CISSP® Common Body of Knowledge Review

Information Security Governance & Risk Management Domain

Version: 5.10

Topics

Information Security & Risk Management Domain

- ➡ Information Security Concept
- Information Security Governance
- Risk Management
- Personnel Security
- Security Education, Training, and Awareness

Security Objectives

- Confidentiality
  - “Preserving authorized restriction on information access and disclosure, including means for protecting personal privacy and proprietary information.” (44 USC Sec. 3542)

- Integrity
  - “Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.” (44 USC Sec. 3542)

- Availability
  - “Ensuring timely and reliable access and use of information.” (44 USC Sec. 3542)

Security Controls

"Security controls are the management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability of the system and its information."

- What security controls are needed to adequately mitigate the risk incurred by the use of information and information systems in the execution of organizational missions and business functions?
- Have the selected controls or is there a realistic plan for their implementation?
- What is the desired or required level of assurance (i.e., grounds for confidence) that the selected security controls, as implemented are effective in their application?

Reference: NIST SP 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems*.

Categories of Security Controls …(1/2)

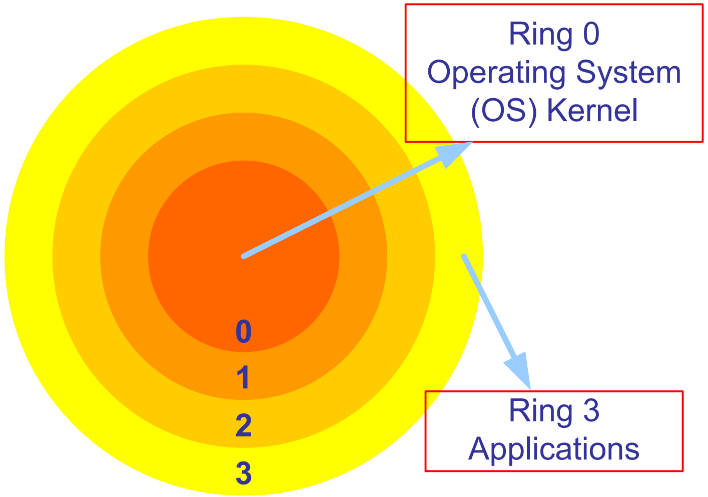
- Management (Administrative) Controls.
  - Policies, Standards, Processes, Procedures, & Guidelines
- Operational (and Physical) Controls.
  - Operational Security (Execution of Policies, Standards & Process, Education & Awareness)
  - Physical Security (Facility or Infrastructure Protection)
- Technical (Logical) Controls.
  - Access Controls, Identification & Authorization, Confidentiality, Integrity, Availability, Non-Repudiation.

Categories of Security Controls …(2/2)

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

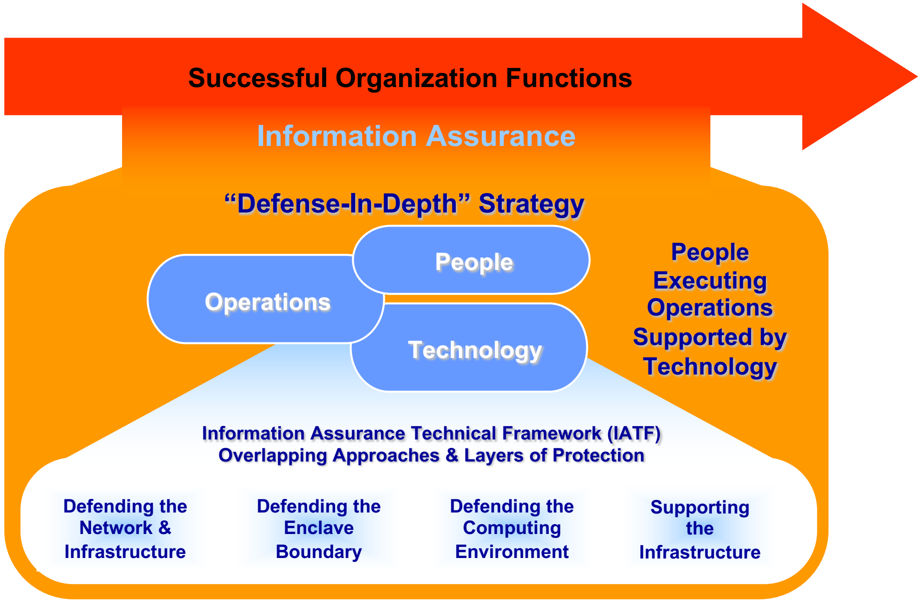
Reference: NIST SP800-53, Rev 3, *Recommended Security Controls for Federal Information Systems*

Defense-in-Depth Model – Rings of Protection



- Ring number determines the access level.
- A program may access only data that resides on the same ring, or a less privileged ring.
- A program may call services residing on the same, or a more privileged ring.
- Ring 0 contains kernel functions of the OS.
- Ring 1 contains the OS.
- Ring 2 contains the OS utilities.
- Ring 3 contains the applications.

Defense-in-Depth Model – Information Security


Successful Organization Functions
Information Assurance
"Defense-In-Depth" Strategy
People
Operations
Technology
People Executing Operations Supported by Technology
Information Assurance Technical Framework (IATF)
Overlapping Approaches & Layers of Protection
Defending the Network & Infrastructure
Defending the Enclave Boundary
Defending the Computing Environment
Supporting the Infrastructure

References

- NSA IA Solution Directions, *Information Assurance Technical Framework*, Release 3.1
- ISO/IEC 27002:2005, *Code of Practice for Information Security Management*

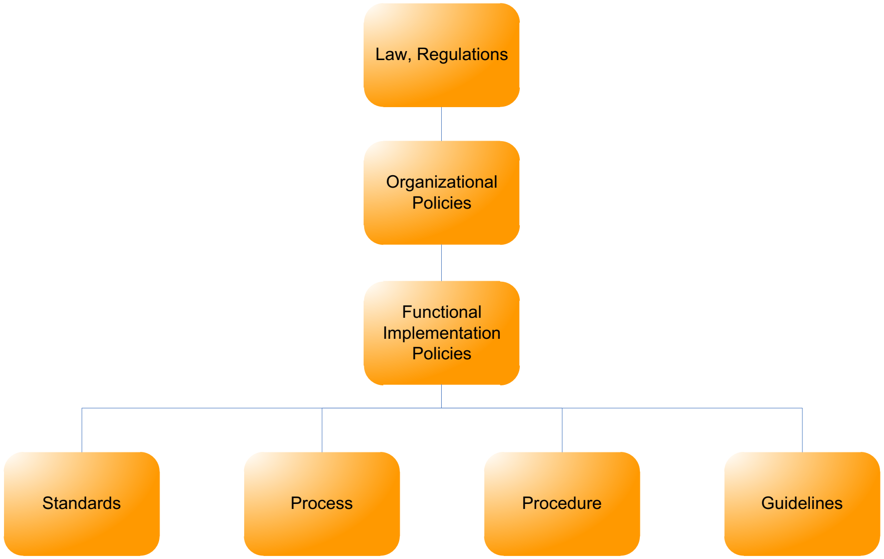
Learning Objectives

Information Security Management Domain

- Information Security Concept
- ➡ Information Security Governance
- Risk Management
- Personnel Security
- Security Education, Training, and Awareness

