CultureLink

CSX – Cybersecurity Fundamentals

Section 4 : Security of Networks, Systems, Applications and Data

Course Plan

Module Titles
Section 1 – Cybersecurity Introduction and Overview
Section 2 – Domain 1: Cybersecurity Concepts
Section 3 – Domain 2: Security Architecture Principles
Section 4 – Domain 3: Security of Networks, Systems, Applications and Data
Section 5 – Domain 4: Incident Response
Section 6 – Domain 5: Security Implications and Adoption of Evolving Technology
Section 7 – Course Review
Section 8 – Practice Exam

Learning Outcomes for this Module

- Knowledge of vulnerability assessment tools, including open source tools, and their capabilities
- Knowledge of basic system administration, network and operating system hardening techniques.
- Knowledge of risk associated with virtualizations
- Knowledge of penetration testing
- Knowledge of network systems management principles, models, methods and tools
- Knowledge of remote access technology
- Knowledge of UNIX command line

Learning Outcomes for this Module

- Knowledge of system and application security threats and vulnerabilities
- Knowledge of system life cycle management principles, including software security and usability
- Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance and reliability
- Knowledge of system and application security threats and vulnerabilities
- Knowledge of social dynamics of computer attackers in a global context
- Knowledge of secure configuration management techniques

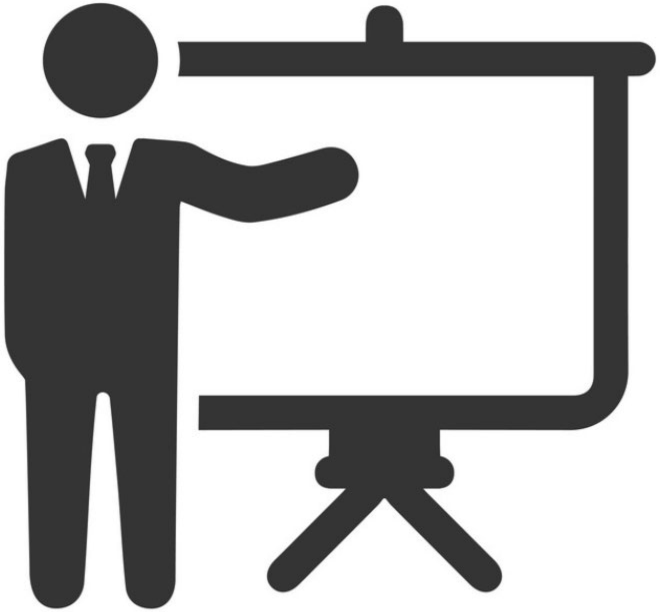
Learning Outcomes for this Module

- Knowledge of capabilities and applications of network equipment including hubs, routers, switches, bridges, servers, transmission media and related hardware
- Knowledge of communication methods, principles and concepts that support the network infrastructure
- Knowledge of the common networking protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP]) and services and how they interact to provide network communications
- Knowledge of different types of network communication (e.g., local area network [LAN], wide area network [WAN], metropolitan area network [MAN], wireless local area network [WLAN], wireless wide area network [WWAN])
- Knowledge of virtualization technologies and virtual machine development and maintenance
- Knowledge of application security (e.g., system development life cycle [SDLC], vulnerabilities, best practices)
- Knowledge of risk threat assessment

Topics for this Module

- **4.1** Process controls – risk assessment
- **4.2** Process controls – vulnerabilities management
- **4.3** Process controls – penetration testing
- **4.4** Network security
- **4.5** Operating system security
- **4.6** Application security
- **4.7** Data security

Current Events



Section 4.1

Process controls – risk assessments

Question

What is Risk?

*“The possibility of **loss** of a **digital asset** resulting from a threat exploiting a **vulnerability** (weakness)”*

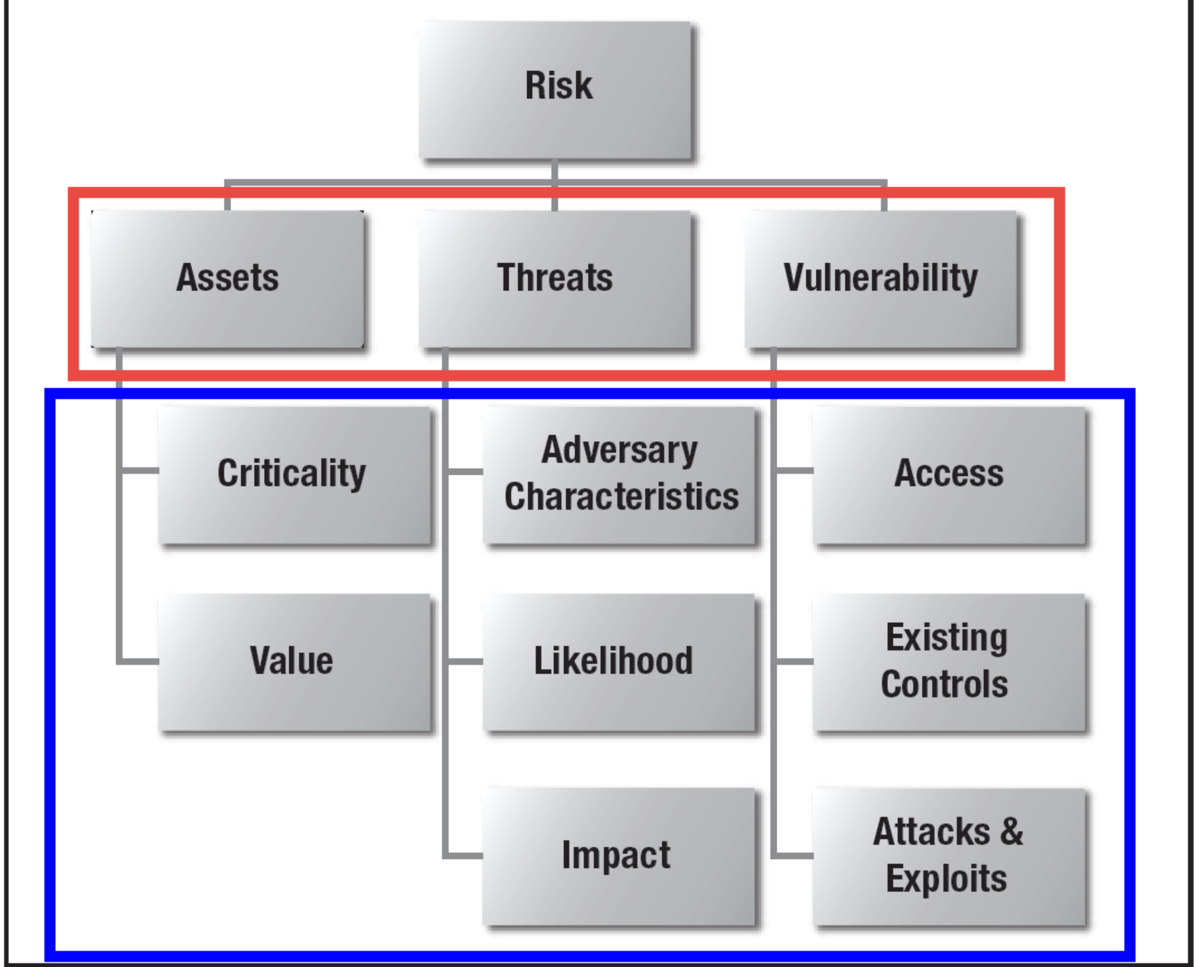
Cyberrisk assessment needed to analyse risk

