CompTIA Security+

Governance, Risk, and Compliance

Domain 5 – 14%

CyberProtex

1

Security Controls

Administrative, technical, and physical controls should work in a synergistic manner to protect a company's assets

Administrative	Policies/procedures including onboarding, off boarding, and backup media
Technical	Hardware, software, firewall, active directory, authentication, and disk encryption
Physical	Doors, locks, fences, and cameras

CyberProtex

2

Security and Risk Frameworks

COBIT

Created by Information Systems Audit and Control Association (ISACA) with IT Governance to assist businesses develop, organize and implement operating procedure. COBIT can be used at the highest level of IT governance, providing an overall control framework based on an IT process model including security, risk management and information governance

ISO 27000 Series

A family of international standards developed by International Organization for Standardization/International Electric Technical Commission for managing sensitive company information. It contains 133 detailed information security controls based upon 11 focus areas. The guidelines provide a roadmap to meet ISO certification. The 2014 published ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements, which helps manage cybersecurity.

NIST SP 800 Series

National Institute of Standards and Technology (NIST) series is a set of documents that provide the structure for policies, procedures, and guidelines for federal government assets. Each series covers a specific area concentration including NIST SP 800-30 focuses on Information System Risk Management, NIST SP 800-39 focuses on organizational risk management, and NIST SP 800-66 was written specifically for HIPPA.

RMF

The Risk Management Framework (RMF) associated with the NIST SP 800-37 guide for "Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," which has been available for Federal Information Security Management Act (FISMA) compliance since 2004.

CyberProtex

Frameworks

Framework	Description
Total Quality Management	A structured approach to improve the quality of good and services through continuous improvement of internal practices
ISO	Code of practice for information security management
ITIL	Set of best practices for IT service management
COSO	Managing internal risks by identifying relevant vulnerabilities and determining impact

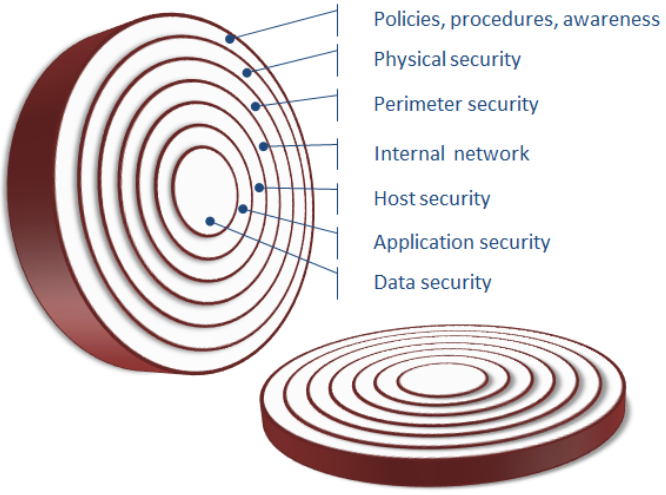
CyberProtex

Frameworks

Framework	Description
COBIT	Sets control points are used by organizations meeting Sarbanes-Oxley Act
Six Sigma	A disciplined, statistical-based, data-driven approached for eliminating risks and establishing continuous improvement
CMMI	Capability Maturity Model Integration used to guide process improvement across a project - Initial, Managed, Defined, Quantitatively Managed, and Optimizing
Basel II	International business standard that requires financial institutions to maintain reserves to cover risks

CyberProtex

Defense in Depth



When dealing with threats, the assumption should always be that any layer can be violated. Thus, protection must be provided by the sequential layers.

Image courtesy of: Theuns, M. Layering Information Security Controls. http://www.content-loop.com/layering-information-security-controls/

CyberProtex

Laws, Directives, and Regulations

- The Sarbanes-Oxley Act (SOX)
- The Health Insurance Portability and Accountability Act (HIPAA)
- The Gramm-Leach-Bliley Act of 1999 (GLBA)
- The Computer Fraud and Abuse Act
- The Federal Privacy Act of 1974
- Payment Card Industry Data Security Standards (PCI-DSS)
- The Computer Security Act of 1987
- The Economic Espionage Act of 1996

CyberProtex

Information security education, training, and awareness

- Establish appropriate levels of awareness, training, and education required for individual organization

- Review periodically for contentrelevancy and update as needed

CyberProtex

How it Fits Together

Industry	Regulation	Audit Framework	Best Practices
Publicly Traded Company (NYSE, NASDAQ)	Sarbanes Oxley (SOX, SARBOX)	COSO, SAS70, COBIT	GAAP, ISO, CIS
Hospital, Medical	Health Insurance Portability and Accountability Act (HIPAA)	COBIT, FISCAM	ISO, CMS, NIST
Credit Card Merchant, Broker, or Clearinghouse	Payment Card Industry (PCI)	COBIT	SANS, ISO, CIS