Information Security Governance

- Policy. Management directives that establish expectations (goals & objectives), and assign roles & responsibilities
- Standards. Functional specific mandatory activities, actions, and rules
- Process & Procedure. Step-by-step implementation instructions
- Guideline. General statement, framework, or recommendations to augment process or procedure



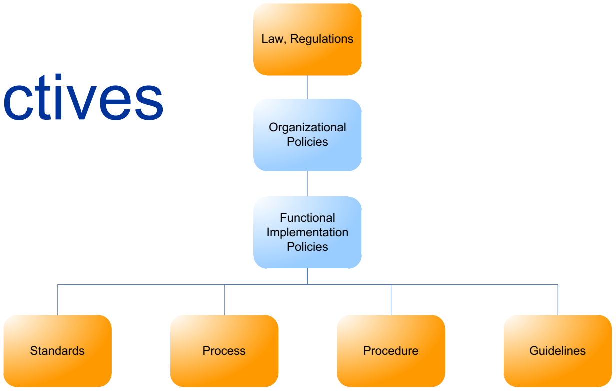
Policies

Policies:

- Explain laws, regulations, business/mission needs, and management expectations (goals & objectives).
- Identify roles and delineate responsibilities.

Examples:

- Executive Orders, Presidential Directives
  - E.O. 13526, PDD-67, HSPD-7, etc.
- Federal (/Civil)
  - OMB Circulars: A-11, A-130, etc.
- Military
  - DoD Directives, Instructions, Manuals, etc.
- Intelligence
  - Director, Central Intelligence Directives (DCID).



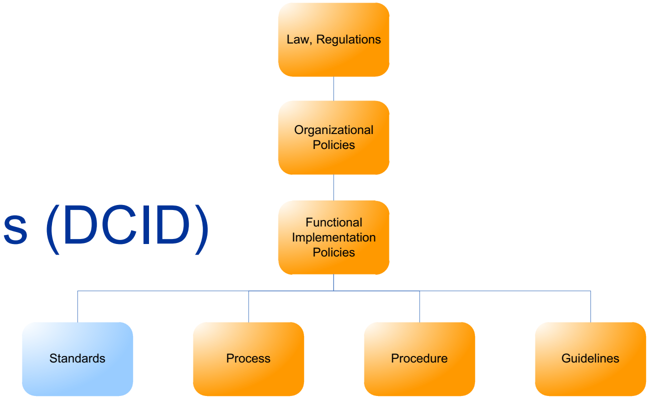
Standards

Standards:

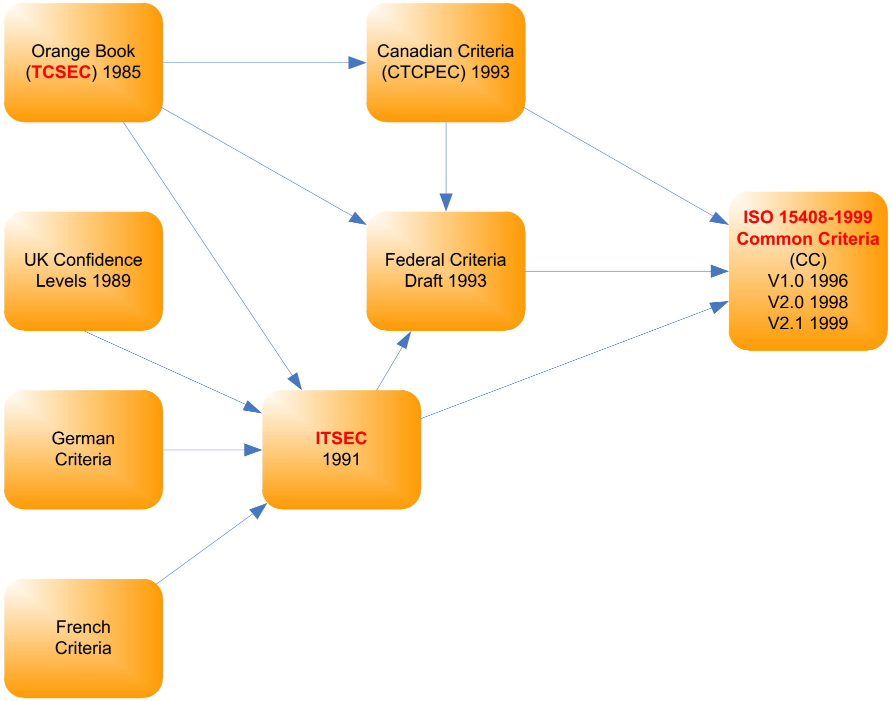
- Mandatory activities, actions, and rules for the execution of management (or administrative) policies

Examples:

- Federal (/ Civil)
  - Federal Information Processing Standards (FIPS)
- Military
  - DoD Regulations, DoD Manuals, etc.
- Intelligence
  - Director, Central Intelligence Directives (DCID)
- Commercial (/ Industry)
  - ISO/IEC 27001, BS 7799, etc.