Cyber risk assessment

Common elements to Risk assessments

Elements to be evaluated

Figure 4.1—Attributes of Risk

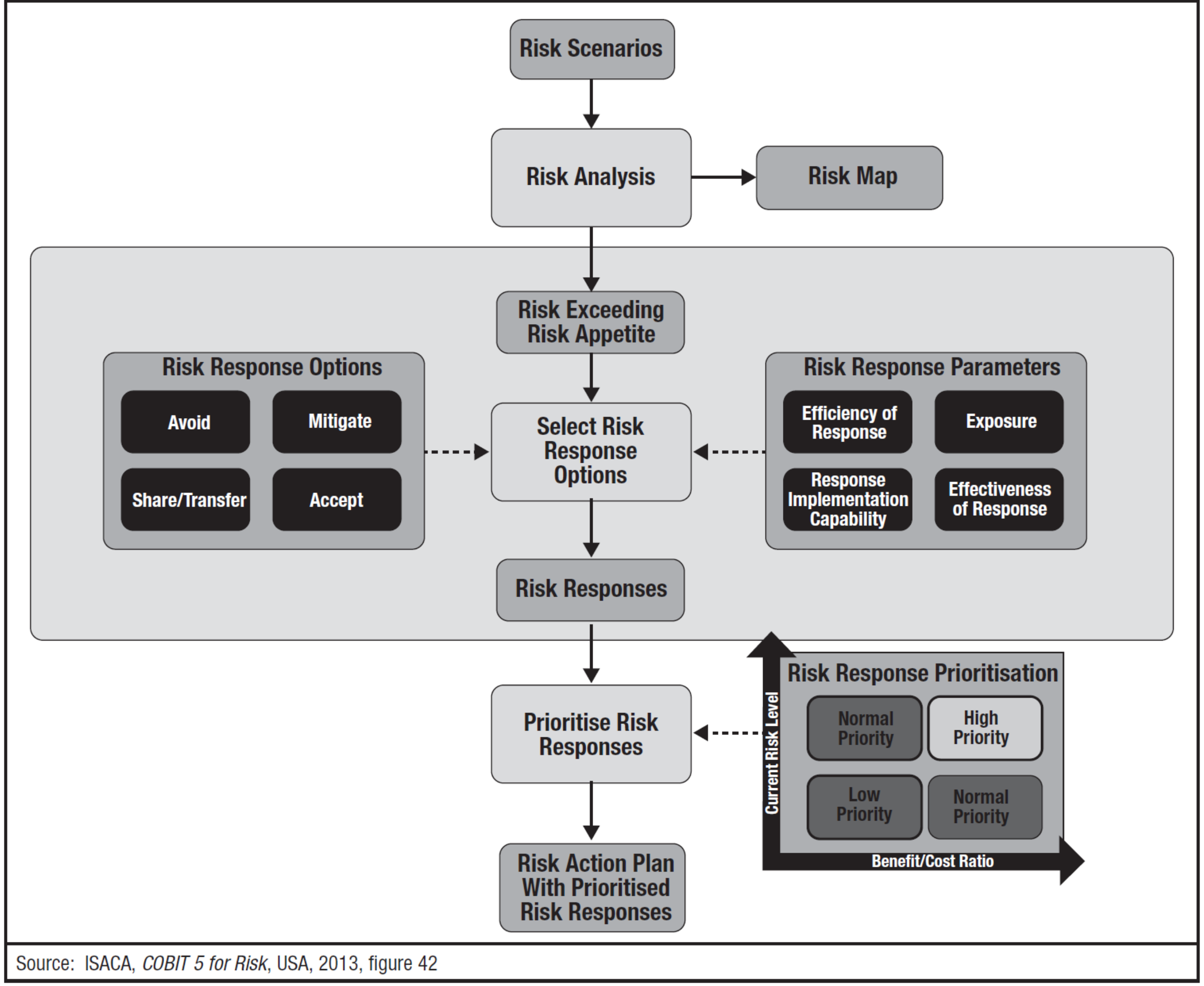


Source: Encurve, LLC.

CultureLink

Risk response workflow

Figure 4.2—Risk Response Workflow



Source: ISACA, *COBIT 5 for Risk*, USA, 2013, figure 42

Risk workflow componets

Risk analysis:

- Oriented toward one of these inputs:

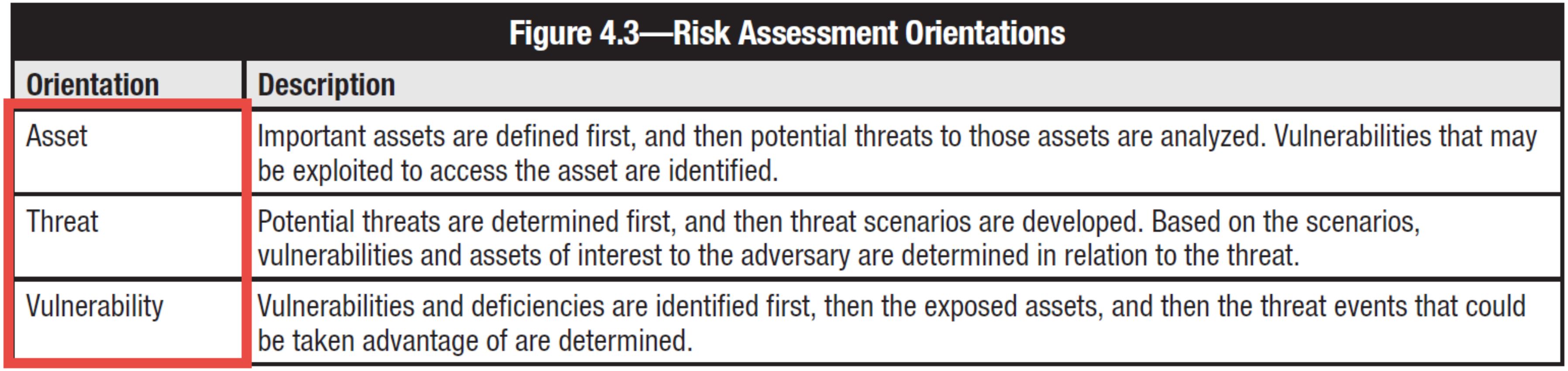


Figure 4.3—Risk Assessment Orientations

Orientation	Description
Asset	Important assets are defined first, and then potential threats to those assets are analyzed. Vulnerabilities that may be exploited to access the asset are identified.
Threat	Potential threats are determined first, and then threat scenarios are developed. Based on the scenarios, vulnerabilities and assets of interest to the adversary are determined in relation to the threat.
Vulnerability	Vulnerabilities and deficiencies are identified first, then the exposed assets, and then the threat events that could be taken advantage of are determined.

One or more can be considered as inputs to assure analysis process is not weakened

Risk workflow components

Evaluating security controls:

- After risk is identified and prioritized, existing controls should be analyzed to determine effectiveness

Risk assessment success criteria:

- Analysis method: **Quantitative** or **Qualitative**
- Understand the business risk appetite, culture
- Assessments are a continue process - not one time deal

Risk Response

What the business needs to decide what to do with the Risk identified:

- **Reduce**
- **Avoid**
- **Transfer**
- **Accept**

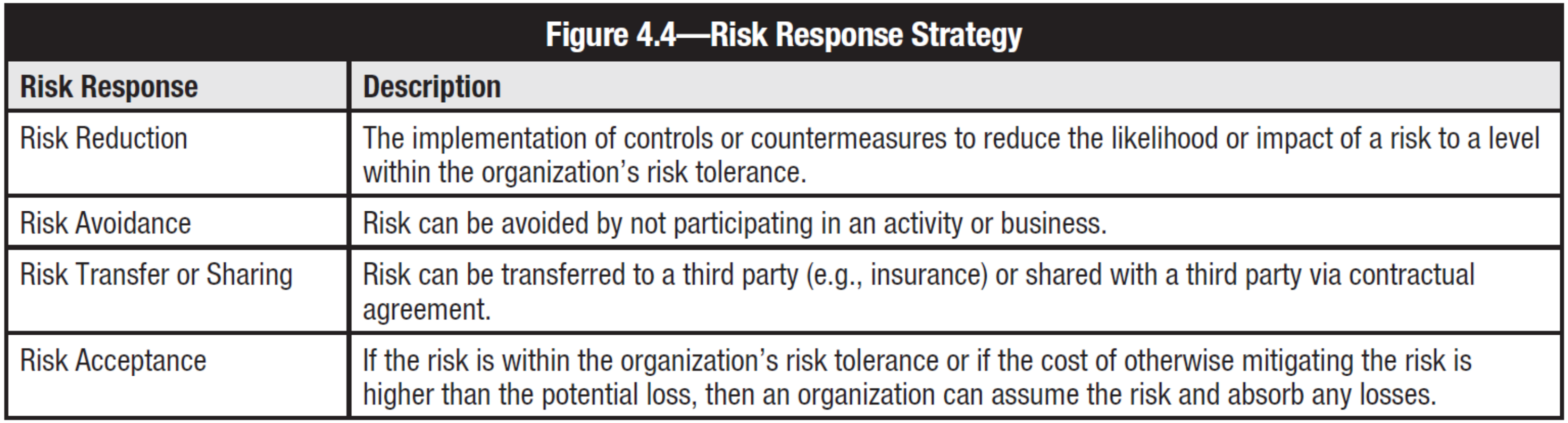


Figure 4.4—Risk Response Strategy

Risk Response	Description
Risk Reduction	The implementation of controls or countermeasures to reduce the likelihood or impact of a risk to a level within the organization's risk tolerance.
Risk Avoidance	Risk can be avoided by not participating in an activity or business.
Risk Transfer or Sharing	Risk can be transferred to a third party (e.g., insurance) or shared with a third party via contractual agreement.
Risk Acceptance	If the risk is within the organization's risk tolerance or if the cost of otherwise mitigating the risk is higher than the potential loss, then an organization can assume the risk and absorb any losses.

Transferring risk does not eliminate accountability to the business

Any questions?

Section 4.2

Process controls – vulnerability management

Question

What is a vulnerability?

“Weakness or security hole that needs to be addresses”

Question

How do you find those holes or weakness?

"You look for them or use software to scan for them and identify them"

Vulnerabilities

The business needs to categorize them and manage them:

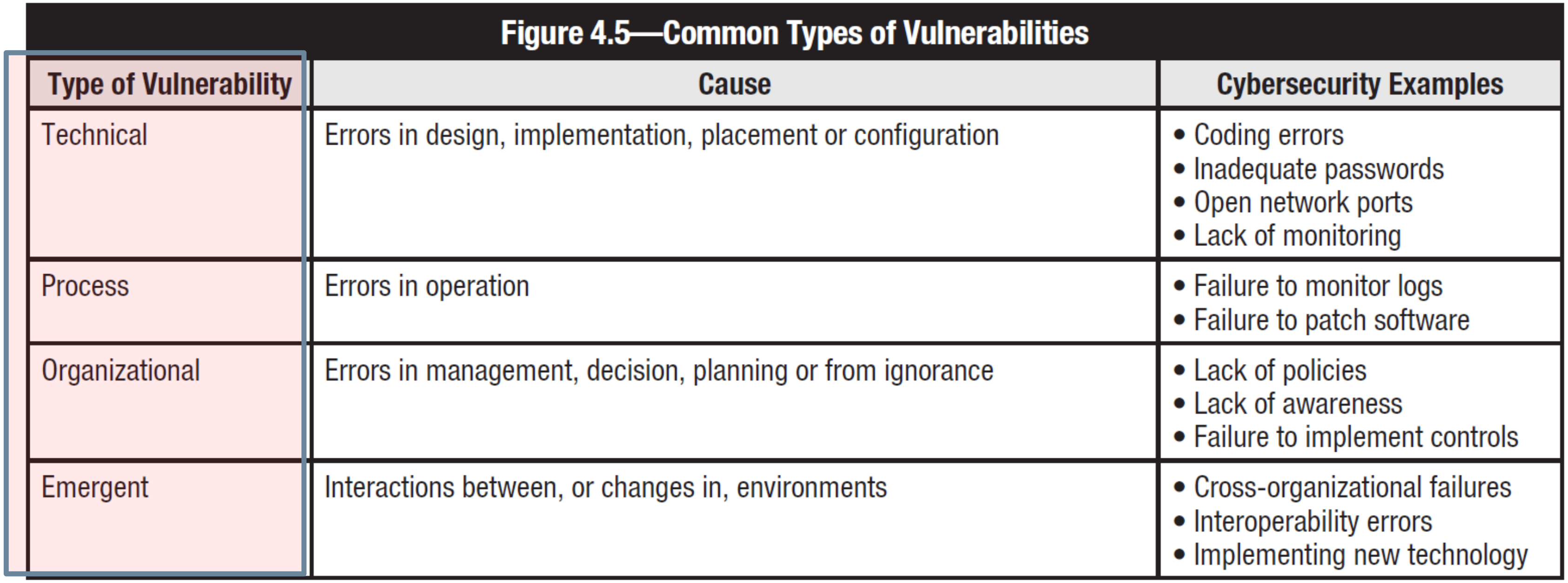


Figure 4.5—Common Types of Vulnerabilities

Type of Vulnerability	Cause	Cybersecurity Examples
Technical	Errors in design, implementation, placement or configuration	• Coding errors • Inadequate passwords • Open network ports • Lack of monitoring
Process	Errors in operation	• Failure to monitor logs • Failure to patch software
Organizational	Errors in management, decision, planning or from ignorance	• Lack of policies • Lack of awareness • Failure to implement controls
Emergent	Interactions between, or changes in, environments	• Cross-organizational failures • Interoperability errors • Implementing new technology