CyberProtex

Ranking of Personnel Management

Access Control	Description	Rank	Justification
Least Privilege	Protects its most sensitive resources by ensuring that the individual should have only the necessary rights and privileges to perform her/his task	1	Easiest to implement and operating systems support available
Implicit Deny	If a situation is not covered by any of the rules, then access cannot be granted. An essential default setting for any security system. Any individual without proper authorization cannot be granted access. The alternative to implicit deny is to allow access unless a specific rule forbids it.	2	Third party software available to support, but requires forethought and is not the default setting
Separation of Duties	Term is applicable to physical environments as well as network and host security. For any given task, more than one individual is affected. A task is broken into different duties, each of which is accomplished by a separate individual.	3	Requires clean division duties and tasking not always found in small companies

CyberProtex

Ranking of Personnel Management

Access Control	Description	Rank	Justification
Job Rotation	Term defines the rotation of individuals through different tasks and duties. The rotation could occur at predetermined time intervals and prevent single point of failure	4	Requires multiple people with spin up time for training with every rotation
Mandatory Vacation	A mandatory vacation policy requires all users to take time away from work to refresh. Mandatory vacation give the employee a chance to refresh, but it also gives the company a chance to make sure that others can fill in any gaps in skills and satisfies the need to have replication or duplication at all levels. Mandatory vacations also provide an opportunity to discover fraud.	5	Requires adequate Personal Time Off (PTO) and two to three deep work force

CyberProtex

11

11

Risk Management And Assessment

- **Risk assessment**
  - ✓ **Identify assets**
  - ✓ **Identify threats**
  - ✓ **Calculating risks**
- **Qualitative and Quantitative Risk Analysis**
- **Delphi Technique**

CyberProtex

12

12

Business Impact Analysis (BIA)

- Evaluates the critical systems and functions for risks and losses (mission essential)
- Tangible and intangibles
- Calculates times you can do without
  - ✓ Maximum tolerable downtime (MTD)
    - Mean Time Between Failure (MTBF)
    - Mean Time To Failure (MTTF)
    - Mean Time To Restore (MTTR)
  - ✓ Recovery Time Objectives (RTO)
  - ✓ Recovery Point Objective (RPO)

CyberProtex

13

13

Risk Analysis

- Annualized loss expectancy (ALE)
- Annualized rate of occurrence (ARO)
- Exposure factor
- Probability
- Threat
- Safeguard
- Vulnerability

CyberProtex

14

14

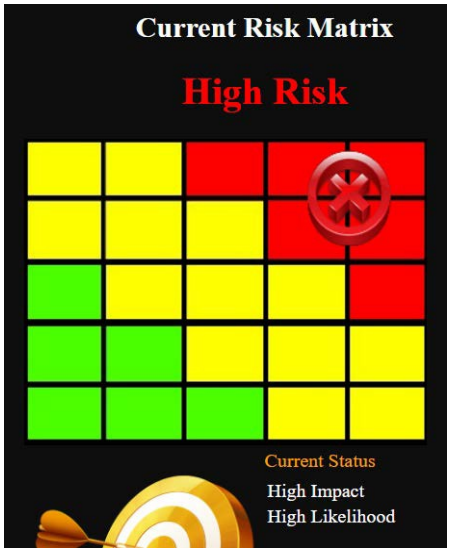
Quantitative vs Qualitative Characteristics

Attribute	Quant-itative	Qual-itative
Requires no calculations		X
Requires more complex calculations	X	
Involves high degree of guesswork		X
Provides general areas and indications of risk		X
Is easier to automate and evaluate	X	
Used in risk management performance tracking	X	
Provides credible cost/benefit analysis	X	
Uses independently verifiable and objective metrics	X	
Provides the opinions of the individuals who know the processes best		X
Shows clear-cut losses that can be accrued within one year's time	X	

Qualitative

Perform reduction analysis

HEAT MAP



Risk Assessments

- SLE x ARO = ALE
- Prioritize threats, vulnerabilities, and impact of losses
- Enumerate through each risk
- Exposure of Company
- Reality Check
  - ✓ Risk assignment/acceptance

CyberProtex

Breaking Down How SLE and ALE Values Are Used

Asset	Threat	Single Loss Expectancy (SLE)	Annualized Rate of Occurrence (ARO)	Annual Loss Expectancy (ALE)
Facility	Fire	$230,000	0.1	$23,000
Trade secret	Stolen	$40,000	0.01	$400
File server	Failed	$11,500	0.1	$1,150
Data	Virus	$6,500	1	$6,500
Customer credit card info	Stolen	$300,000	3	$900,000