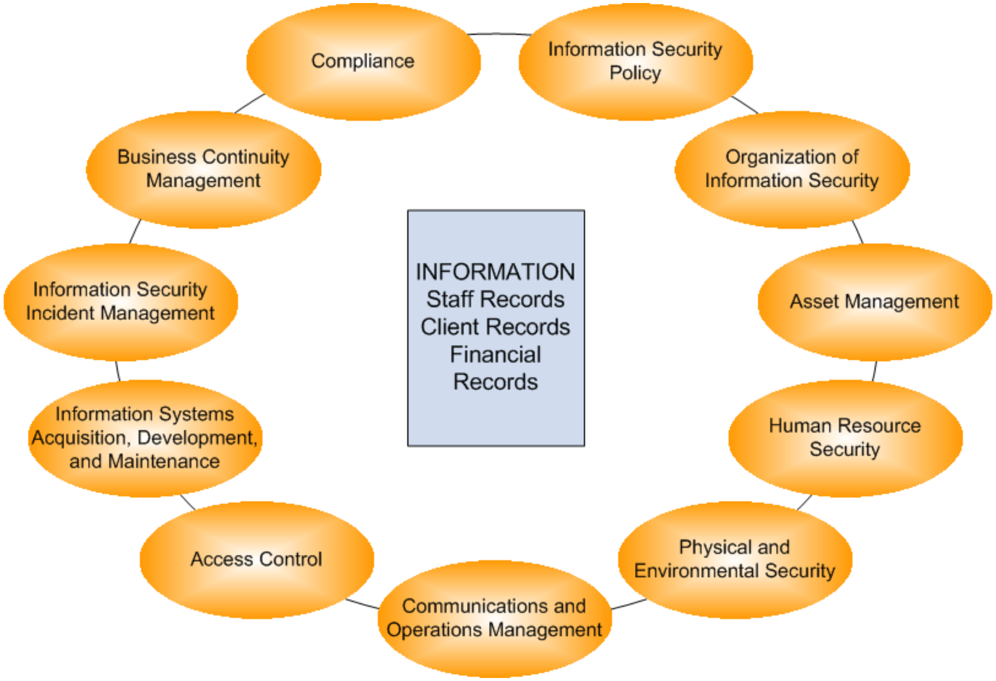


Standards


Orange Book (TCSEC) 1985
Canadian Criteria (CTCPEC) 1993
UK Confidence Levels 1989
Federal Criteria Draft 1993
ISO 15408-1999 Common Criteria (CC) V1.0 1996 V2.0 1998 V2.1 1999
German Criteria
ITSEC 1991
French Criteria

- DoD 5200.28-STD *Trusted Computer System Evaluation Criteria* (TCSEC)
  - Evaluates Confidentiality.
- Information Technology Security Evaluation Criteria (ITSEC)
  - Evaluates Confidentiality, Integrity and Availability.
- Common Criteria (CC)
  - Provided a common structure and language.
  - It's an International standard (ISO 15408).

Standards – ISO/IEC 27001:2005


Compliance
Information Security Policy
Business Continuity Management
Organization of Information Security
Information Security Incident Management
INFORMATION
Staff Records
Client Records
Financial Records
Asset Management
Information Systems Acquisition, Development, and Maintenance
Human Resource Security
Access Control
Physical and Environmental Security
Communications and Operations Management

- ISO/IEC 27001 is an Information Security Management System Standard.
- Commercially, the systems are certified based on meeting ISO/IEC 27001 (not ISO/IEC 27002!)
- ISO/IEC 27002:2005 is a “Code of practice” for information security management

Reference:
ISO/IEC 27001:2005, *Information Security Management Systems - Requirements*, 2005.
ISO/IEC 27002:2005, *Code of Practice for Information Security Management*, 2005.

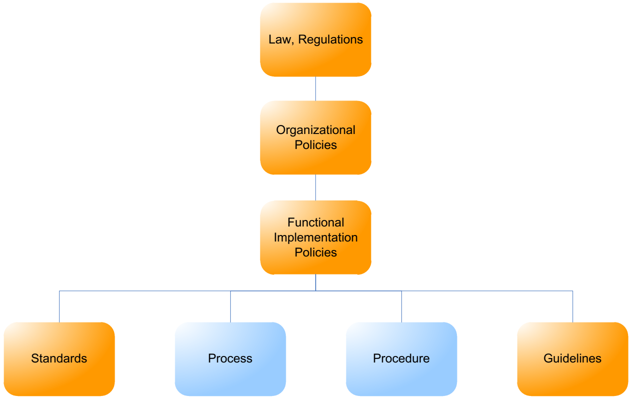
Process & Procedure

Process & Procedure:

- Step-by-step explanation of how to implement or execute security instructions.

Examples:

- System Development Life Cycle (SDLC) System & Services Acquisition Process
  - Project Planning and Management Process
  - Change Control Process
  - Risk Management Process
  - Certification & Accreditation Process
- Standard Operations Procedure (SOP)
- Incident Management Process
- Contingency Planning Process
- Security Assessment Process



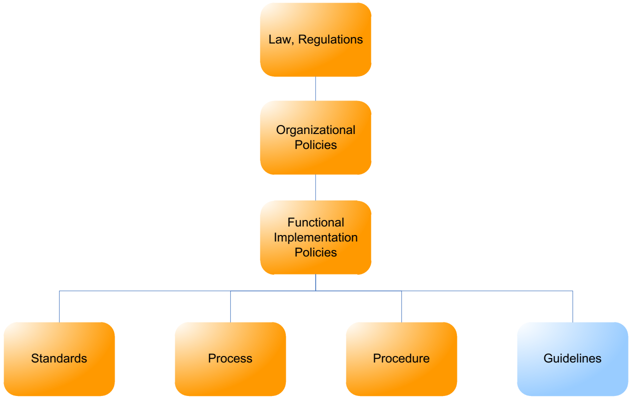
Guidelines

Guidelines:

- Frameworks or recommendations that facilitate implementation of policies, standards, processes, and procedures.

Examples:

- Federal (/ Civil)
  - NIST Special Publications (NIST SP 800 series).
- Military
  - NSA-IATF, NSA-IAM, NSA-IEM.
  - NSA SNAC SCGs, DISA FSO STIGs.
- Commercial
  - ISO/IEC 17799: 2005.
  - CIS Benchmarks.



Learning Objectives

Information Security Management Domain

- Information Security Concepts
- Information Security Governance
- ➡ Risk Management
- Personnel Security
- Security Education, Training, and Awareness

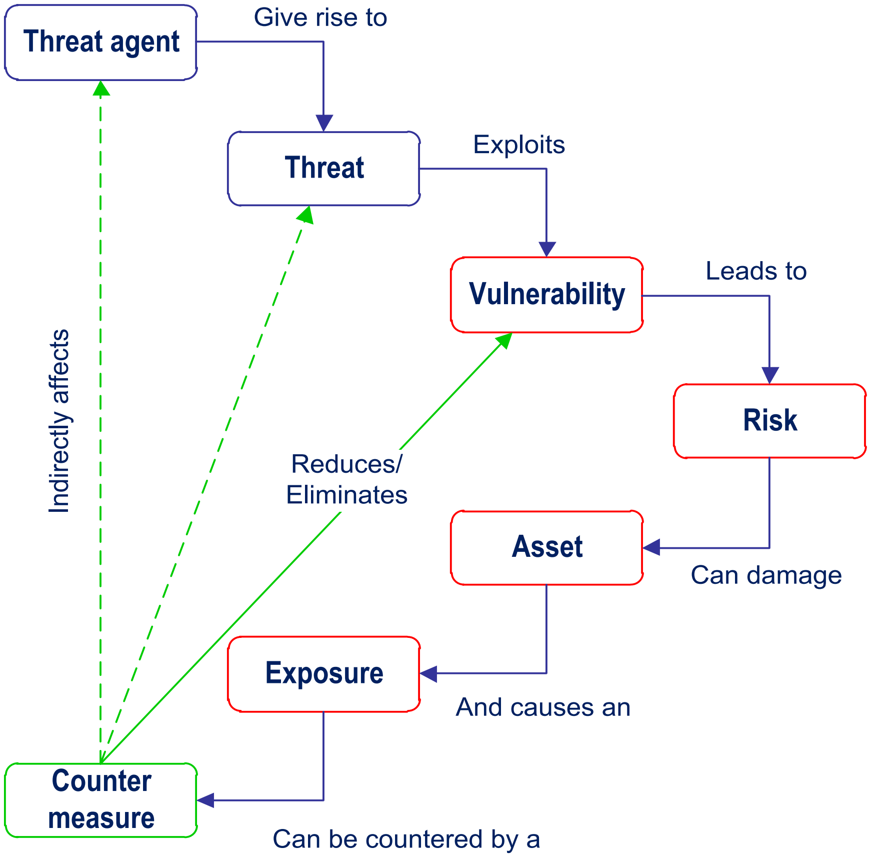
What is a Risk?

