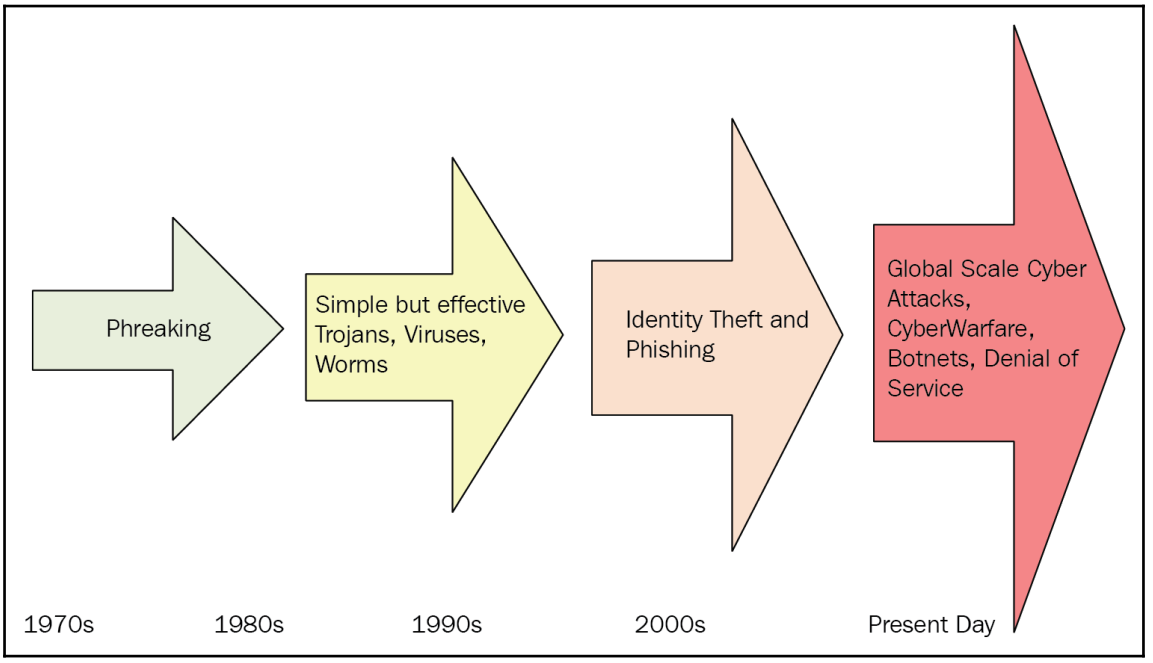
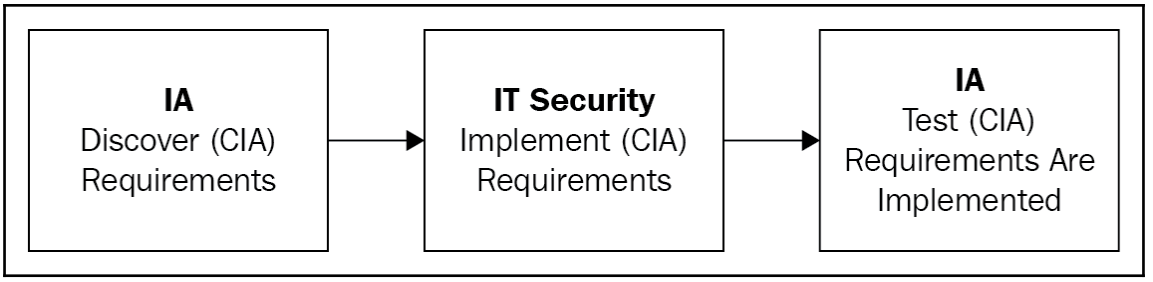
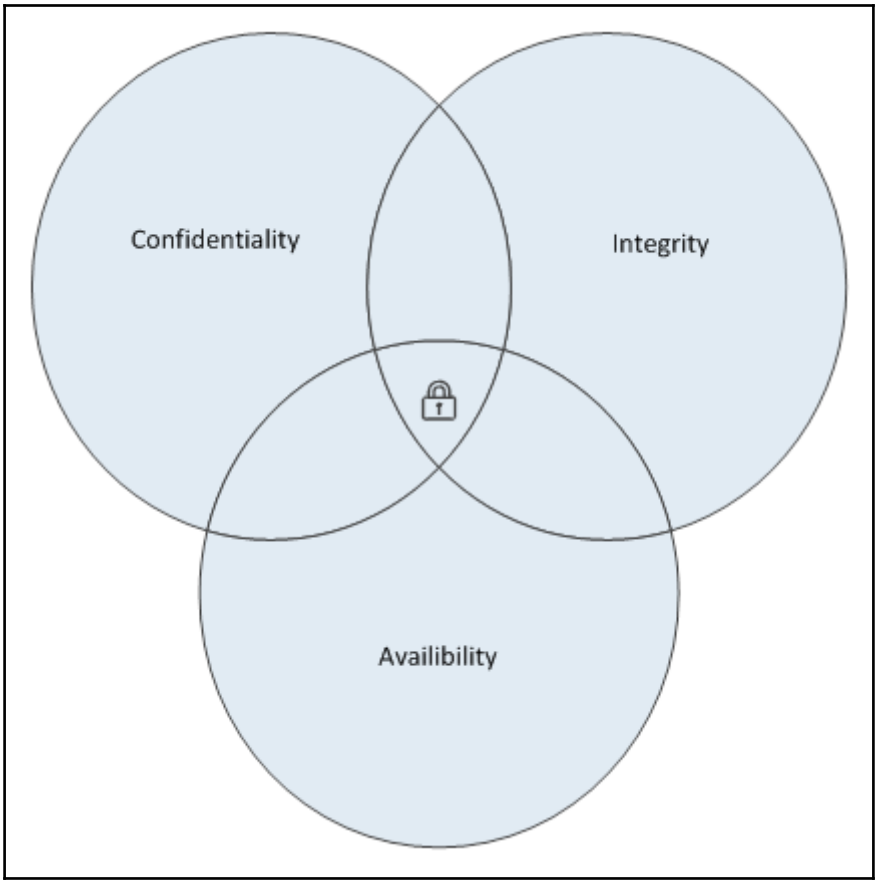