Categories

Vulnerabilities

Remediation:

- After assessed, decision whether to eliminate or mitigate has to be made
- Most often remediation involves patching or reconfiguration process

Reporting:

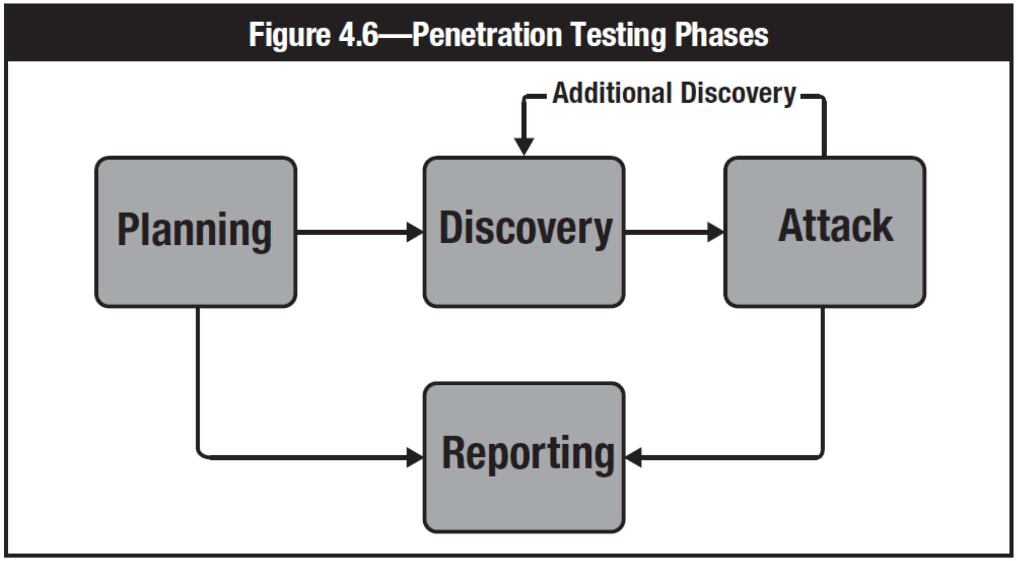
- Tracking vulnerabilities is important
- Opportunity to report back to management

Any questions?

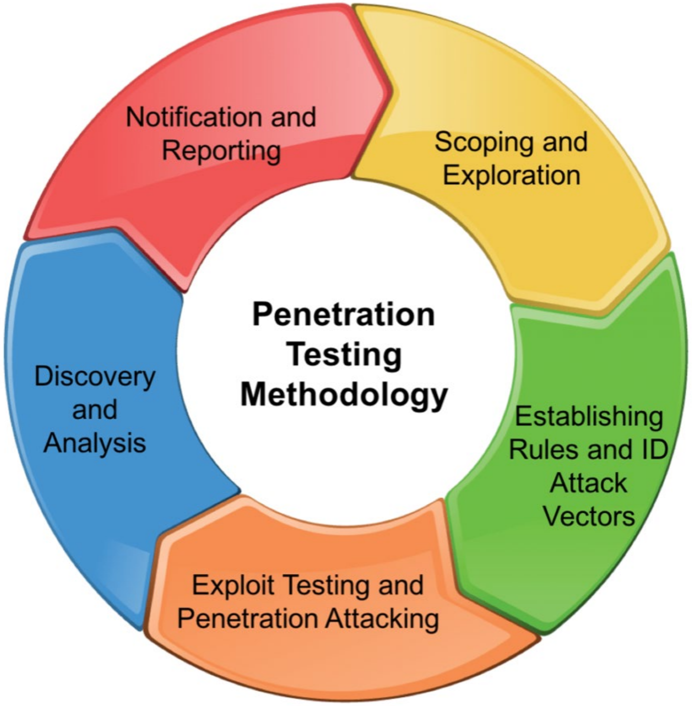
Section 4.3

Process controls – penetration testing

Penetration testing phases



Source: ISACA


Penetration Testing Methodology
Scoping and Exploration
Establishing Rules and ID Attack Vectors
Exploit Testing and Penetration Attacking
Discovery and Analysis
Notification and Reporting

Source: trushieldinc.com

CultureLink

Any questions?