- Risk is the relationship between the likelihood of a loss and the potential impact to the business (/ mission).

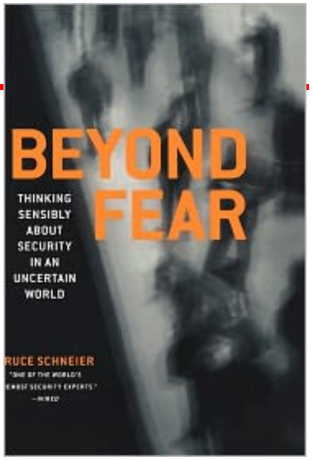
- For information security, risk is defined as:
  - The likelihood of a threat agent (a threat) exploiting vulnerabilities in a “system” (/ system of systems), where “system” = people + process + technology; and
  - The potential impact of a successful attack to an organization’s information operations.

Relationship between Threat, Risk, and Countermeasure

- Threat Agent. An entity that may act on a vulnerability.
- Threat. Any potential danger to information life cycle.
- Vulnerability. A weakness or flaw that may provide an opportunity for a threat agent.
- Risk. The likelihood of a threat agent exploits a discovered vulnerability.
- Exposure. An instance of being compromised by a threat agent.
- Countermeasure / safeguard. An administrative, operational, or logical mitigation against potential risk(s).



“All Security Involves Trade-offs”



- Step 1: What assets are you trying to protect?
- Step 2: What are the risks to these assets?
- Step 3: How well does the security solution mitigate those risks?
- Step 4: What other risks does the security solution cause?
- Step 5: What cost and trade-offs does the security solution impose?

Reference:

- *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*, Bruce Schneier, Springer, 2003.
- *The Black Swan: The Impact of the Highly Improbable*, Nassim Nicholas Taleb, Random House, 2007.

Risk Management

Current State of Insecurity in Federal Agencies

- “The 25 major agencies of Federal government continue to improve information security performance relative to C&A (Certification and Accreditation) rate and testing of contingency plans and security

% of System with a:	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009
Certification and Accreditation (C&A)	85%	88%	92%	96%	**95%**
Tested Contingency Plan	61%	77%	86%	92%	**86%**
Tested Security Controls	72%	88%	95%	93%	**90%**
Total Systems Reported	10,289	10,595	10,304	10,679	12,930

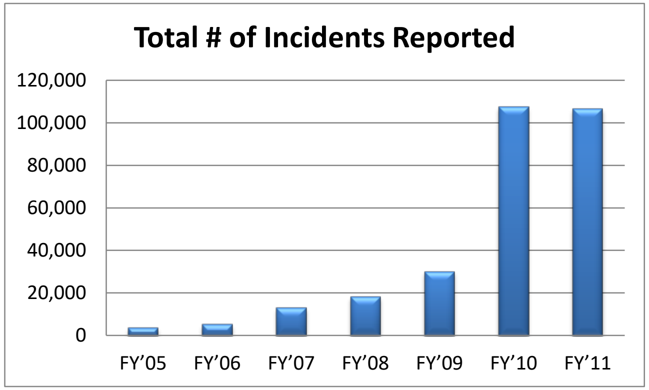
Incident Categories	FY 2005	FY 2006	FY 2007	FY2008	FY2009
1. Unauthorized Access	304	706	2,321	3,214	**4,848**
2. Denial of Service	31	37	36	26	48
3. Malicious Code	1,806	1,465	1,607	2,274	**6,977**
4. Improper Usage	370	638	3,305	3,762	**6,148**
5. Scans/Probes/Attempted Access	976	1,388	1,661	1,272	1,152
6. Under Investigation	82	912	4,056	7,502	**10,826**
Total Incidents Reported	3,569	5,146	12,986	18,050	29,999

* **Source:** OMB and US-CERT

C&A ≠ Risk Management

– For FY08, OMB reported 93% of federal information systems had their security controls tested.

– Yet, between FY05 and FY09, the total number of reported security incidents had increased by over 740%.**



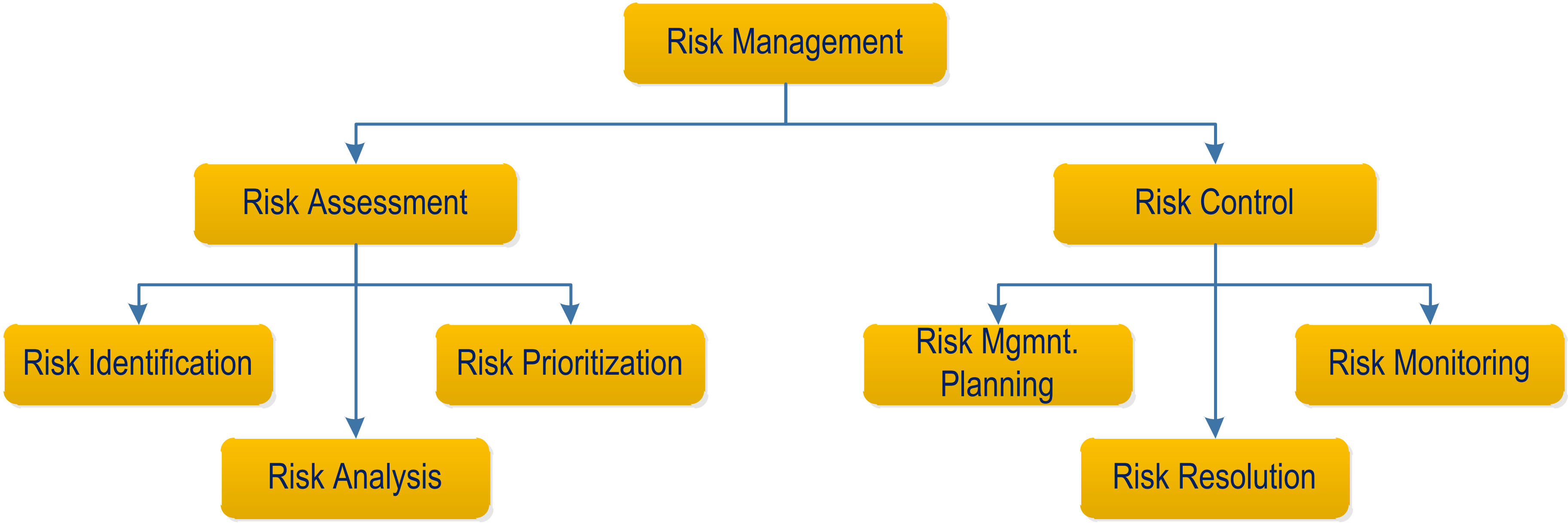
Source:

* Congressional hearing: *More Security, Less What Makes Sense for our Federal Cyber Defense*, October 29, 2009.