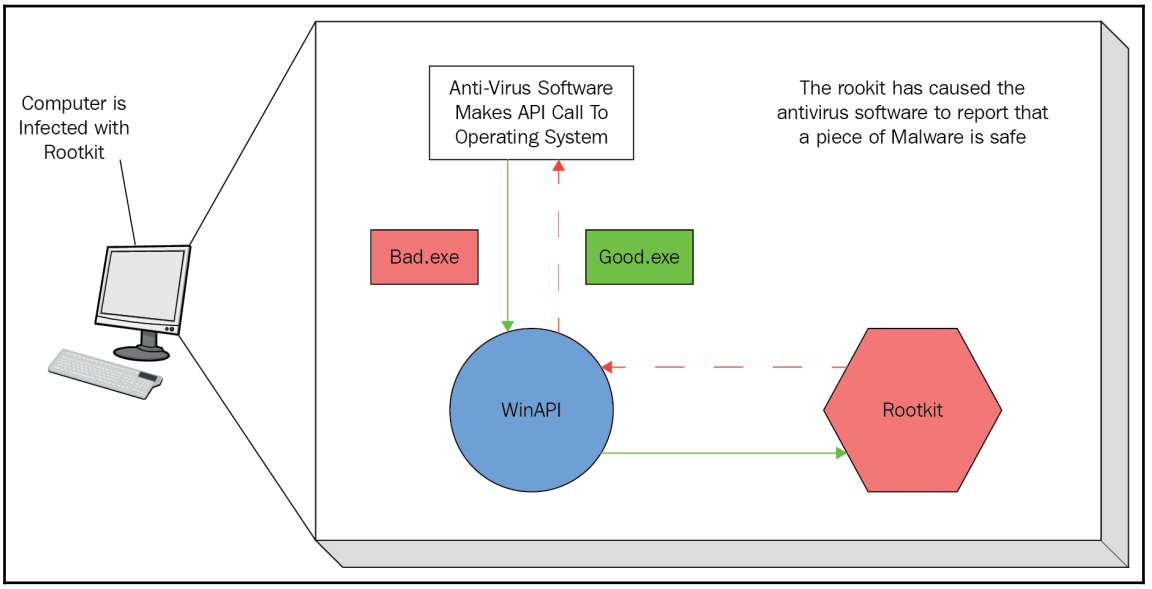
Chapter 1: Information and Data Security Fundamentals

