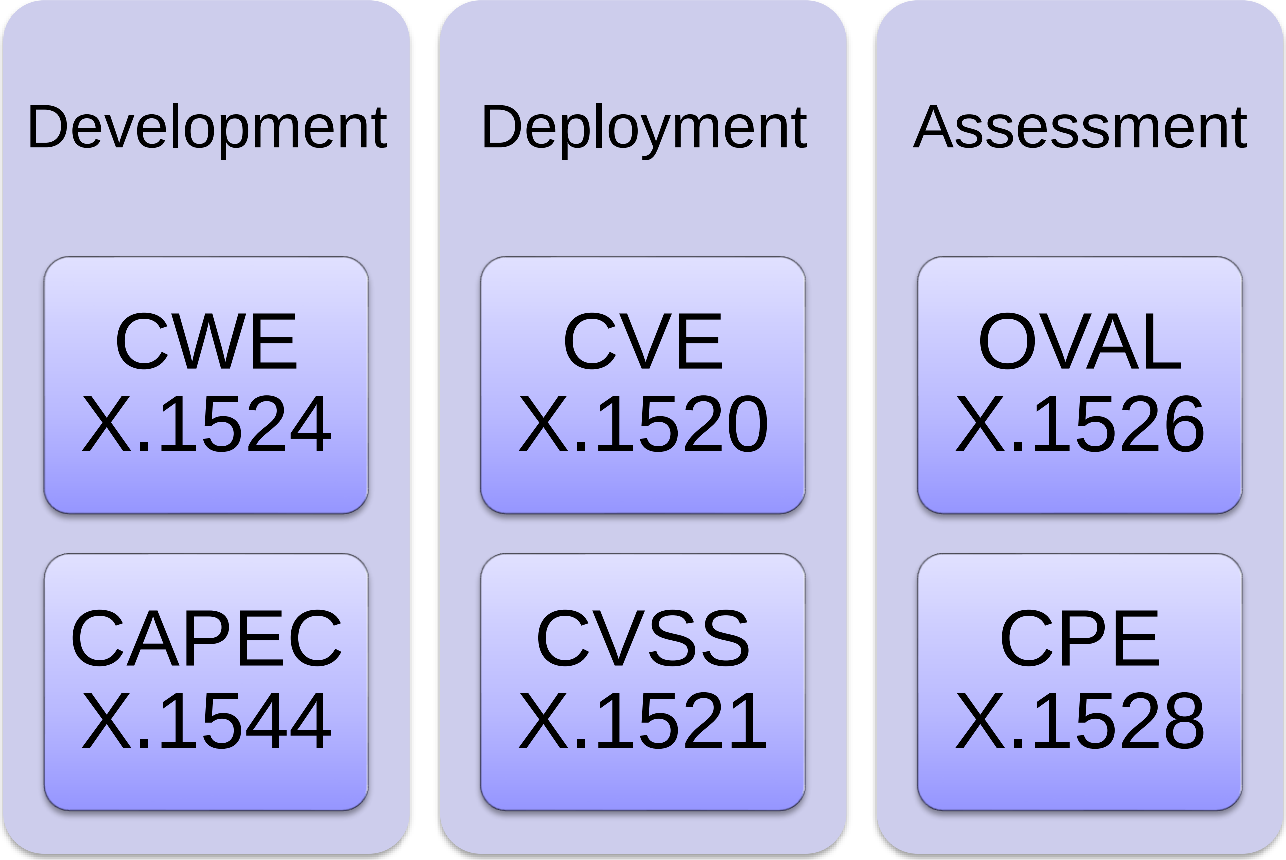
- **OVAL: Language for the open definition of vulnerabilities and for the assessment of a system state**
  - A standard for assessment and reporting of machine state of computer systems.
  - OVAL includes a language to encode system details, and an assortment of content repositories held throughout the community.

