Which Best Practices Are Best For Me?

Version 1.0

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Sponsored by the U.S. Department of Defense

Today’s Objective

Our objective is to present an alternative way for you and your organization to think about information security best practices and to provide you with an approach for evaluating and selecting best practices in your organization.

Lots Of Best Practices

There exists a significant body of information security best practices, processes, and guidelines from which an organization can choose:

ISO 17799	(International Organization for Standardization)
CoBiT	(Control Objectives for Information & Related Technology)
NIST 800 Series	(National Institute of Standards and Technology)
FIPS 199	(Federal Information Processing Standards)
FFIEC Handbooks	(Federal Financial Institutions Examination Council)
ISSA-GAISP	(Information System Security Association – Generally Accepted Information Security Principles)
ITIL	(IT Infrastructure Library)
BITS	(Banking Industry Technology Secretariat)
NERC	(North American Electric Reliability Council)

Defining Security Practices

What they are:

A security practice is any action, procedure, technique, or measure that provides assurance that a control objective will be achieved.

What they do:

Security practices apply controls in a manner that best achieves a control objective and supports the security requirements of an information asset or system.

Information Security and Assets

Traditionally information security best practices are focused on tangible assets that are of one of two types:

- Information assets (data and information)
- Technology assets (information systems and their supporting technical infrastructure)

Significant Range in Levels of Practice

High-Level Practice:

Senior management actively manage information security risks.

Low-Level Practice:

System Administrators should disable the guest account on all windows systems.

Three Types Of Practices

Administrative Practices:

Senior management should demonstrate their commitment to information security by allocating sufficient organizational resources.

Technical Practices:

System Administrators should disable the guest account on all systems.

Physical Practices:

Sensitive materials should be stored in locked cabinets when not in use.

Example: Deconstructing Practices

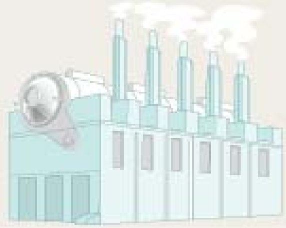
Information Asset	Human Resources Database (HRD)
Security Requirement	Only human resources personnel may create, modify, update, or delete records
Control Objective	Ensure that access to the HRD is limited to only human resources personnel
Best Practice	Users of an information asset should be authorized by the asset owner.
Implemented Best Practice	System administrators will only grant access to the HRD when authorized in writing by the director of the human resources department

Choosing Best Practices - 1

What motivates an organization to choose a best practice?

- Legislation or Regulation
  - GLB (1999), Sarbanes-Oxley (2002), HIPAA (1996)
  - DoD Regulation 5200.1-R: Information Security Program

- Industry Guidelines/Benchmarks
  - ISSA, ISACA



- Technology Deployment
  - Hardware, Software, Development, Remote Access, Telecommunications

Choosing Best Practices - 2

Should organizations choose best practices for reasons other than governmental decrees or because they are industry standards?

How can organizations determine which practices are appropriate and effective?

Guiding Information Security Principle

Organizations should focus their limited resources (personnel, time, and money) on the identifying and managing the information security risks that are most important to supporting its business drivers and ensuring its long term survivability of its mission.

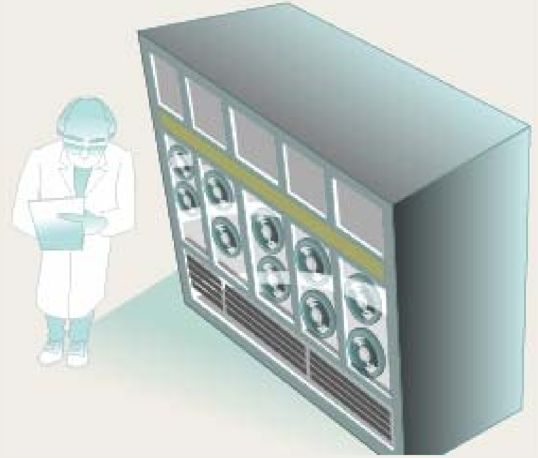
Decision Criteria For A Best Practice

A criteria for selecting practices:

1. Does the practice actually mitigate a risk or satisfy a security requirement?

2. Can the practice be implemented as planned?

3. Does the benefit from a practice outweigh its cost?



Moving In The Right Direction

In order to evaluate a practice against this criteria an organization must be able to describe:

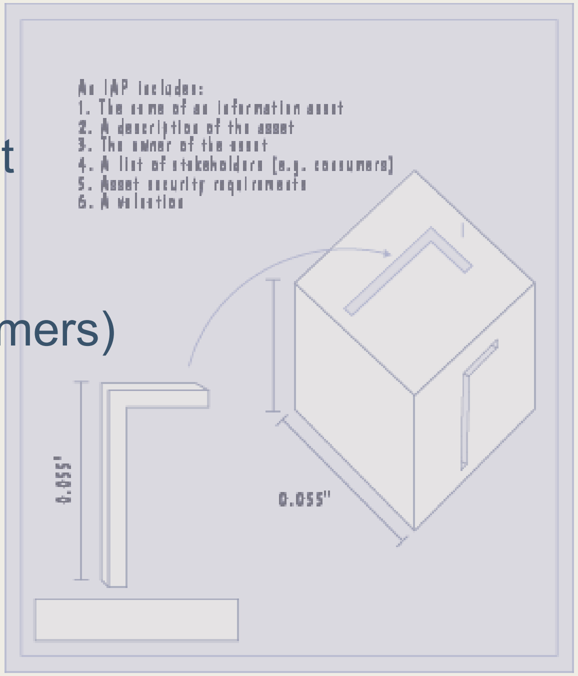
- The asset to be protected and its security requirements
- The asset's relative and specific value
- How the practice would contribute to an assets' protection

Start With Information Asset Profiles

An Information Asset Profile (IAP) provides an organization with consistent, unambiguous, and agreed upon description of an information asset.

An IAP includes:

1. The name of an information asset
2. A description of the asset
3. The owner of the asset
4. A list of stakeholders (e.g. consumers)
5. Asset security requirements
6. A valuation


An IAP includes:
1. The name of an information asset
2. A description of the asset
3. The owner of the asset
4. A list of stakeholders (e.g. consumers)
5. Asset security requirements
6. A valuation

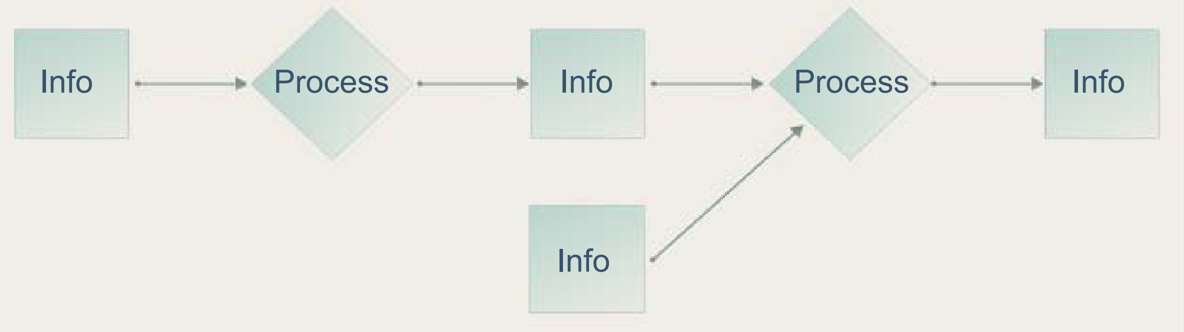
Challenges In Building Profiles

1. Ambiguous boundaries

2. Owners and custodians

3. Determining value

Challenge: Ambiguous Boundaries



1. Is the new information asset substantially different than those assets from which it was derived?

2. Who is the owner of the new asset?

3. What are the security requirements for the new asset?

Challenge: Owners and Custodians

Challenge: Owners and Custodians

Many organizations fail to distinguish between an information asset’s owners and it’s custodians.