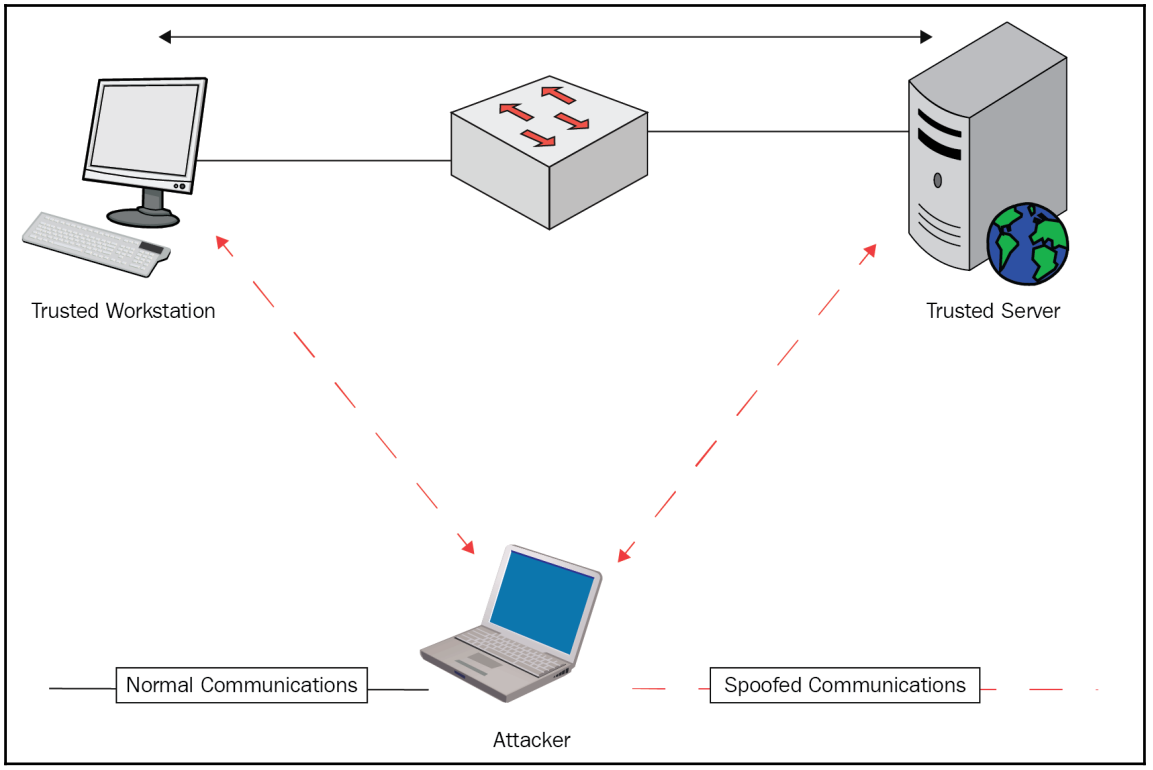


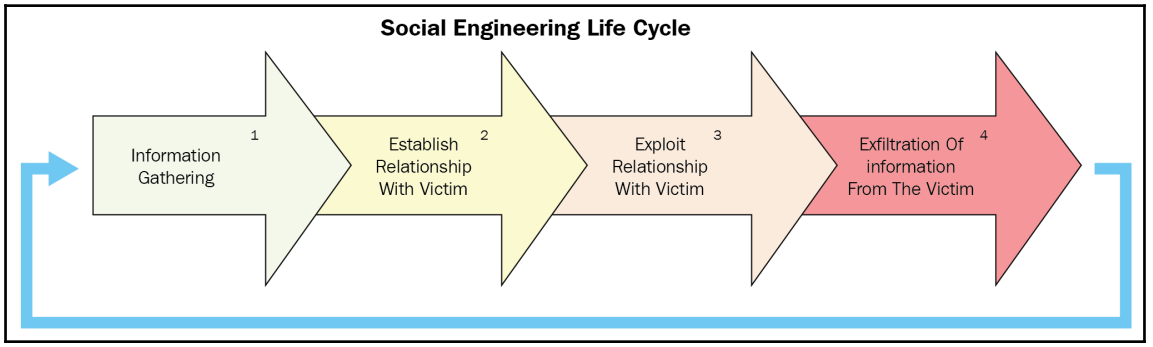


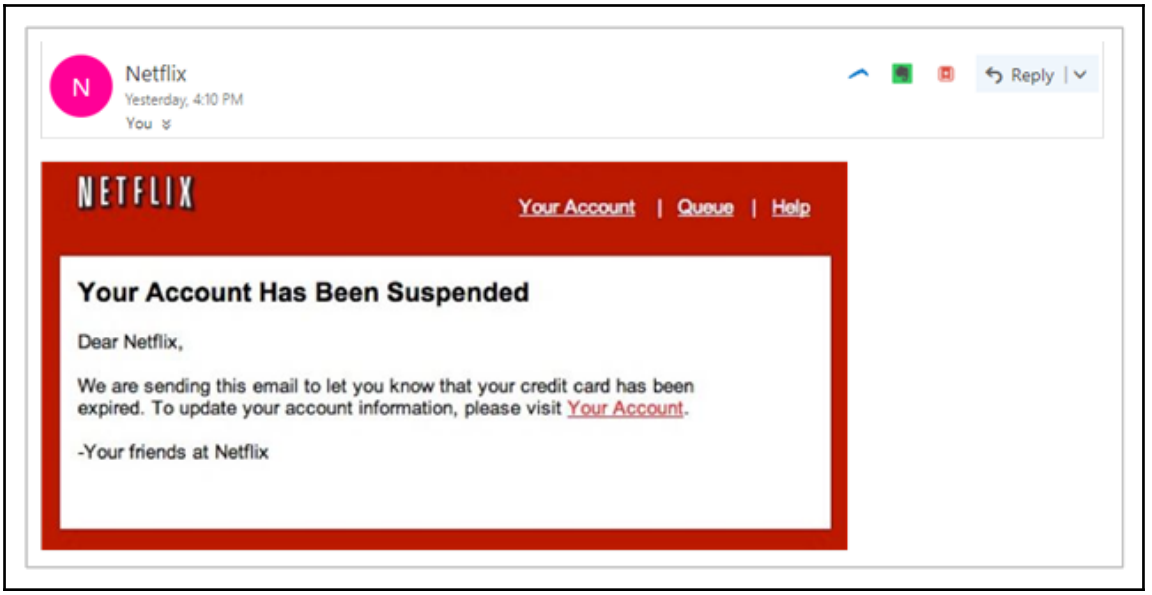