  - http://oval.mitre.org/
  - Standardized as ITU-T Recommendation X.1526

Major ITU-T standards for cybersecurity
Definitions, knowledge base standards

- X.1205, Overview of Cybersecurity
- X.1251, A framework for user control of digital identity
- X.1252, Baseline identity management terms and definitions
- X.1254, Entity authentication assurance framework
- X.1500, Overview of cybersecurity information exchange
- X.1520, Common vulnerabilities and exposures
- X.1521, Common vulnerability scoring system
- X.1524, Common weakness enumeration
- X.1526, Language for the open definition of vulnerabilities and for the assessment of a system state
- X.1528, Common platform enumeration
- X.1544, Common attack pattern enumeration and classification
- X.1546, Malware attribute enumeration and characterization

Improving cybersecurity and data protection throughout IT infrastructure lifecycle



Knowledge bases, compatible products, informed communities and ITU-T Recommendations are already helping diverse organizations to protect their IT infrastructures and customers

Section Summary

- ITU-T cybersecurity standards provide critical instruments to deal with rapidly changing and diversifying cybersecurity phenomena, directly contributing to data protection

- Enumeration standards provides effective means of communication across businesses, government agencies as well as communities

- Cyber-risks are highly volatile and manifests through unexpected combination of components, that requires careful examination of technical risks through knowledge-base standards

Security architecture vulnerabilities

Dr. Drew Hamilton

Reference: Kirk A. Burns, SHSU

Definition and Key Concepts

- Architecture
  - High-level perspective of how business requirements are to be structured and aligned with technology and processes
- Framework
  - Defined approach to the process used to achieve the goals of an architecture, based on policy
- Infrastructure
  - Integrated building blocks that support the goals of the architecture
- Model
  - Outlines how security is to be implemented within the organization

Definition and Key Concepts

- Good security architecture
  - Strategic
    - Provides a long-range perspective that is less subject to tactical changes in technology
  - Business requirements based
    - Understand business and security and design a system that meets those requirements
  - Holistic
    - Understanding all the parts of the business and interconnecting them
  - Design
    - Blueprint
      - Integration and development of technology infrastructure into the business process
    - Multiple implementations
      - Flexibility due to location and business constraints

Definition and Key Concepts

- **Benefits of a good security architecture**
  - Consistently manage risk
  - Reduce the costs of managing risk
  - Accurate security-related decisions
  - Promote interoperability, integration, and ease of access
  - Provide a frame of reference (for other organizations interacting with the enterprise)

Architecture Components

- What are the security limitations and benefits of each component?
  - Hardware
  - Firmware
  - Central processing units
  - Input/output devices
  - Software
  - Architectural structures
  - Storage and memory

Separation

- Temporal isolation
  - Accomplished through time limits. Person cannot access an area of the building or an area of the network, or an application outside of certain authorized hours.
- Physical isolation
  - Refers to separating out sensitive areas from common access, such as setting up compartmentalized areas or secure rooms.
- Virtual isolation
  - Protects against malicious activity by not permitting a process to execute outside of a strict set of boundaries.

Privilege Levels

- Identifying, authenticating, and authorizing subjects
- Subjects of higher trust can access more system instructions and operate in privileged mode
- Subjects with lower trust can access a smaller portion of system instructions and operate only in user mode

Process Isolation

- Preserves Object’s integrity and subjects adherence to access controls
- Prevents interaction – prevents objects from interacting with each other and their resources
- Independent states – actions of one object should not affect the state of other objects
- Process isolation method
  - Encapsulation – objects, data, and functions are packaged together
  - Time multiplexing – assignment specific time slots for processing information
  - Naming distinctions – to distinguish between processes
  - Virtual mapping/domains – mapping info objects to virtual locations to ensure applications can find their data

Trusted Computer Base

- Trusted computer base – includes all the components and their operating processes and procedures that ensure that the security policy of the organization is enforced.
  - Hardware
  - Firmware
  - Software
  - Processes
  - Inter-process communications
- Simple and testable

Trusted Computer Base

- **Enforces security policy – must be able to enforce security policy regardless of user input and be protected from interference or tampering**

- **Monitors four basic functions**
  - **Process activation**
  - **Execution domain switching**
  - **Memory protection**
  - **Input/output operations**

Reference Monitors

- **Abstract machine concept – abstract machine that is regulating all access on the system and enforcing security controls**
  - **Must be tamperproof**
  - **Always invoked**
  - **Verifiable**
- **Security kernel**
  - **Components of an OS perform various protection tasks designed to control and monitor system evens and prevent things from occurring that might disrupt normal execution or threaten the stability of the system or any of its resources.**
- **Subject**
  - **Active entity**
- **Object**
  - **Passive entity**

Summary

- Assessment and test strategies
- Security process data (e.g. management and operational controls)
- Security control testing
- Test outputs (e.g. automated, manual)
- Security architecture vulnerabilities