Owners are designated by an organization to be responsible for:

- Defining and scoping
- Determining value
- Setting the security requirements
- Communicating security requirements to all custodians
- Ensuring that security requirements have been implemented

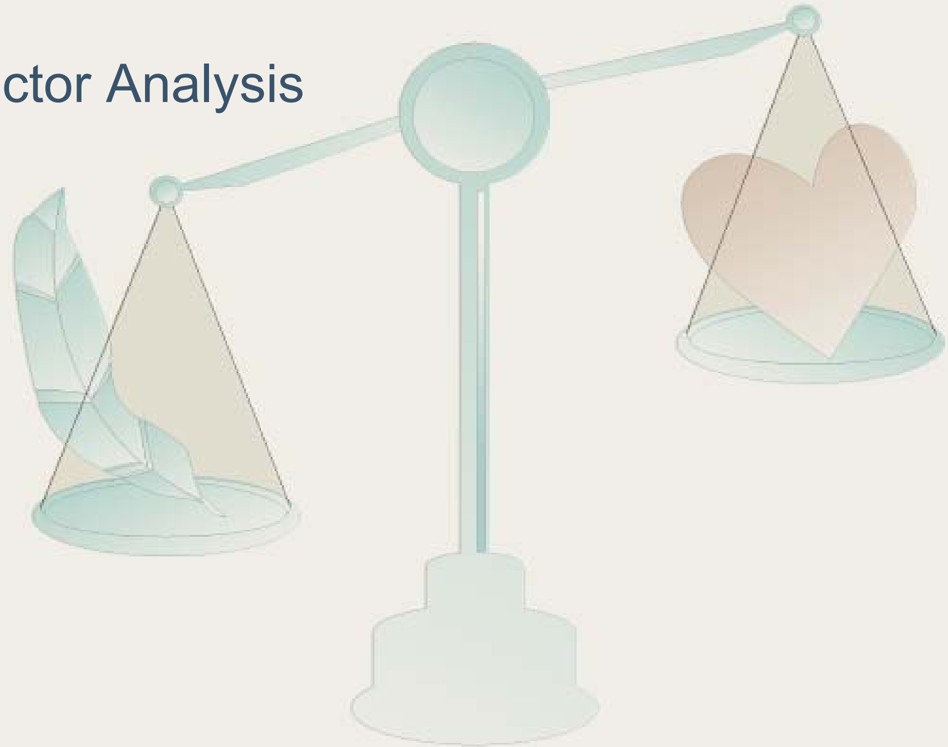
Custodians of an information asset are responsible for:

- Implementing security controls in places where it is stored, transported, or processed.

Challenge: Determining Value

How does an organization decide which assets are the most important and then value them?

- Critical Success Factor Analysis
- FIPS 199
- Regulations



Following The Data Trail

Following the trail of a valuable information asset will lead to the places where it is stored, transported, or processed (containers).

These containers define a boundary for information security risk management activities.

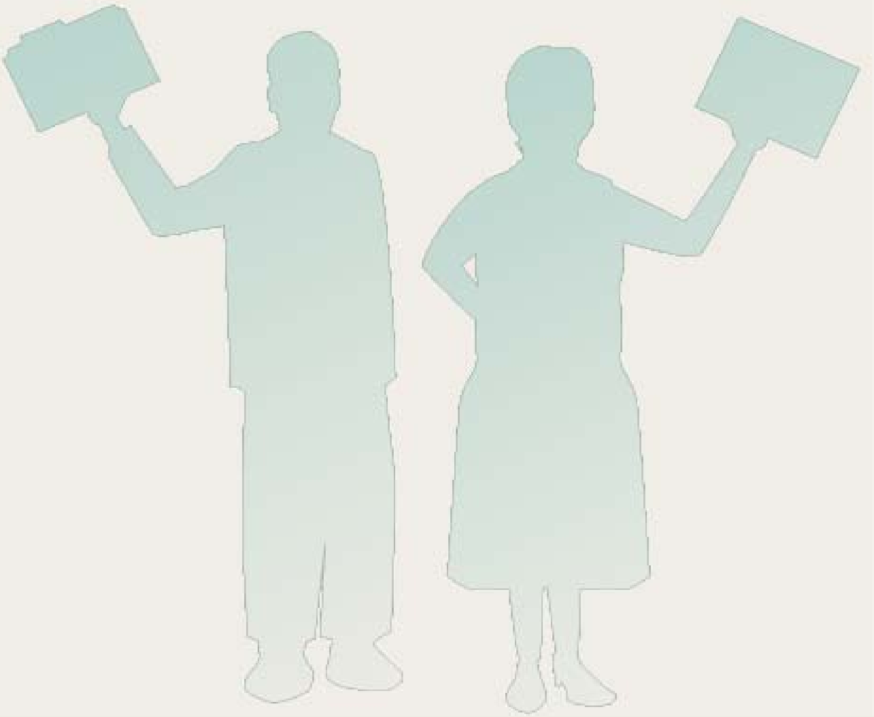
This data-centric approach ensures that the scope of information security activities are properly focused and efficient.