Confidentiality
Integrity
Availibility

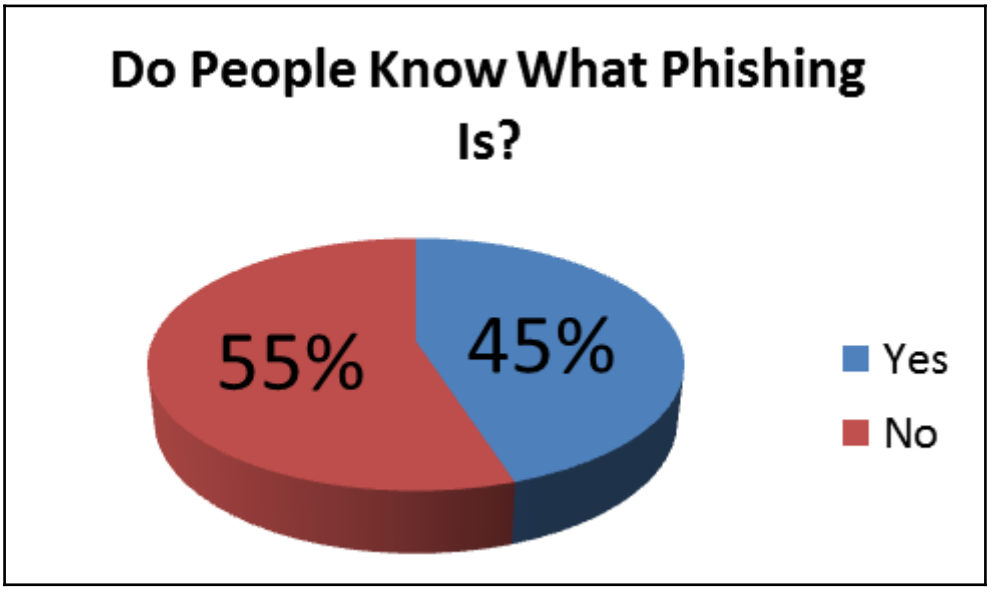
Chapter 2: Defining the Threat Landscape