Section 4.4

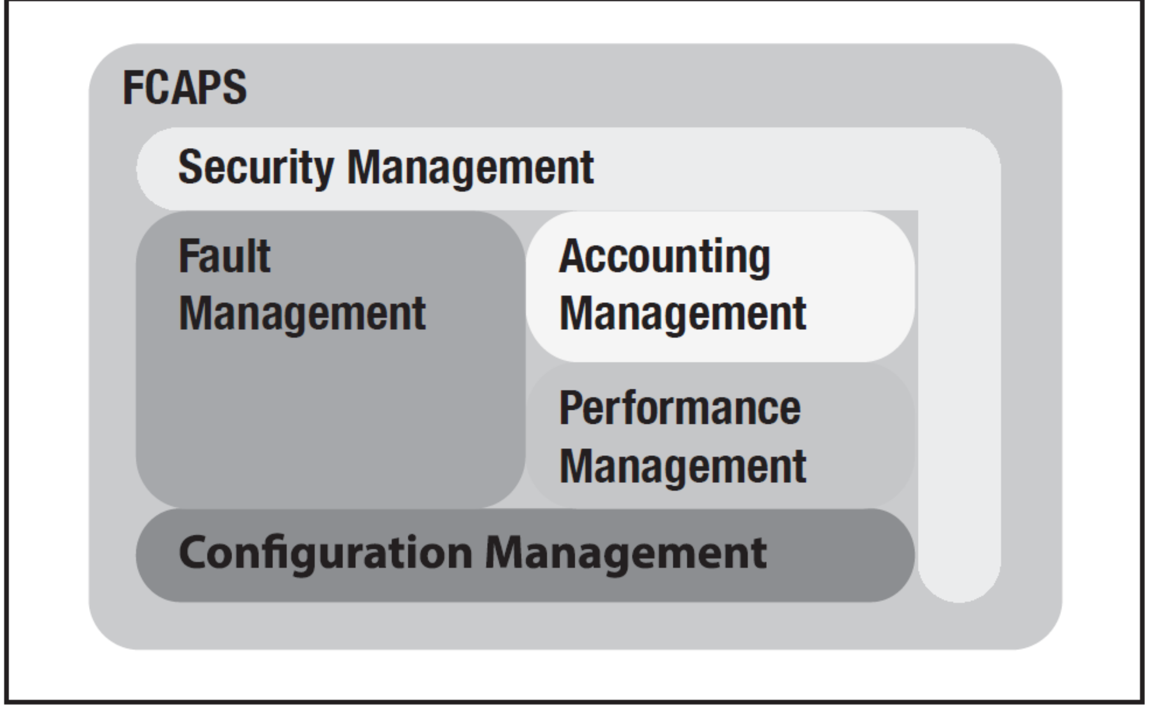
Network security

Network security

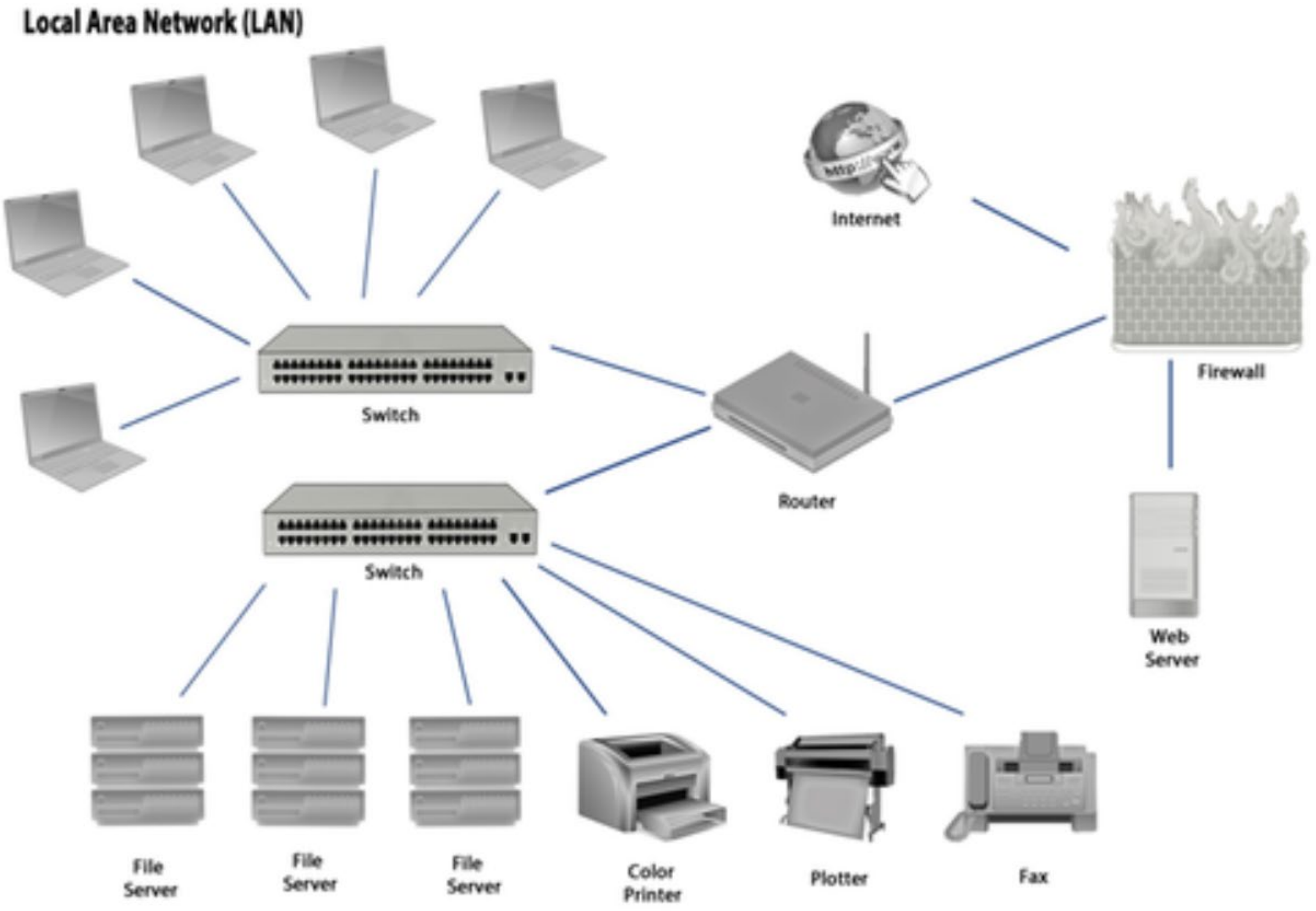
Network management:

- Five functional areas (FCAPS)

Figure 4.8—Five Functional Areas of Network Management (FCAPS)



Local Area Network (LAN)



LAN / WAN Security

- LAN represents decentralized computing, which can provide more computing environment
- Challenge: Administrators frequently lack experience and can’t manage a complex LAN
- Need appliances to assist:
  - Network Access Control (NAC)
  - NAC can auto remediate according to policies

LAN risk issues

- Loss of data and program integrity through unauthorized changes
- Lack of current data protection through inability to maintain version control
- Exposure to external activity through limited user verification and potential public network access from dial-in connections
- Virus and worm infection
- Improper disclosure of data because of general access rather than need-to-know access provisions
- Violation of software licenses by using unlicensed or excessive numbers of software copies

Wireless

- Wireless introduces new elements of risk
- Existing application might need to retrofitted
- Bandwidth
- Synchronization issues
- Unresolved security and privacy issues

Wireless Local Area Networks (WLAN)

- WLANs allow greater flexibility and portability than traditional wired LANs.
- Unlike a traditional LAN, which requires a wire to connect a user's computer to the network, a WLAN connects computers, tablets, smartphones and other components to the network using an access point device
- Access range 300 feet
- WLAN technologies offer varies levels of security features (WEP, WPA)

Wireless network protection

- IEEE 802.11's **Wired Equivalent Privacy (WEP) encryption uses symmetric, private keys**, which means the end user's radio-based network interface controller (NIC) and access point must have the same key

- **WPA and WPA V2 (preferred) are applicable to most wireless networks and commonly used in networks** that involve PCs. Messages transmitted using portable wireless devices should also be protected with encryption and, where possible, VPN methods can be used to provide additional security.

Ports / Protocols

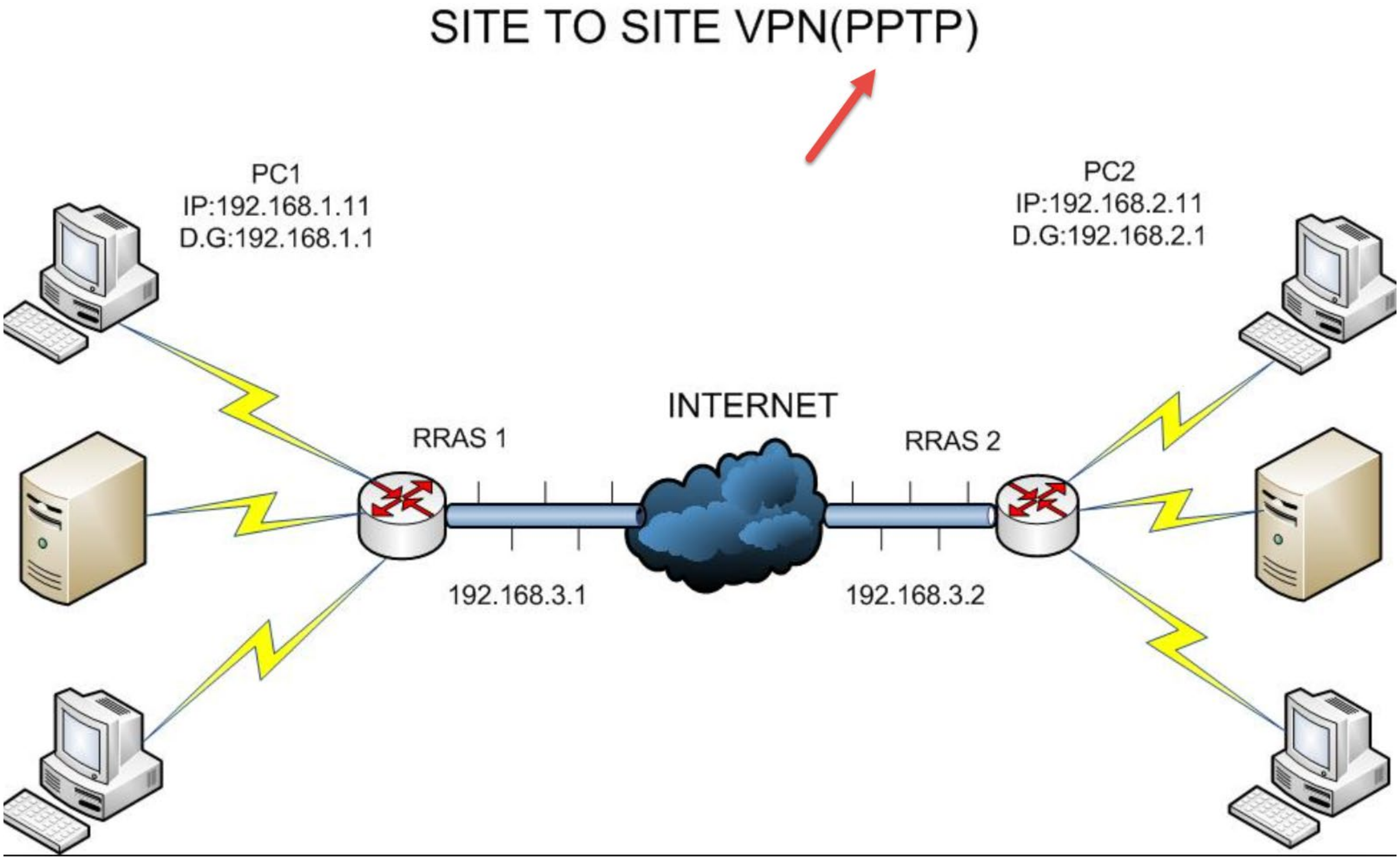
- A port is a **logical connection**. When using the Internet communications protocol, Transmission Control Protocol/Internet Protocol **(TCP/IP)**, designating a port is **the way a client program specifies a particular server program** on a **computer in a network**

- Ports range 0 – 65535

Examples:

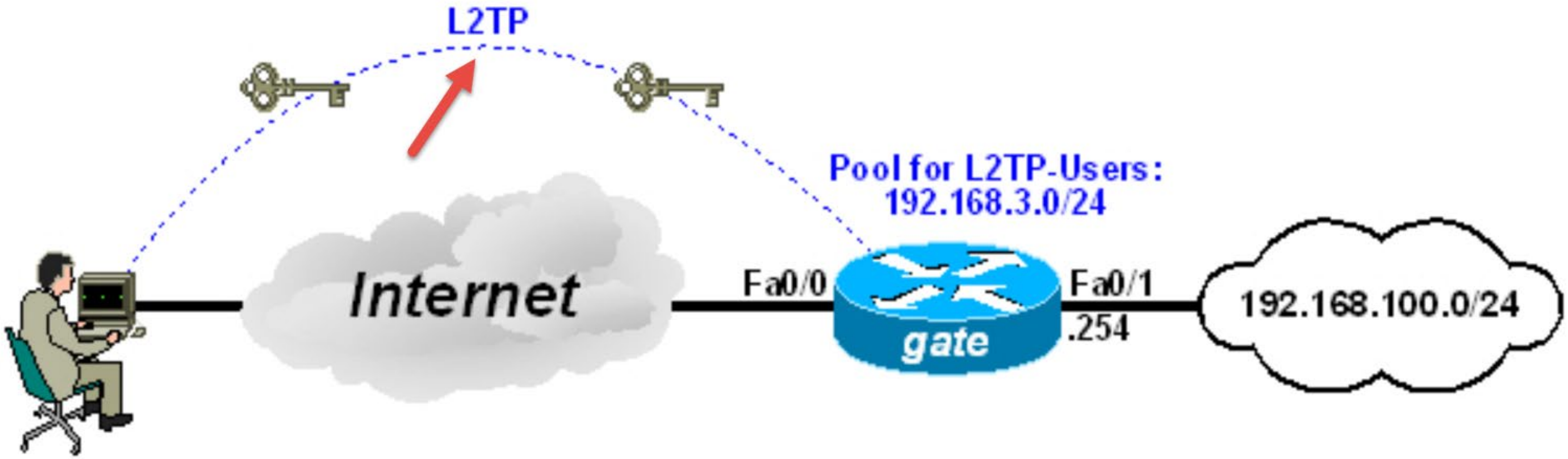
- FTP uses port 21
- HTTP uses port 80
- HTTPS uses 443