Dilemma of Data -1

- The owner of the information asset and the owner of the container are the same.

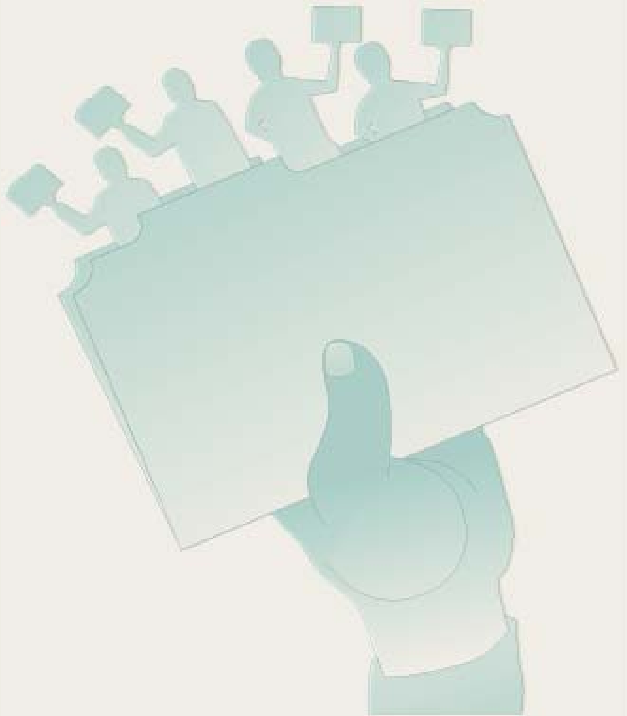
Dilemma of Data - 2

- The owner of the information asset and the owner of the container are different.



Dilemma of Data - 3

- There are multiple information assets with multiple owners in a container with a different owner.



Post-IAP Information Security Activities

Developing asset profiles can be a last step, but many benefits are derived from using IAP information to drive other security activities

- IAP feeds strategic information security activities, such as threat and risk assessments, by defining the information assets to analyze for threats, risks, and impacts
- IAP promotes the selection of proper security control and best practice selection, by insuring security requirements are addressed
- IAP helps to refine policy and procedure, by defining the information asset, its user-base, its custodians, its owner/stewardship, its boundaries, and its characteristics

Use IAP To Drive Risk Activities

Step 1: Develop information asset profiles

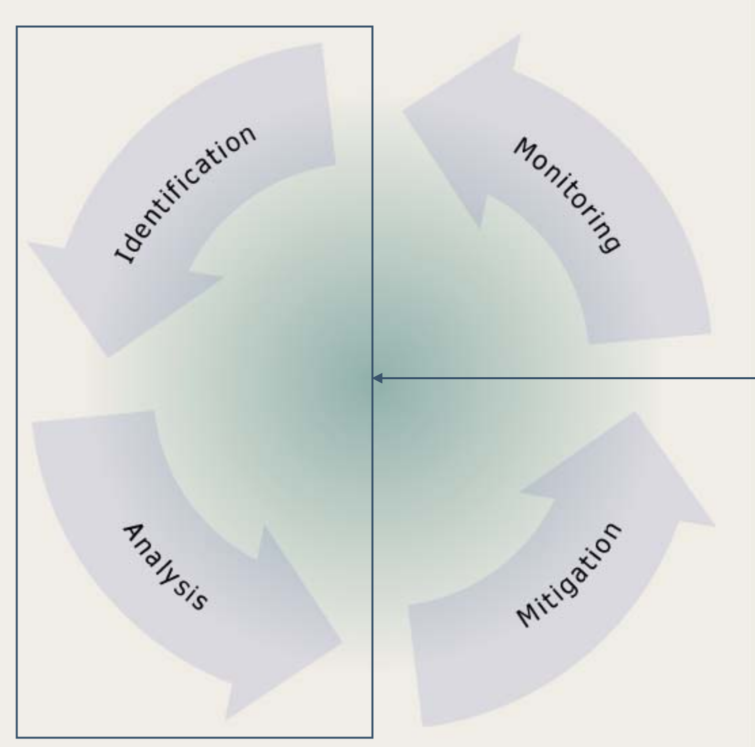
Step 2: Determine where information asset is stored, transported and processed