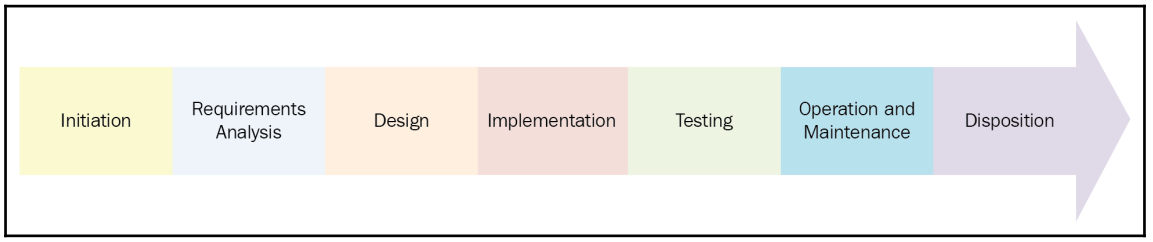

Trusted Workstation
Trusted Server
Normal Communications
Spoofed Communications
Attacker

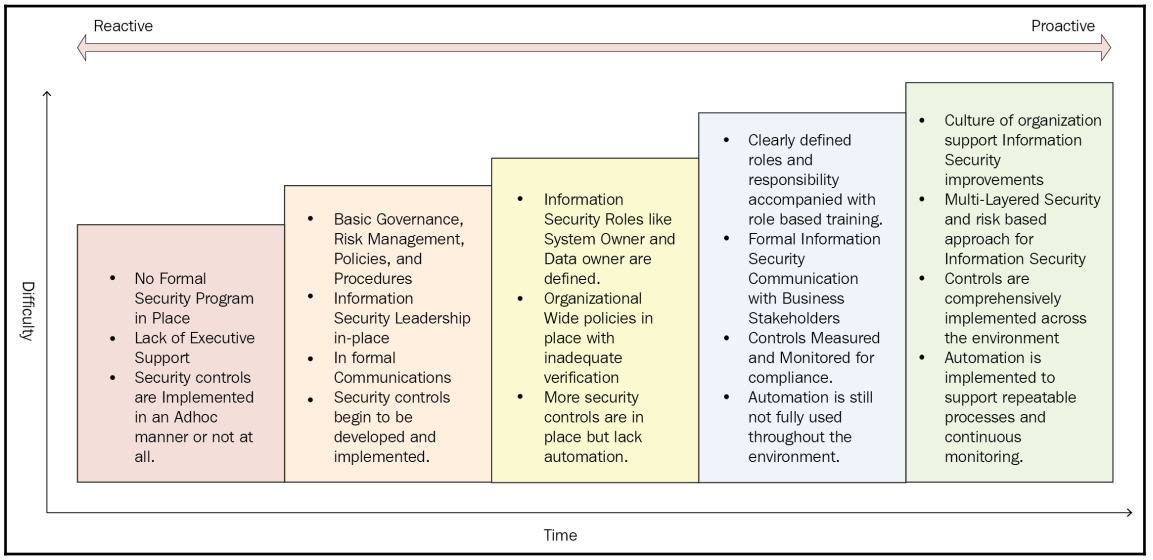

Social Engineering Life Cycle
1
Information Gathering
2
Establish Relationship With Victim
3
Exploit Relationship With Victim
4
Exfiltration Of information From The Victim

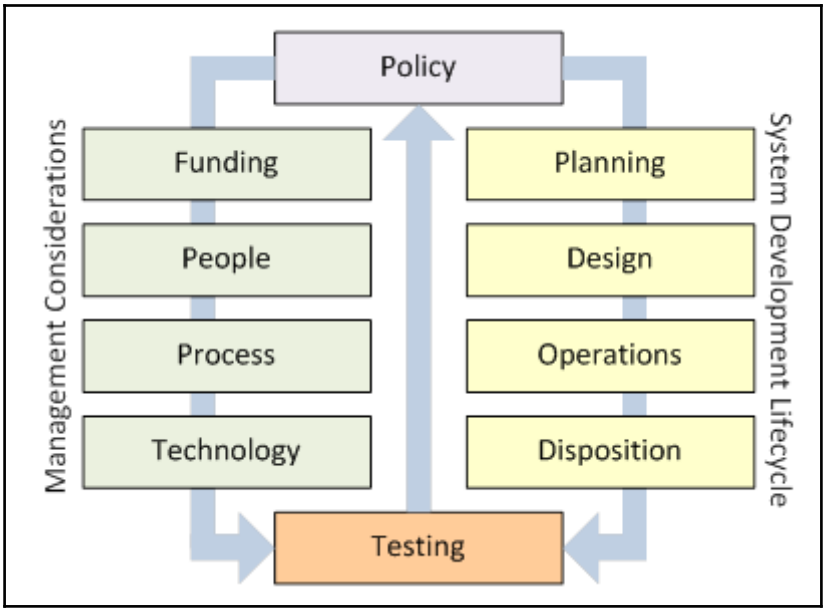

N
Netflix
Yesterday, 4:10 PM
You
Reply
NETFLIX
Your Account | Queue | Help
Your Account Has Been Suspended
Dear Netflix,
We are sending this email to let you know that your credit card has been expired. To update your account information, please visit Your Account.
-Your friends at Netflix