Virtual private networks

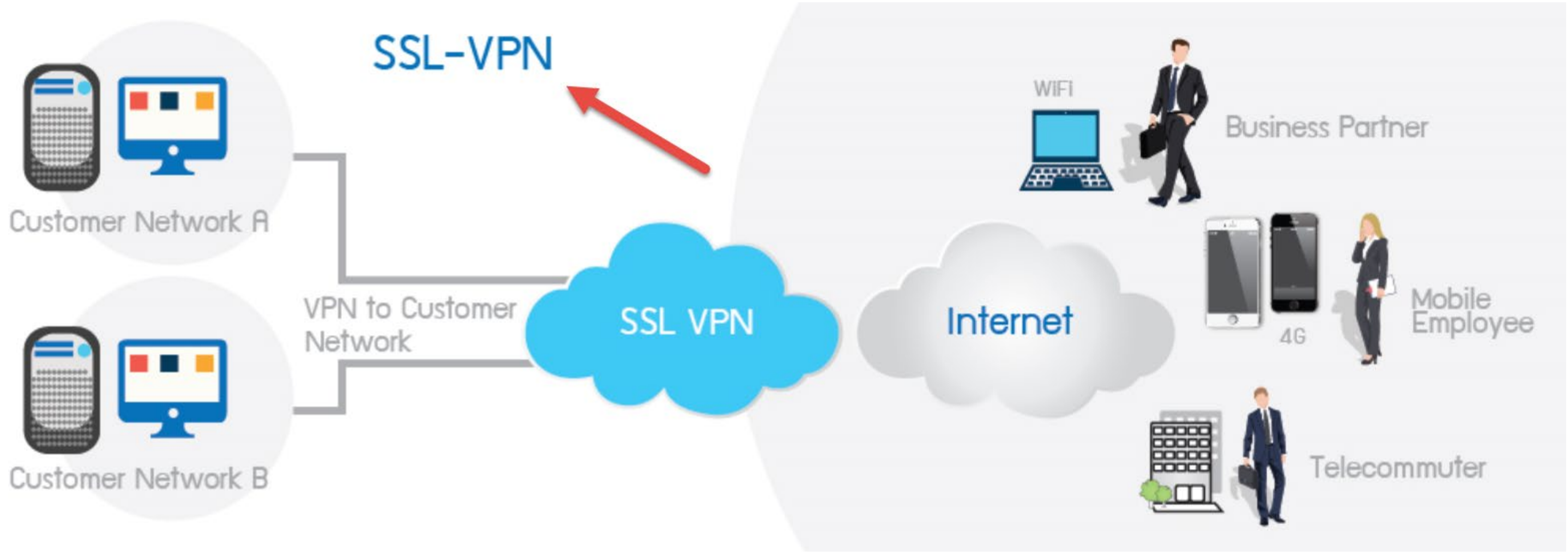


CultureLink

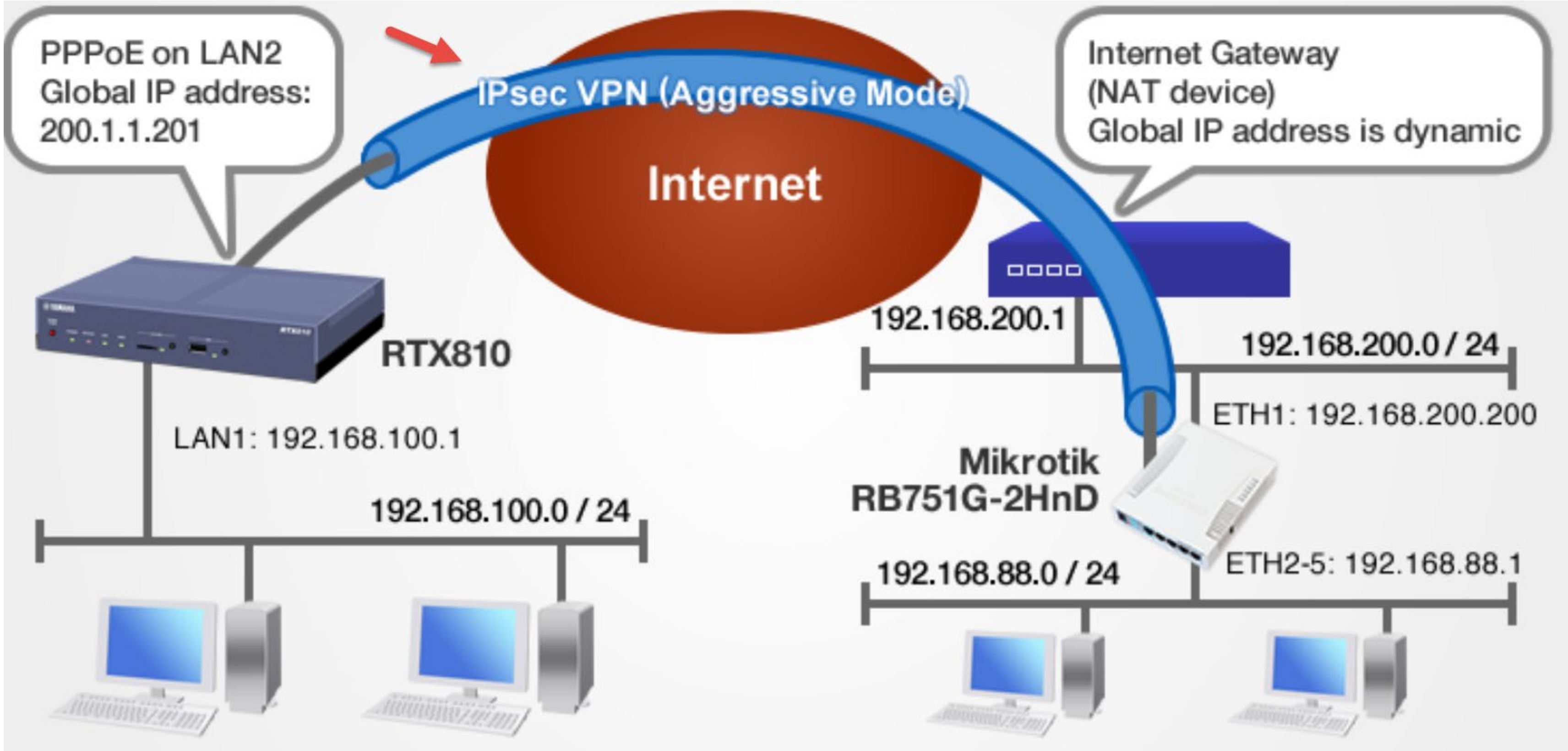
Virtual private networks



Virtual private networks



Virtual private networks



Voice-over internet protocol (VOIP)

- **Any VoIP device is an IP device**; therefore, it is vulnerable to the **same types of attacks as any other IP device.**

- DoS, or the flooding of the data network with data, is a common issue in the protection of data networks but needs to be revisited as quality of service (QoS) becomes implemented for VoIP networks. **The IP end point is often overlooked, but it can be singled out as a point of attack and flooded with data**, causing the device to reboot and eventually become unusable.

Remote access

- Employees, vendors, consultants are given remote access to the company network
- TCP/IP protocol is the cost effective approach
- VPN technologies used
- Organization should be aware that VPN connection introduce holes in security infrastructure
-

Remote access

- Employees, vendors, consultants are given remote access to the company network
- TCP/IP protocol is the cost effective approach
- VPN technologies used
- Organization should be aware that VPN connection introduce holes in security infrastructure

Remote access risks/controls

Remote Access Risks	Remote Access Controls
DoS	Policies standards
3rd party gain access to data	Proper authoraizations
Misconfigurations	Identification and authorization mechanisms
Host not secured	Encryption tools, such as VPN
Physical security issues over remote users computers	System and management (NAC)
	Restrict access to controlled systems

Any questions?

Section 4.5

Operating system security

Operating system security

System / Platform hardening:

- The process of implementing security controls
- Vendors tend to leave things “open” = vulnerabilities
- Hardening means tightening, closing holes

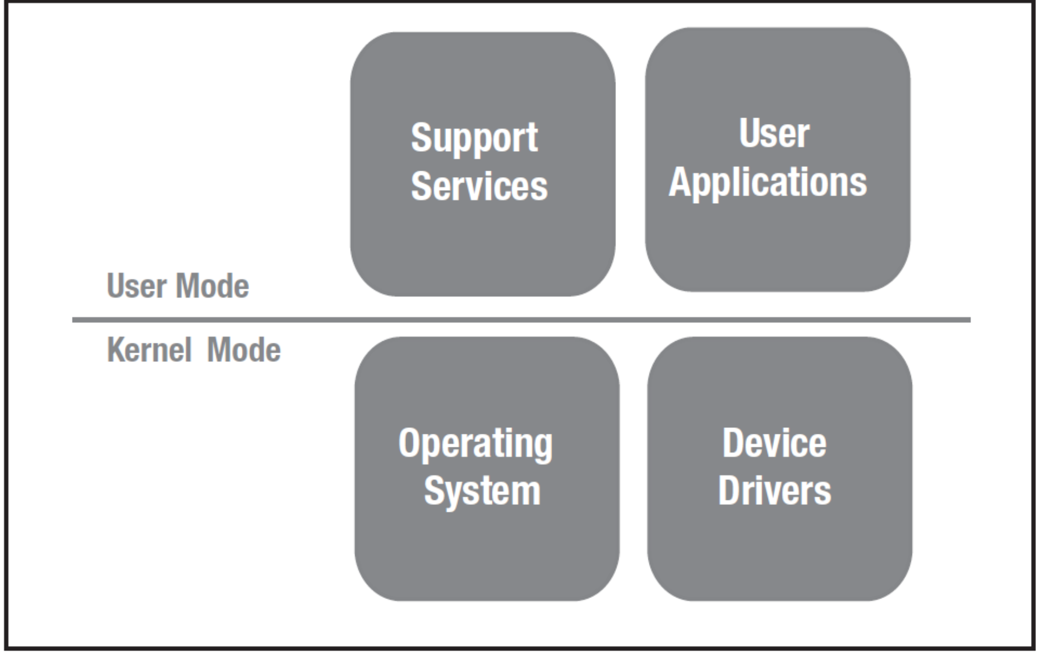
Some controls:

- Authentication and authorization
- File system permissions
- Access privileges
- Logging and system monitoring
- System services
- Configuration restrictions

Modes of operation

Operating Systems have two Modes – **User / Kernel mode**

Figure 4.9—User Mode vs. Kernel Mode

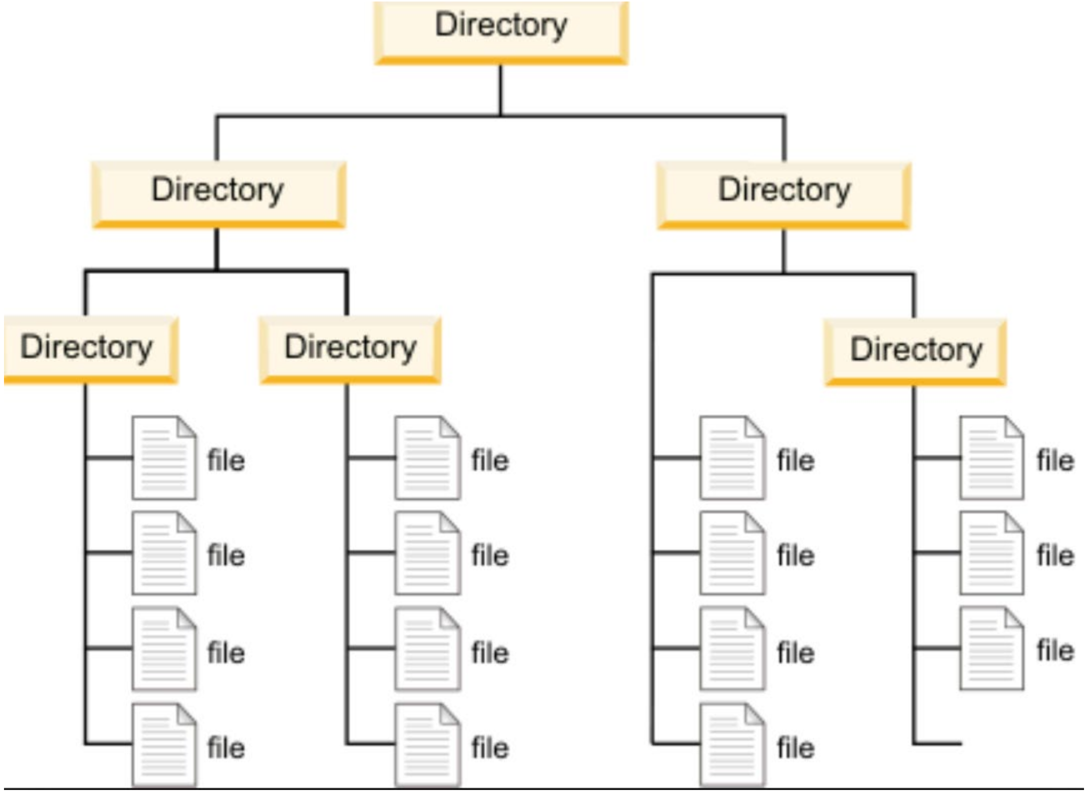


Most attacks seek to gain privileged or kernel mode access to the system in Order to circumvent security controls

File system permissions

Common file accesses include:

- File creation
- Modification
- Read
- Write
- Delete



Credential and privileges

- A users credentials define who they are and what permissions they have to access resources within the system
- Passwords are the standard mechanism to authenticate a user
- Administrator need to limit the ways in which a user access systems

Platform hardening

In UNIX, the following directories require additional consideration:

- /etc/passwd—Maintains user account and password information
- /etc/shadow—Retains the encrypted password of the corresponding account
- /etc/group—Contains group information for each account
- /etc/gshadow—Contains secure group account information
- /bin—Location of executable files
- /boot—Contains files for booting system
- /kernel—Kernel files
- /sbin—Contains executables, often for administration
- /usr—Include administrative commands

Platform hardening

For Windows, you need not look any further **than the Registry:** A central **hierarchical database** that stores configuration settings and options.63 A hive is a logical group of keys, subkeys and values in the registry that has a set of supporting files and backups of its data.64

- HKEY_CURRENT_CONFIG—Contains volatile information generated at boot
- HKEY_CURRENT_USER—Settings specific to current user
- HKEY_LOCAL_MACHINE\SAM—Holds local and domain account information
- HKEY_LOCAL_MACHINE\Security—Contains security policy referenced and enforced by kernel
- HKEY_LOCAL_MACHINE\Software—Contains software and Windows settings
- HKEY_LOCAL_MACHINE\System—Contains information about Windows system setup
- HKEY_USERS\.DEFAULT—Profile for Local System account

Most of the supporting files for the hives are in the SystemRoot%\System32\Config directory. These files are updated each time a user logs on

Unix commands

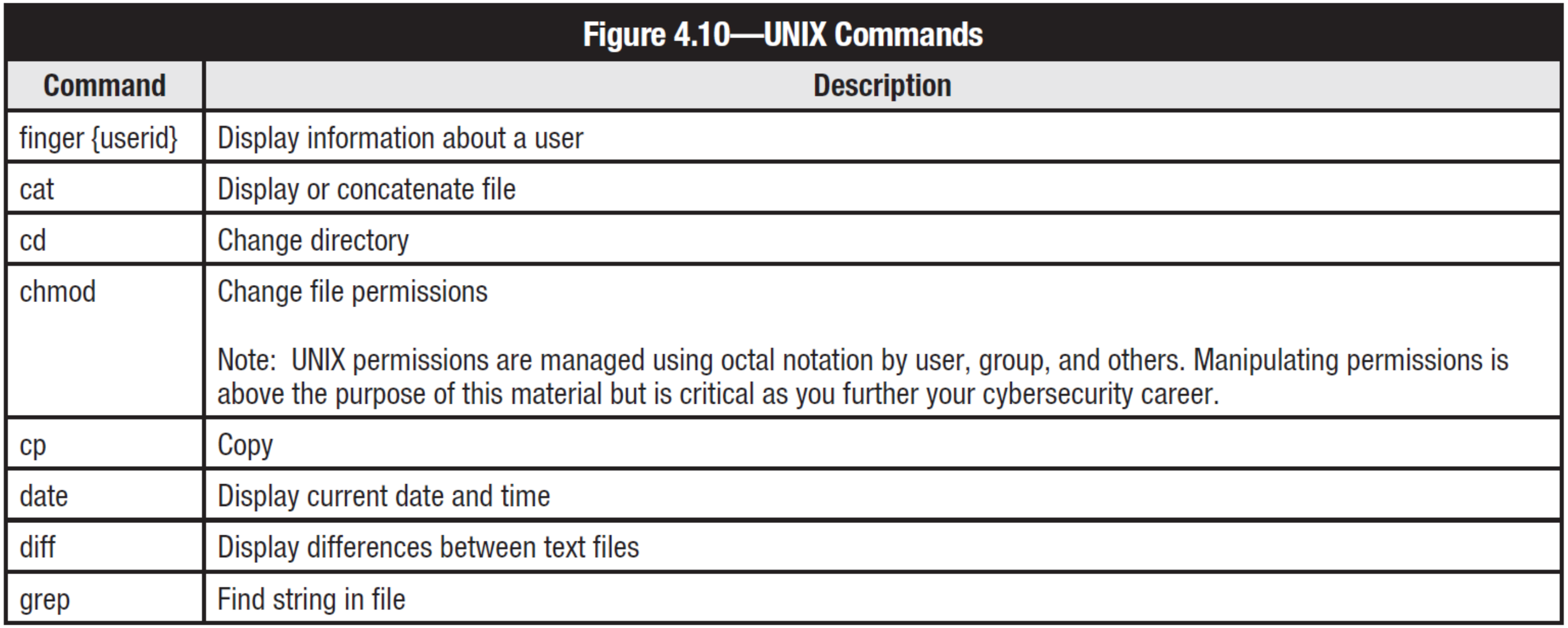


Figure 4.10—UNIX Commands

Command	Description
finger {userid}	Display information about a user
cat	Display or concatenate file
cd	Change directory
chmod	Change file permissions Note: UNIX permissions are managed using octal notation by user, group, and others. Manipulating permissions is above the purpose of this material but is critical as you further your cybersecurity career.
cp	Copy
date	Display current date and time
diff	Display differences between text files
grep	Find string in file