Step 3: Assess risk at each location where asset is stored, transported or processed

Step 4: Develop protection strategy which acceptably mitigates organizational risk

The Risk Management Process

There are four phases in the risk management process:



The *identification* and *analysis* phases are often collectively referred to as the **risk assessment phase**

Risk-aware Security Requirements and Controls

After a value driven data-centric risk assessment is performed, security controls can be implemented to:

- Provide information security, that is, the protection of the information asset within a system against unauthorized disclosure, modification, or destruction and protection of the computer system itself.

- Prevent or detect unauthorized use, modification, or denial of service, which are the requirements of security as determined in the IAP.

Security Requirements

	Requirement Definition
Confidentiality	The protection of information in the system so that unauthorized persons cannot access it.
Integrity	The protection of system data from intentional or accidental unauthorized changes.
Availability	The assurance that a computer system is accessible by authorized users whenever needed.

Source: Krause, M., Tipton, H. Handbook of Information Security Management. CRC Press LLC, 1999.

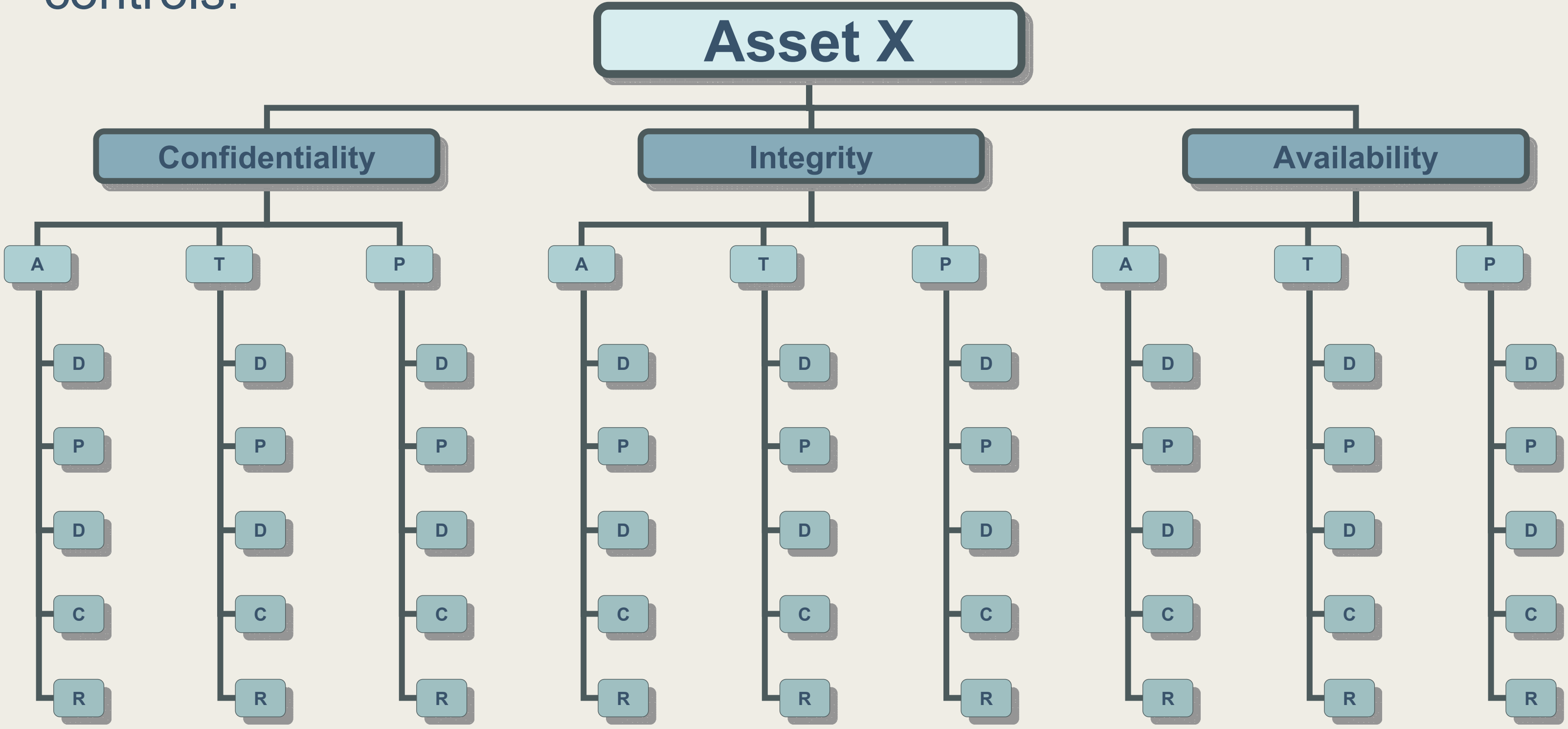
Information Security Controls

CONTROLS	Physical, Technical, and Administrative
Preventive	Attempt to avoid the occurrence of unwanted events
Detective	Attempt to identify unwanted events after they have occurred
Deterrent	Attempt to discourage individuals from intentionally violating information security policies or procedures
Corrective	Attempt to remedy the circumstances that allowed the unauthorized activity or return conditions to what they were before the violation
Recovery	Attempt to restore lost computing resources or capabilities and help the organization recover monetary losses caused by a security violation

Source: Krause, M., Tipton, H. Handbook of Information Security Management. CRC Press LLC, 1999.

Asset Protection

Asset protection is the attempt to assure security requirements are met through the implementation of appropriate security controls.



Asset X

Confidentiality

A
D
P
D
C
R

T
D
P
D
C
R

P
D
P
D
C
R

Integrity

A
D
P
D
C
R

T
D
P
D
C
R

P
D
P
D
C
R

Availability

A
D
P
D
C
R

T
D
P
D
C
R

P
D
P
D
C
R

Example: Security requirements through security controls

Confidentiality

Only authorized HR personnel and immediate supervisors may view employee records

Integrity

Only authorized HR personnel may add, modify, or delete information in an employee record