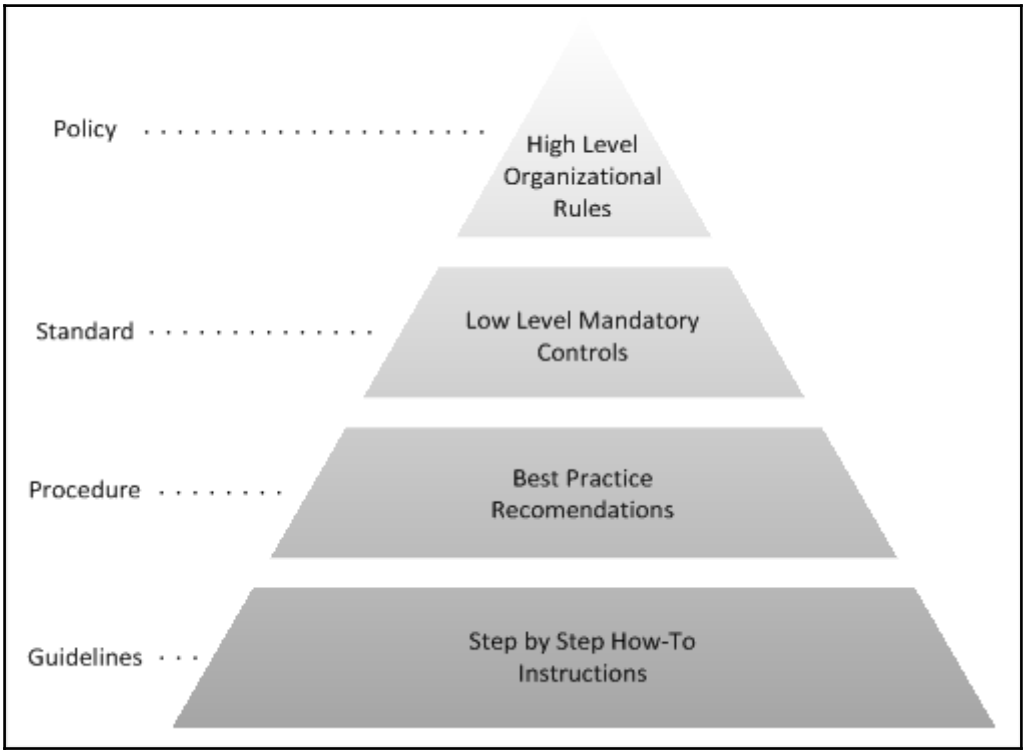

Do People Know What Phishing Is?
55%
45%
Yes
No

Chapter 3: Preparing for Information and Data Security



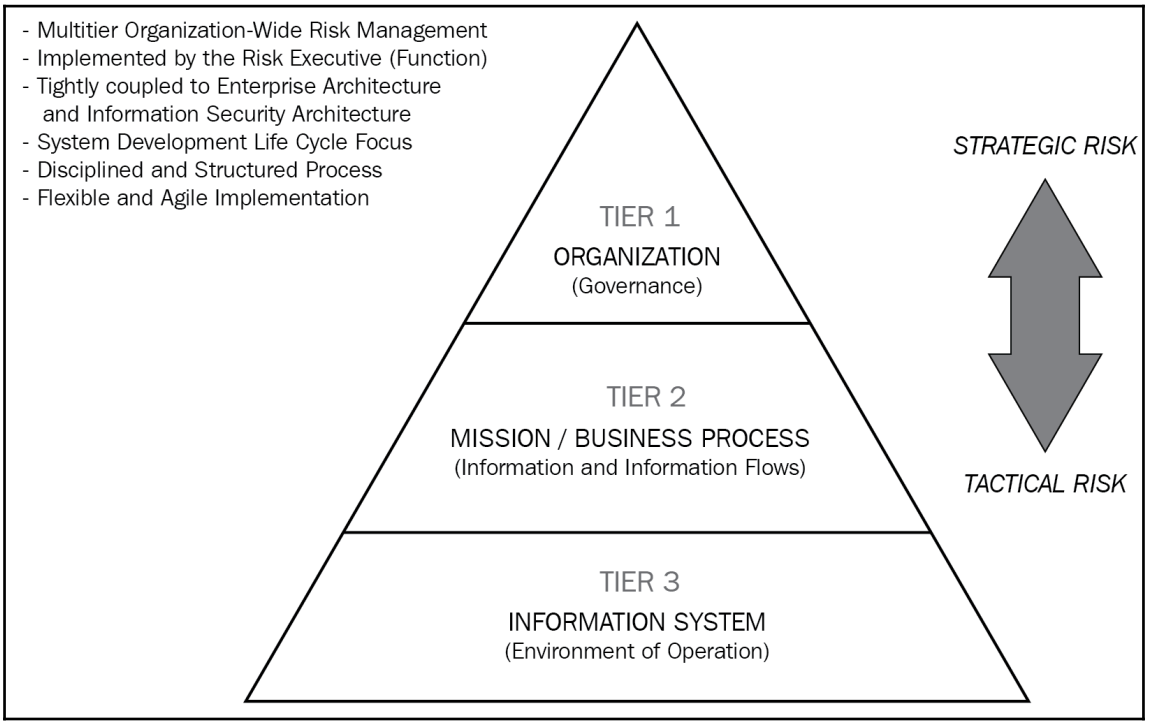