** US-CERT

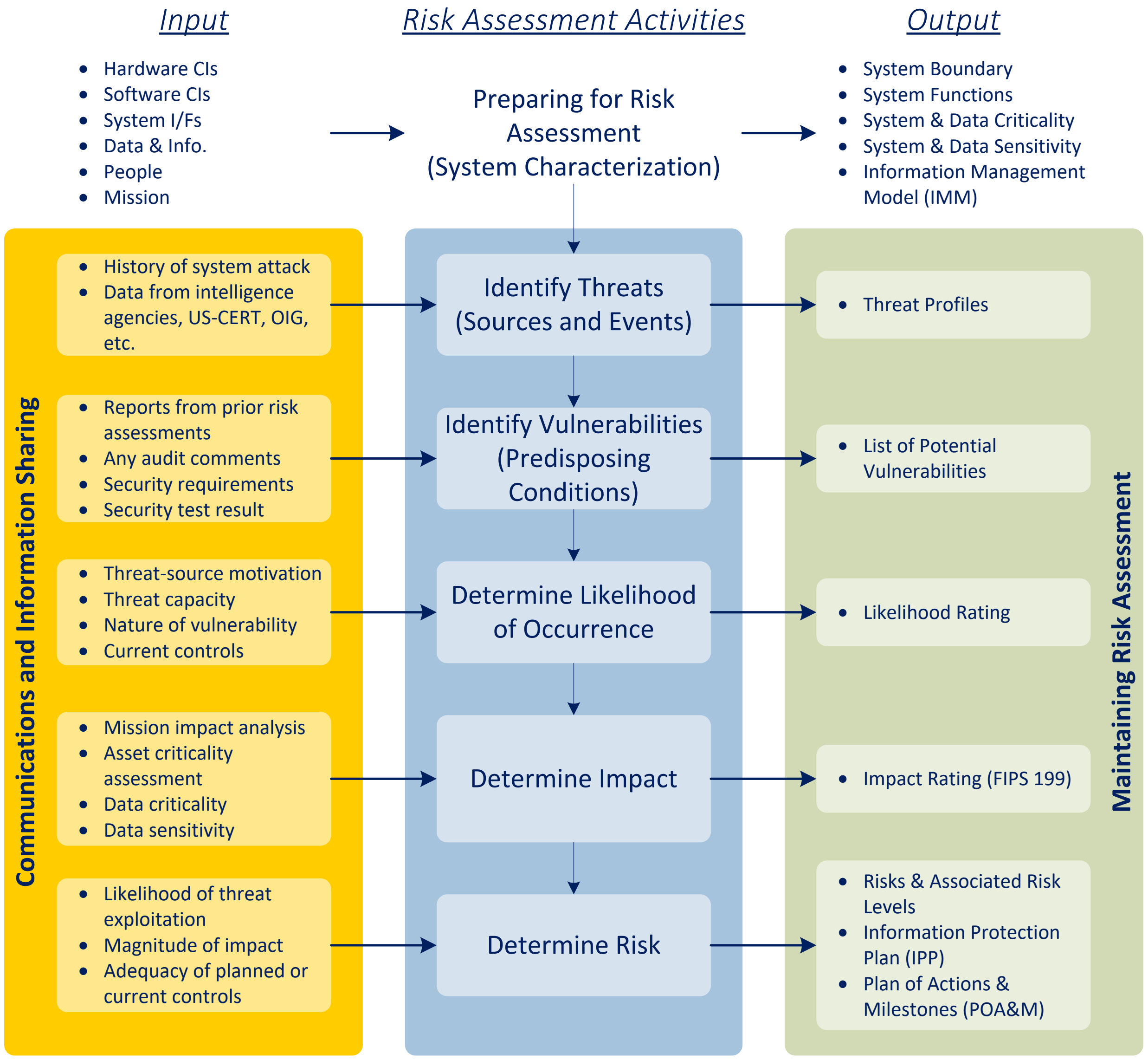
Fundamental

- Risk assessment activities: risk identification, risk analysis, and risk prioritization
- Risk control activities: risk management planning, risk resolution, and risk monitoring



Reference: *Software Risk Management*, B. Boehm, IEEE Computer Society Press , 1989.

Risk Assessment Process



Input

- Hardware CIs
- Software CIs
- System I/Fs
- Data & Info.
- People
- Mission

Risk Assessment Activities

Preparing for Risk Assessment (System Characterization)

Output

- System Boundary
- System Functions
- System & Data Criticality
- System & Data Sensitivity
- Information Management Model (IMM)

Communications and Information Sharing

- History of system attack
- Data from intelligence agencies, US-CERT, OIG, etc.

Identify Threats (Sources and Events)

- Threat Profiles

- Reports from prior risk assessments
- Any audit comments
- Security requirements
- Security test result

Identify Vulnerabilities (Predisposing Conditions)

- List of Potential Vulnerabilities

- Threat-source motivation
- Threat capacity
- Nature of vulnerability
- Current controls

Determine Likelihood of Occurrence

- Likelihood Rating

- Mission impact analysis
- Asset criticality assessment
- Data criticality
- Data sensitivity

Determine Impact

- Impact Rating (FIPS 199)

- Likelihood of threat exploitation
- Magnitude of impact
- Adequacy of planned or current controls

Determine Risk

- Risks & Associated Risk Levels
- Information Protection Plan (IPP)
- Plan of Actions & Milestones (POA&M)

Maintaining Risk Assessment

Reference:
- NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments, Sept. 2011*

Risk Assessment Methods

Quantitative

ALE = SLE x ARO

SLE = AV x EF

- Annualized Lost Expectance (ALE).
- Single Loss Expectance (SLE). Monetary loss (impact) for each occurrence of a threatened event
- Annualized Rate of Occurrence (ARO). The frequency which a threat is expected to occur on an annualized basis
- Asset Value (AV). Monetary value of the information asset
- Exposure Factor (EF). Percentage of loss from a specific threat.

Qualitative

- Likelihood Determination
  - Threat agent motivation & capability
  - Nature of the vulnerability
  - Existence and effectiveness of current controls.
- Impact Analysis (Confidentiality, Integrity & Availability)
  - System mission (e.g., the processes performed by the IT system)
  - System and data criticality (e.g., the system's value or importance to an organization)
  - System and data sensitivity.