Virtualization

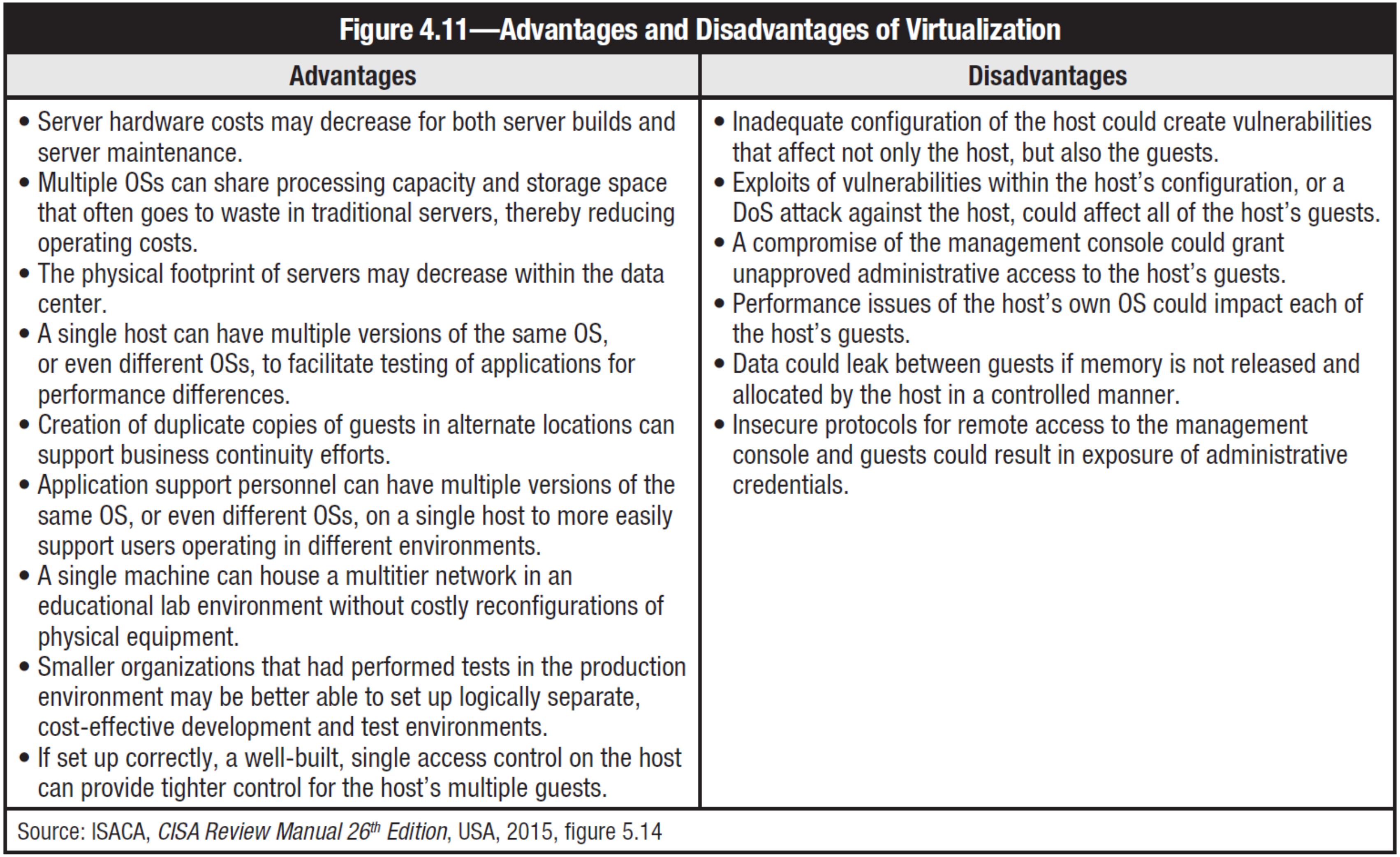


Figure 4.11—Advantages and Disadvantages of Virtualization

Advantages	Disadvantages
• Server hardware costs may decrease for both server builds and server maintenance. • Multiple OSs can share processing capacity and storage space that often goes to waste in traditional servers, thereby reducing operating costs. • The physical footprint of servers may decrease within the data center. • A single host can have multiple versions of the same OS, or even different OSs, to facilitate testing of applications for performance differences. • Creation of duplicate copies of guests in alternate locations can support business continuity efforts. • Application support personnel can have multiple versions of the same OS, or even different OSs, on a single host to more easily support users operating in different environments. • A single machine can house a multitier network in an educational lab environment without costly reconfigurations of physical equipment. • Smaller organizations that had performed tests in the production environment may be better able to set up logically separate, cost-effective development and test environments. • If set up correctly, a well-built, single access control on the host can provide tighter control for the host's multiple guests.	• Inadequate configuration of the host could create vulnerabilities that affect not only the host, but also the guests. • Exploits of vulnerabilities within the host's configuration, or a DoS attack against the host, could affect all of the host's guests. • A compromise of the management console could grant unapproved administrative access to the host's guests. • Performance issues of the host's own OS could impact each of the host's guests. • Data could leak between guests if memory is not released and allocated by the host in a controlled manner. • Insecure protocols for remote access to the management console and guests could result in exposure of administrative credentials.

Source: ISACA, *CISA Review Manual 26th Edition*, USA, 2015, figure 5.14

https://www.youtube.com/watch?v=iBI31dmqSX0

Any questions?

Section 4.6

Application security

Application security

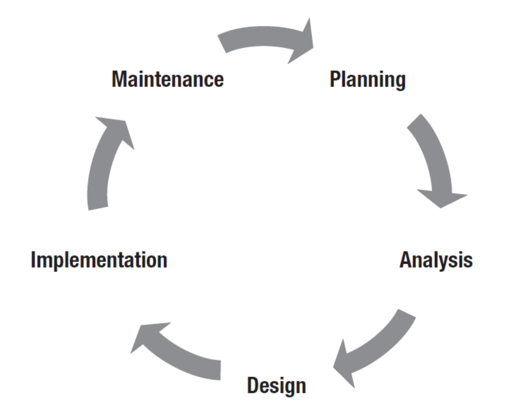
Why is application security important?

- Insecure application open holes to attackers
- Access, steal, modify sensitive information

How do you manage application security?

- Establish a framework SDLC

Figure 4.12—SDLC Process



Source: National Institute of Standards and Technology (NIST), Special Publication (SP) 800-64 Revision 2, *Security Considerations in the System Development Life Cycle*, USA, October 2008

Security with SDLC

- **Business requirements** containing descriptions of what a system should do
- **Functional requirements** and the use of case models describing how users will interact with a system
- **Technical requirements**, design specifications and coding specifications describing how the system will interact, conditions under which the system will operate and the information criteria that the system should meet
- **Risk mitigation and control requirements** to protect the integrity of the system, confidentiality of information stored, processed or communicated as well as adequate authentication and authorization mechanisms

OWASP

- The **Open Web Application Security Project is an online community** that produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security.

- Top 10 application concerns - 2017
  - https://www.owasp.org/index.php/Top_10-2017_Top_10

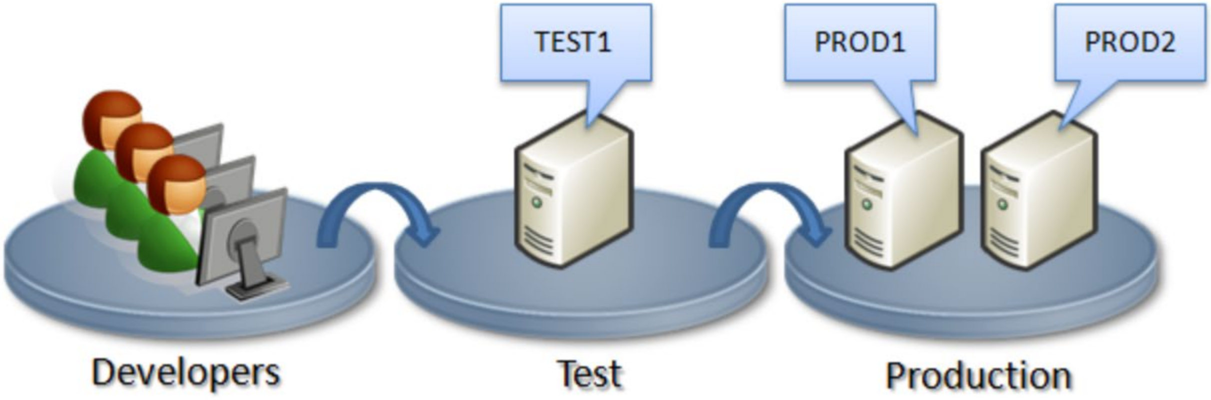
- Injection
- Broken authentication
- Sensitive data exposure
- XML External entities
- Broken access list
- Security misconfiguration

Few examples

Development, testing, production environments

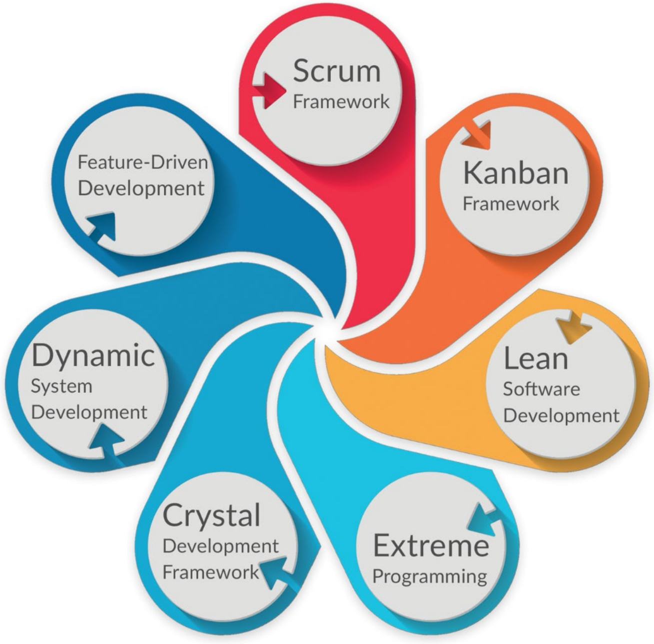
Recommendations:

- **KEEP THEM SEPARATE**
- Production data used in test, private or personal environment should be scrambled, so condifential data is not disclosed



Agile development

- Agile allows for projects, including software development, to be built in a more flexible, iterative fashion in order to respond more quickly to changes that occur during a project.