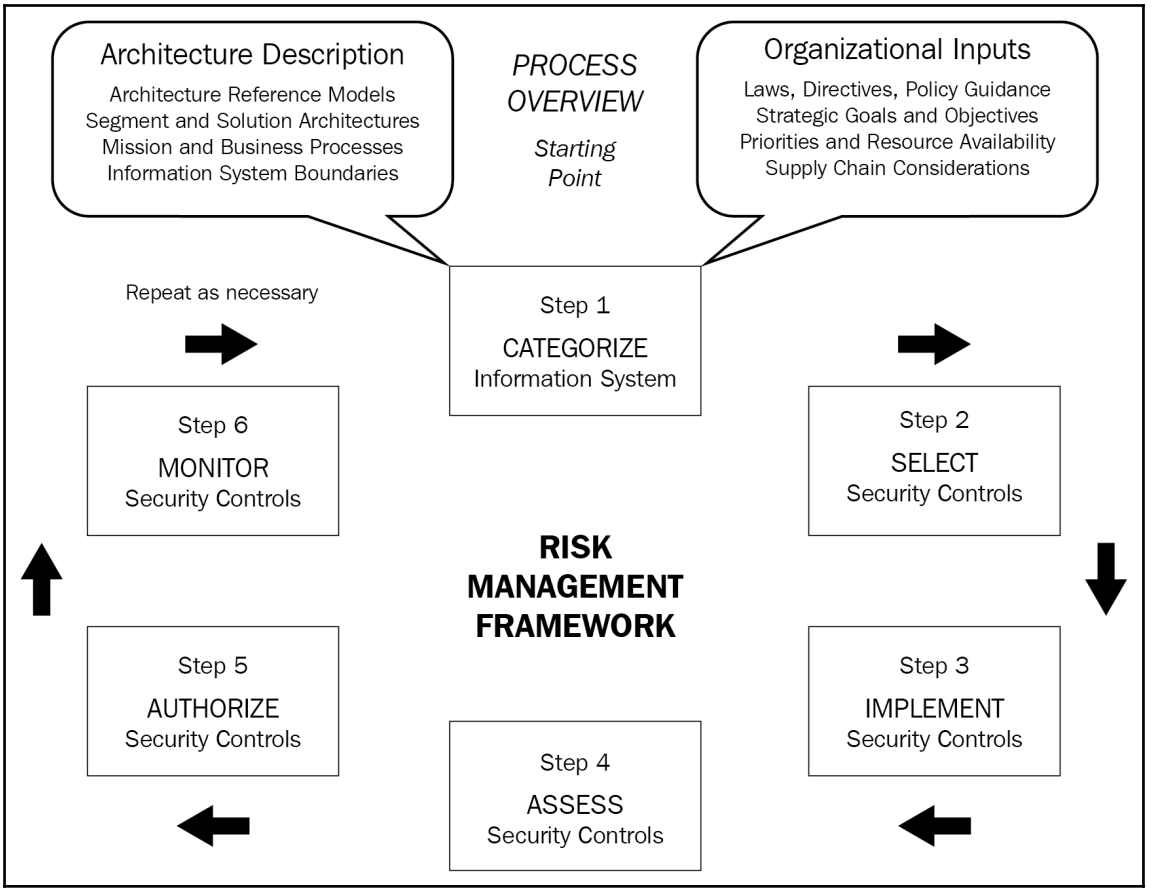

Policy
Funding
People
Process
Technology
Planning
Design
Operations
Disposition
Testing
Management Considerations
System Development Lifecycle