CyberProtex

Security Management

- Information security policies
- Assets
- Risks
- Threats
- Cost/benefit analysis
- Security awareness

Apply risk management concepts

- Countermeasure selection
- Implementation
- Types of controls
  - ✓ Technical
  - ✓ Administrative
  - ✓ Physical
  - ✓ Deterrent
  - ✓ Preventive
  - ✓ Detective
  - ✓ Corrective
  - ✓ Compensating

Security Controls

Control	Description
Technical	Using technology to address a physical security issue
Administrative	Policy or procedure to limit a security risk
Physical	Prevents physical action
Deterrent	Discourages an attacker by reduces the likelihood of success
Preventive	Prevents a malicious action from occurring by blocking or stopping
Detective	Helps to detect any malicious activities
Corrective	Attempts to get the system back to normal and reduce damage
Compensating	Restores but does not prevent an attack

Data Sensitivity

Sensitivity Level	Description
Public	No restrictions
Private	Disclosure would cause harm or disruption to the organization
Confidential	Disclosure would cause serious harm to the organization
Proprietary	Property of the organization - trade secrets
Personally Identifiable Information (PII)	Data that can be used to identify an individual
Protected Health Information (PHI)	Health information of an individual

Detecting Risks

Internal Monitoring

- Performance monitor
- Systems monitor
- Performance baseline
- Protocol analyzers
- Vulnerability Scanning Regiment
- Continuous Diagnostics and Mitigation (CDM)

External Actions

- Third party auditors
- Penetration tests

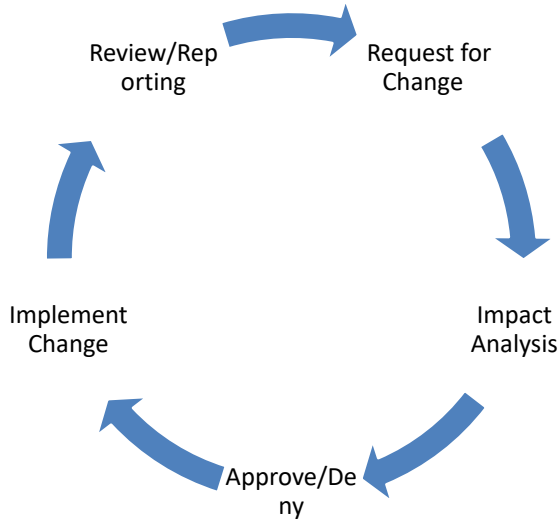
CyberProtex

Risk Responses

Action	Example
Avoid	Isolate the system, block the service or port
Transference	Insurance or use a third party
Acceptance	System owner and/or executive owner assumes responsibility
Mitigation	Compensating controls and Plan of Action and Milestone (POA&M)

CyberProtex

Mitigation Leads to Change Management



Critical elements:

- What is the change (software, hardware, firewall…)
- What is the impact on landscape
- Clear procedures to make request and validate the change

CyberProtex

Incident Response

Step	Description
Preparation	Establishes the foundation - train employees on roles and responsibilities, drill scenarios, review plan yearly
Detection	Process to determine if breached - when did it occur, how was it discovered, who discovered, impact to landscape, scope, and source
Containment	Contain impacted area
Eradication	Mitigation phase which analyzes the incident including determining the root cause. Final step is to prevent the future impact
Recovery	Return to normal operations
Lesson Learned	Document

CyberProtex

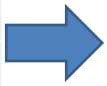
Image courtesy of: https://blog.e-janco.com/2012/08/09/feds-issue-a-computer-security-incident-handling-guide/

Business Continuity

Contingency Plan Test
- Tabletop

Recovery Site

Cold	No hardware, no data, no employees
Warm	Limited setup, empty rack space, no data
Hot	Replica or operational setup, hardware and applications replicated and up to date



Failover Site
- Prepare recovery site
- Disaster is declared
- Address disaster
- Return to normal operations site

Business Continuity Backup Strategies

Type	Data Selection	Archive Attribute
Full	All data	Cleared
Differential	Contains all combined file changes since the last full backup	Not cleared
Incremental	Contains all the changed files since the last backup (no matter which level)	Cleared

Backup Type	Backup Time	Restore Time	Storage Space
Full	Slowest	Fast	High
Differential	Moderate	Fast	Moderate
Incremental	Fast	Moderate	Lowest