Types of agile frameworks

Reference

- https://medium.com/innodev/agile-development-for-dummies-dd161da253c7

Additional threats

- Important to keep on top
- Read, keep learning
- Get to know what the cyber risk the industry is facing
- Continue to network with industry peers and enthusiast
- Source out good organizations that are in-tune with cybersecurity and current threats

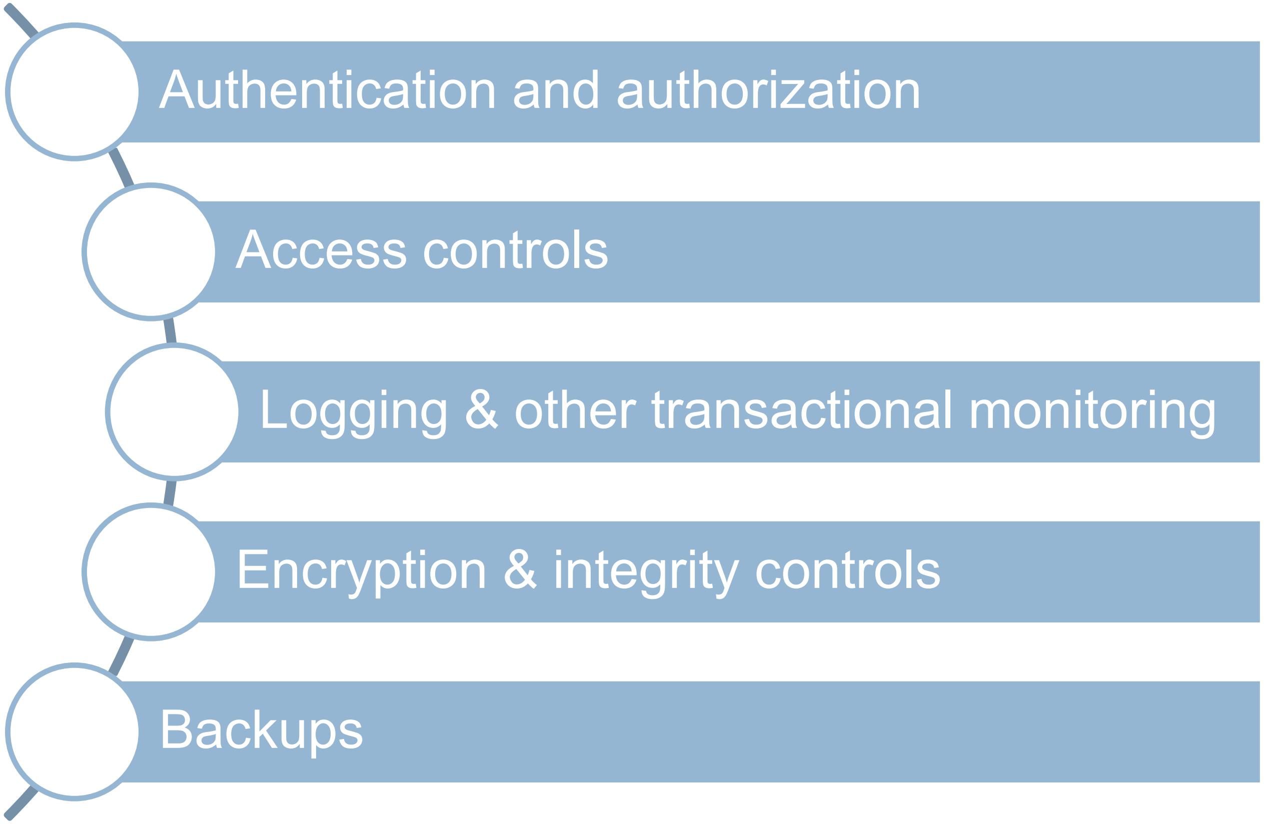
Any questions?

Section 4.7

Data security

Data security

- Databases can be individually protected with control that is similar to protections applied at the system level



Authentication and authorization

Access controls

Logging & other transactional monitoring

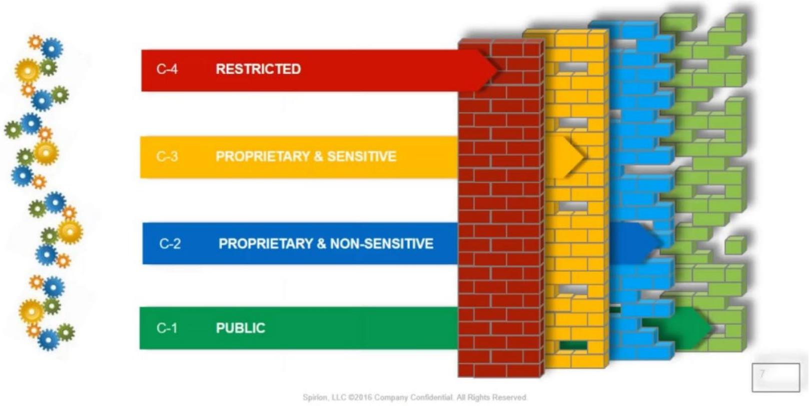
Encryption & integrity controls

Backups

CultureLink

Data classification

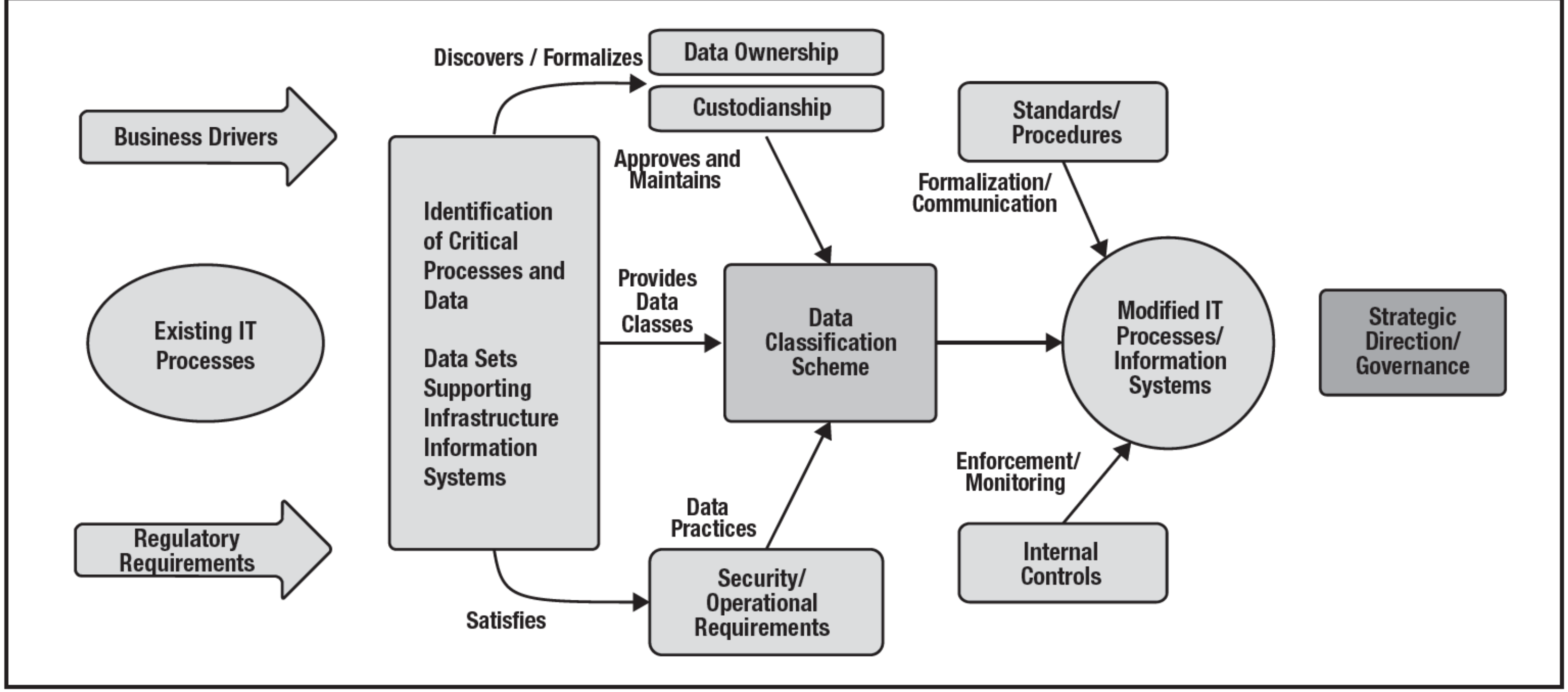
- In order to protect assets (data / information), it needs to be classified
- The business needs to understand its value and the impact it can have if it is threatened
- Sensitivity, impact and loss is considered
- Helps with backup strategies
- Don’t carry too many classifications labels, hard to manage



Spirion, LLC ©2016 Company Confidential. All Rights Reserved

Database owners

Figure 4.14—Data Classification Process



Discovers / Formalizes
Data Ownership
Custodianship
Business Drivers
Standards/ Procedures
Approves and Maintains
Formalization/ Communication
Identification of Critical Processes and Data
Data Sets Supporting Infrastructure Information Systems
Existing IT Processes
Provides Data Classes
Data Classification Scheme
Modified IT Processes/ Information Systems
Strategic Direction/ Governance
Enforcement/ Monitoring
Data Practices
Regulatory Requirements
Internal Controls
Security/ Operational Requirements
Satisfies

Database owners - classification

Classification data to be considered:

- **Access and authentication**—Determine access requirements including defining users profiles, access approval criteria and validation procedures
- **Confidentiality**—Determine where sensitive data are stored and how they are transmitted
- **Privacy**—Use controls to warn an affected user that his or her information is about to be used
- **Availability**—Determine the uptime and downtime tolerances for different data types.
- **Ownership and distribution**—Establish procedures to protect data from unauthorized copy and distribution
- **Integrity**—Protect data from unauthorized changes using change control procedures and automated monitoring and detection for unauthorized changes and manipulation
- **Data retention**—Determine retention periods and preserve specific versions of software, hardware, authentication credentials and encryption keys to ensure availability
- **Auditability**—Keep track of access, authorizations, changes and transactions

Any questions?

Thank You