		Likelihood Level		
		Low	Medium	High
Magnitude of Impact	Significant (High)	2	3	3
	Serious (Moderate)	1	2	3
	Mild (Low)	1	1	2

Risk Assessment Methods: Quantitative vs. Qualitative

Quantitative

- **Pros**
  - Assessment & results are based substantially on independently objective processes & metrics. Thus, meaningful statistical analysis is supported.
  - The value of information are expressed in monetary terms with supporting rationale, is better understood. Thus, the basis for expected loss is better understood.
  - A credible basis for cost/benefit assessment of risk mitigation measures is provided. Thus, information security budget decision-making is supported.
- **Cons**
  - Calculations are complex. If they are not understood or effectively explained, management may mistrust the results.
  - A substantial amount of information about the target information & its IT environment must be gathered
  - There is not yet a standard, independently developed & maintained threat population & frequency knowledge base.

Qualitative

- **Pros**
  - Calculations are simple and readily understood and executed.
  - Not necessary to determine quantitative threat frequency & impact data.
  - Not necessary to estimate the cost of recommended risk mitigation measures & calculate cost/benefit.
  - A general indication of significant areas of risk that should be addressed is provided.
- **Cons**
  - Risk assessment & results are essentially subjective in both process & metrics. Use of independently objective metrics is eschewed.
  - No effort is made to develop an objective monetary basis for the value of targeted information assets.
  - No basis is provided for cost/benefit analysis of risk mitigation measures. Only subjective indication of a problem.
  - It is not possible to track risk management performance objectively when all measures are subjective.

Risk Control – Determine Information Protection Needs

Mode of Operations: **System-High**

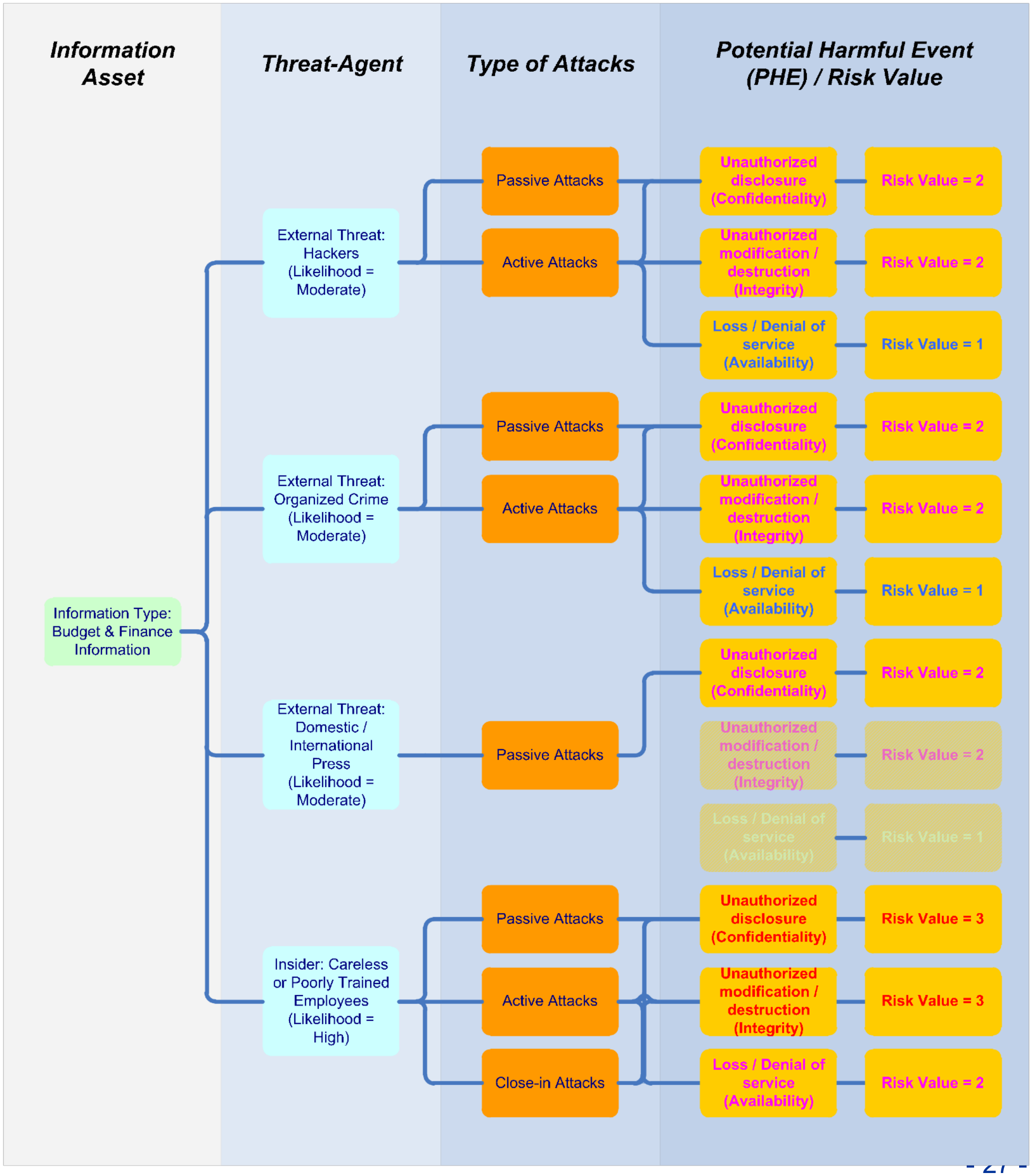
Data Sensitivity: **SBU/FOUO**

SC (**Budget & Finance**) = {Conf.(**M**), Integ.(**M**), Avail.(**L**)}

Threat agent (Likelihood):

- Hackers (**Moderate**)
- Organized Crime (**Moderate**)
- International Press (**Moderate**)
- Careless/Poorly Trained Employees (**High**)

	PHE (Threat Likelihood)		
Severity of HTI (Impact)	Low	Moderate	High
Significant (High)	2	3	3
Serious (Moderate)	1	2	3
Mild (Low)	1	1	2



Information Asset | *Threat-Agent* | *Type of Attacks* | *Potential Harmful Event (PHE) / Risk Value*

Information Type: Budget & Finance Information

External Threat: Hackers (Likelihood = Moderate)
- Passive Attacks
- Active Attacks
  - Unauthorized disclosure (Confidentiality) — Risk Value = 2
  - Unauthorized modification / destruction (Integrity) — Risk Value = 2
  - Loss / Denial of service (Availability) — Risk Value = 1

External Threat: Organized Crime (Likelihood = Moderate)
- Passive Attacks
- Active Attacks
  - Unauthorized disclosure (Confidentiality) — Risk Value = 2
  - Unauthorized modification / destruction (Integrity) — Risk Value = 2
  - Loss / Denial of service (Availability) — Risk Value = 1

External Threat: Domestic / International Press (Likelihood = Moderate)
- Passive Attacks
  - Unauthorized disclosure (Confidentiality) — Risk Value = 2
  - Unauthorized modification / destruction (Integrity) — Risk Value = 2
  - Loss / Denial of service (Availability) — Risk Value = 1

Insider: Careless or Poorly Trained Employees (Likelihood = High)
- Passive Attacks
- Active Attacks
- Close-in Attacks
  - Unauthorized disclosure (Confidentiality) — Risk Value = 3
  - Unauthorized modification / destruction (Integrity) — Risk Value = 3
  - Loss / Denial of service (Availability) — Risk Value = 2

Risk Control – Risk Management Actions

- Risk Acceptance
  - Establish risk acceptance criteria to determine what is acceptable.
- Risk Mitigation
  - Establish plan of action & milestone (POA&M) for implementing safeguards and countermeasures.
- Risk Transfer
  - Transfer the potential liability to another entity (e.g., insurance company.)