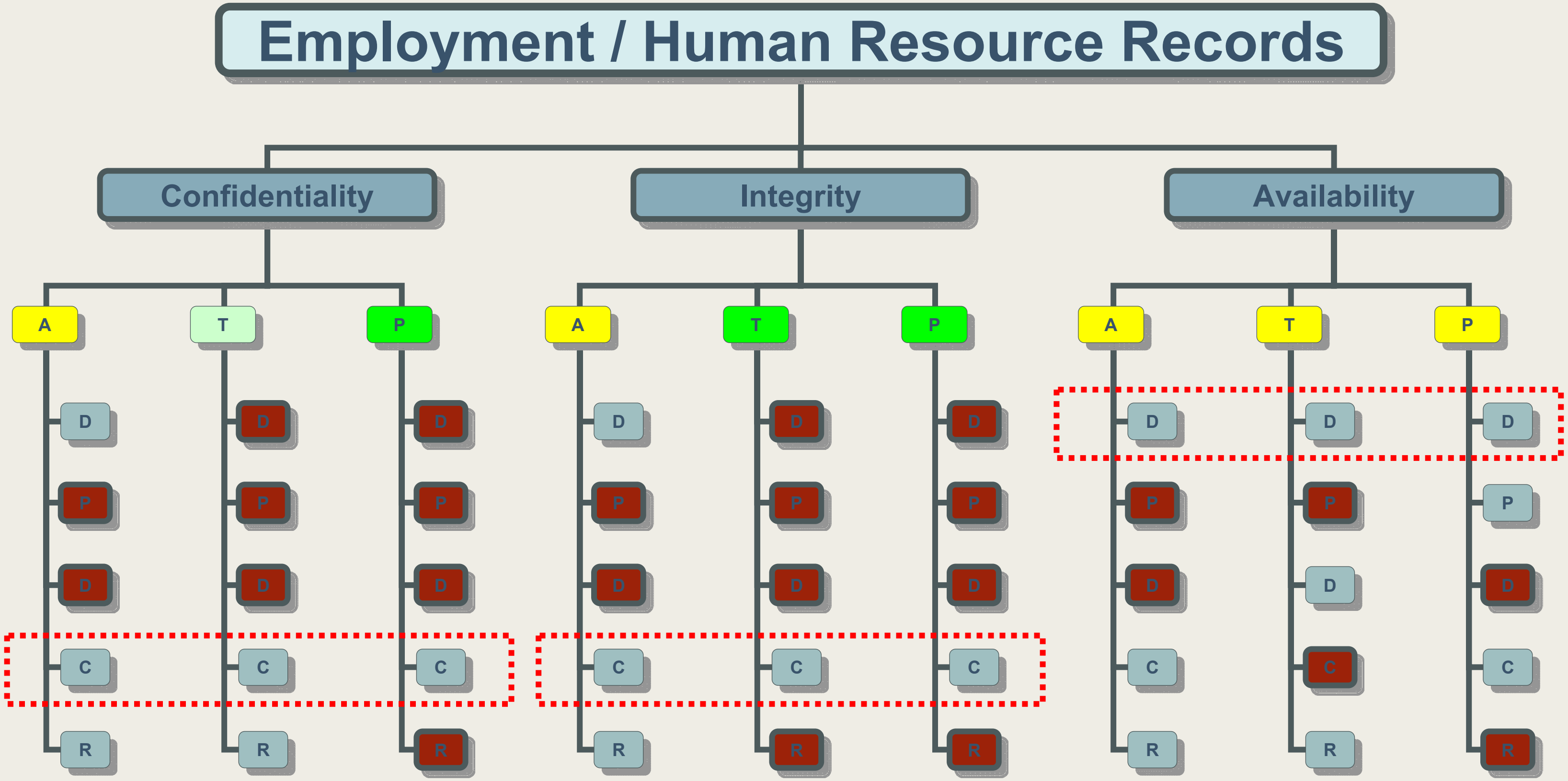
Availability

HR employee records must be available on-demand, during business hours, M – F, 365 days

Example: Security requirements through security controls - 2

CONTROLS	Physical	Technical	Administrative
Preventive	Secure key-card access reader to enter HR area.	System and network monitoring (spy ware).	Policy: Access to HR data (including excepted situations).
Detective	Seals on archive file cabinets.	Log message to HR system administrator regarding incorrect password attempts.	Audit of HR change-management procedures and payroll records, for anomalies.
Deterrent	Closed-circuit camera (for non-office hours)	Account lock-out after 3 successive incorrect password attempts.	Process: All modifications to employee benefits must be approved by someone other than the HR person making the request.
Corrective	Physical isolation of all HR servers from public areas.	IDS providing updated firewall policy, from learned events (DoS, AV).	New Process: Ensuring building custodial functions only access HR areas at times when an HR employee is present.
Recovery	Electronic HR records used to re-create physical files.	Self-healing system, uses integrity services to repair lost/damaged processes, data, etc.	Policy: Contacting law enforcement after an internal or external breach in security.

Example: Security requirements through security controls - 3



Employment / Human Resource Records

- Confidentiality
  - A: D, P, D, C, R
  - T: D, P, D, C, R
  - P: D, P, D, C, R
- Integrity
  - A: D, P, D, C, R
  - T: D, P, D, C, R
  - P: D, P, D, C, R
- Availability
  - A: D, P, D, C, R
  - T: D, P, D, C, R
  - P: D, P, D, C, R

Summary

Organizations should decide for themselves which best practices are best for them using security requirements, risk, practicality, and value as the primary selection criteria.

A data driven approach (IAP) provides a framework for organizations to make informed choices when selecting best practices to implement.

For more information

Networked Systems Survivability Program
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213 USA

http://www.cert.org
http://www.sei.cmu.edu

James Stevens
jfs@sei.cmu.edu

Bradford Willke
bwillke@sei.cmu.edu