NIST SP 800–30

- Standard NIST SP 800–30 – metodyka jakościowa
- Metodyka opracowana przez National Institute of Standards and Technology (ang. Special Publication 800–30 – Risk Management Guide for Information Technology). W dokumencie zostało określonych 9 faz procesu analizy ryzyka dla systemów teleinformatycznych.

NIST SP 800–30 - Step 1

Wybór systemów objętych oceną, określenie zakresu oceny oraz zgromadzeni informacji dotyczących wybranych systemów.

NIST SP 800–30 - Step 2

Identyfikacja i stworzenie kompletnej listy zagrożeń odnoszących się do systemów informatycznych objętych przeprowadzaną oceną ryzyka.

NIST SP 800–30 - Step 3

Identyfikacja i stworzenie kompletnej listy podatności w objętych oceną systemach informatycznych, które mogą zostać wykorzystane przez zidentyfikowane uprzednio zagrożenia.

NIST SP 800–30 - Step 4

Analiza zaimplementowanych bądź planowanych mechanizmów kontrolnych i zabezpieczających mających na celu minimalizację istotności potencjalnych zidentyfikowanych zagrożeń bądź ich całkowitą eliminację.

NIST SP 800–30 - Step 5

- Określenie możliwości wykorzystania podatności przez zagrożenie.

Poziom Wysoki (1): Czynnik sprawczy o wysokiej motywacji, posiadający wystarczający potencjał rażenia, zabezpieczenia zaś mające chronić przed wykorzystaniem podatności są nieskuteczne

Poziom Średni (0,5): Czynnik sprawczy posiada motywację i możliwość, lecz zabezpieczenia są w stanie skutecznie przeciwstawić się wykorzystaniu podatności

Poziom Niski (0,1): Czynnik sprawczy nie ma motywacji lub wystarczającego potencjału rażenia, albo zabezpieczenia są skuteczne, albo przynajmniej w wystarczający sposób chronią przed wykorzystaniem podatności.

NIST SP 800–30 - Step 6

- Umowne określenie poziomu skutków wykorzystania podatności przez zagrożenie według NIST

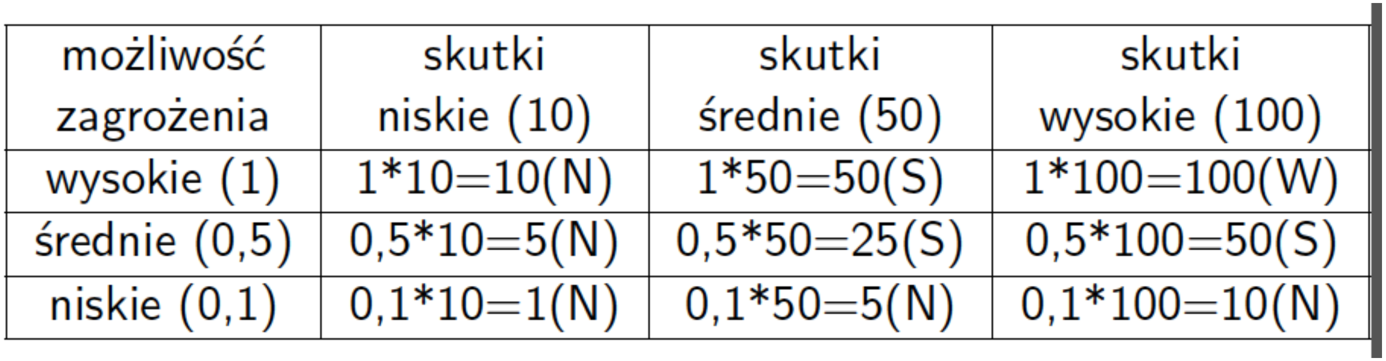
Poziom Wysoki (100): Wykorzystanie podatności może: spowodować najwyższe możliwe straty dla ważnych zasobów, wstrzymać lub znacząco zakłócić realizację ciągłości funkcjonowania, poważnie zaszkodzić interesom lub reputacji instytucji, spowodować utratę życia lub zdrowia ludzkiego

Poziom Średni (50): Wykorzystanie podatności może: spowodować duże straty dla ważnych zasobów, zakłócić realizację celów organizacji, zaszkodzić interesom lub reputacji instytucji, spowodować utratę zdrowia ludzkiego

Poziom Niski (10): Wykorzystanie podatności może: spowodować stratę niektórych ważnych zasobów, zakłócić w sposób zauważalny realizacje celów instytucji, wpłynąć negatywnie na interesy lub reputację instytucji.

NIST SP 800–30 - Step 7

- Określane jest ryzyko na podstawie macierzy ryzyka. Ryzyko dla konkretnego zasobu jest iloczynem dwóch parametrów: możliwości zajścia danego zagrożenia oraz skutków danego zagrożenia. Jakościowe oszacowanie tych czynników jest mapowane na konkretne liczby, które dalej wykorzystywane są podczas obliczeń. Macierz możliwych wartości ryzyka przedstawiona jest w tabeli 1.



możliwość zagrożenia	skutki niskie (10)	skutki średnie (50)	skutki wysokie (100)
wysokie (1)	1*10=10(N)	1*50=50(S)	1*100=100(W)
średnie (0,5)	0,5*10=5(N)	0,5*50=25(S)	0,5*100=50(S)
niskie (0,1)	0,1*10=1(N)	0,1*50=5(N)	0,1*100=10(N)

NIST SP 800–30 - Step 7

- Wartości ryzyka są bezpośrednio związane z wymaganymi Poziomami bezpieczeństwa.

Poziom Wysoki (W) - Silna potrzeba redukcji, działań korygujących, wdrożenia systemu zabezpieczeń. System może kontynuować pracę, jednak plan zabezpieczeń powinien zostać wdrożony niezwłocznie

Poziom Średni (S) - Działania korygujące są konieczne. Plan zabezpieczeń powinien zostać wdrożony w rozsądnym horyzoncie czasowym.

Poziom Niski (N) - Osoba odpowiedzialna za akredytację systemu powinna niezwłocznie podjąć decyzję o podjęciu działań korygujących lub akceptacji ryzyka i dopuszczeniu systemu do eksploatacji

NIST SP 800–30 - Step 8

- Wybór środków ochrony redukujący ryzyka.
- Opracowanie z uwzględnieniem istniejących ograniczeń technologicznych, organizacyjnych i finansowych, rekomendacji dla mechanizmów kontrolnych i zabezpieczających oraz innych rozwiązań mających na celu minimalizację ryzyka systemów informatycznych do poziomu akceptowalnego przez organizację bądź jego całkowitą eliminację.
- Jeśli wykryto podatność (lukę), to należy zastosować środki ograniczające możliwość (prawdopodobieństwo) wykorzystania tej podatności przez czynnik sprawczy zagrożenia. Jeżeli podatność może zostać wykorzystana, to należy zastosować zespół środków - różnego typu zabezpieczeń składających się na ochronę wielowarstwową.
- Jeśli koszt przeprowadzenia ataku jest mniejszy od potencjalnych korzyści (atak opłacalny), to należy zastosować środki zwiększające koszt ataku. Jeśli straty mogą być znaczne, to należy zastosować zespół różnego typu środków ograniczających zasięg ewentualnego incydentu oraz wielkość strat z nim związanych.

NIST SP 800–30 - Step 9

- Przygotowanie dokumentacji wyników przeprowadzonej oceny ryzyka systemów informatycznych w postaci oficjalnego raportu, którego odbiorcami jest kadra zarządzająca

Learning Objectives

Information Security Management Domain

- Information Security Concepts
- Information Security Governance
- Risk Management

➡ Personnel Security

- Security Education, Training, and Awareness

Personnel Security Best Practice

- Hiring…
  - Personnel security interviews.
  - Background investigation.
  - Adjudication.
  - Non-disclosure agreement.
- Operating…
  - Separation of duties.
  - Rotation of jobs.
  - Security awareness briefing.
- Exiting…
  - Debriefing / exit interview.
  - Inventory & close accounts.
  - Escort.

- Personnel security is critical to information security.
- DIA reported 80% of security incidents are originated from internal threat agents.
  - Navy, the Walkers.
  - FBI, the Hanssen.
- Security Awareness
  - Protect against social engineering, dumpster diving, transmission of virus.
  - Kevin Mitnick

References:

- E.O. 13467, *Reforming Process to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, June 30, 2008.
- DCID 6/4, *Personnel Security Standards and Procedure Governing Eligibility for Access to Sensitive Compartmented Information*
- DoD 5200.2-R, *Personnel Security Program*

Insider Threats... (1/2)

- Employees, former employees, and business partners may be the biggest information security threat to an enterprise...

Source of Incidents*	2007	2008
Unknown	**N/A**	42%
Employees	**48%**	**34%**
Hackers	41%	28%
Former employees	**21%**	**16%**
Business partners	**19%**	**15%**
Customer	9%	8%
Other	20%	8%
Terrorist/ foreign government	6%	4%

References:

* *The Global State of Information Security 2008*, CSO Online (http://www.csoonline.com/article/print/454939)

Insider Threats... (2/2)

- Software Engineering Institute (SEI) CERT Program's insider threat studies also found that…
  - 68% of the insider attack occurred at the workplace
  - 73% of crimes were committed during working hours
  - Over three-quarters of the insider had authorized access to information assets
  - None of the insider had privileged access (i.e. system/database administrator.)

References: *Insider Theft of Intellectual Property for Business Advantage: A Preliminary Model, CERT Program*, Software Engineering Institute and CyLab at Carnegie Mellon University, June 2009.

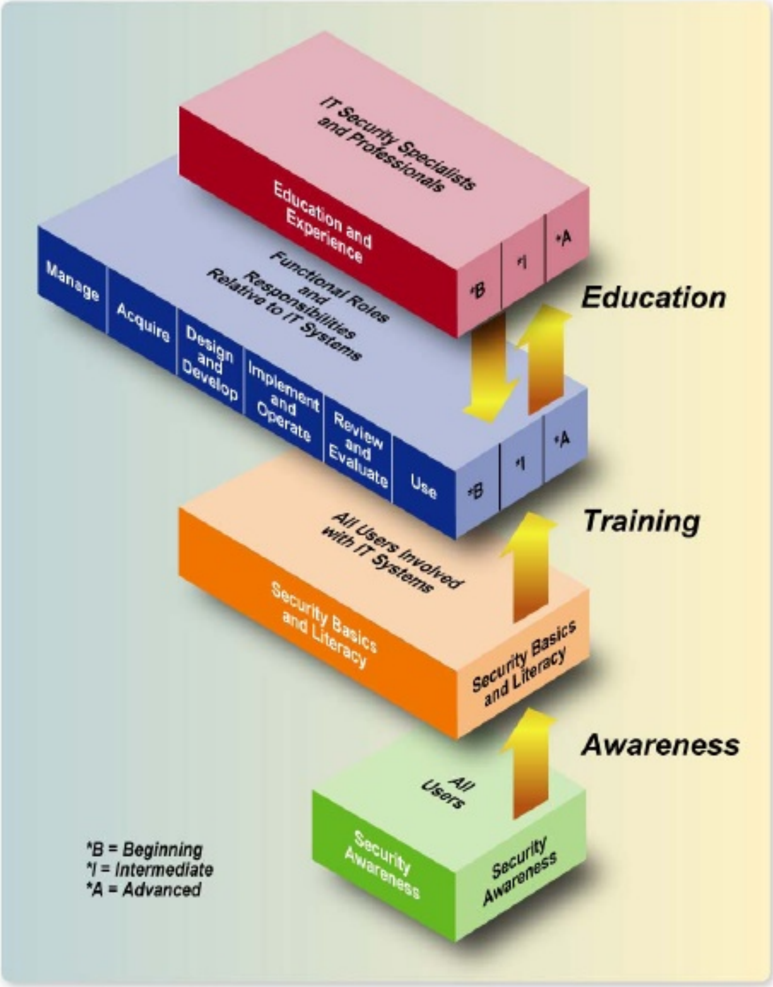
Learning Objectives

Information Security Management Domain

- Information Security Concepts
- Information Security Governance
- Risk Management
- Personnel Security
- ➡ Security Education, Training, and Awareness

Security Education, Training and Awareness (SETA)

- Awareness
  - Orientation briefs and materials to inform and remind employees of their security responsibilities and management’s expectation.
- Training
  - Course and materials to provide employees the necessary skills to perform their job functions.
- Education
  - Course and materials to provide employees the necessary decision-making and management skills to improve their promotional ability and mobility.



Reference: NIST SP800-50, *Building an IT Security Awareness and Training Program.*