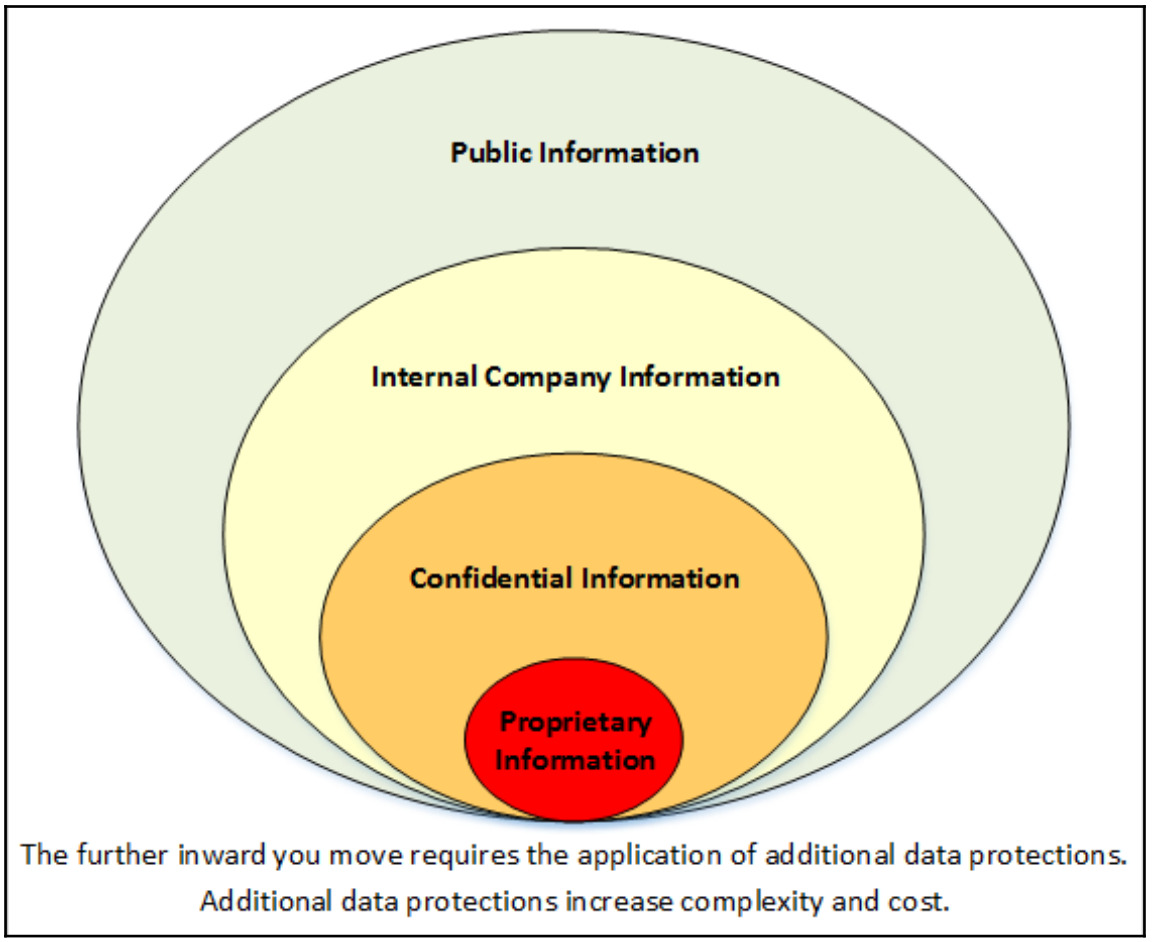

Policy
High Level Organizational Rules
Standard
Low Level Mandatory Controls
Procedure
Best Practice Recomendations
Guidelines
Step by Step How-To Instructions

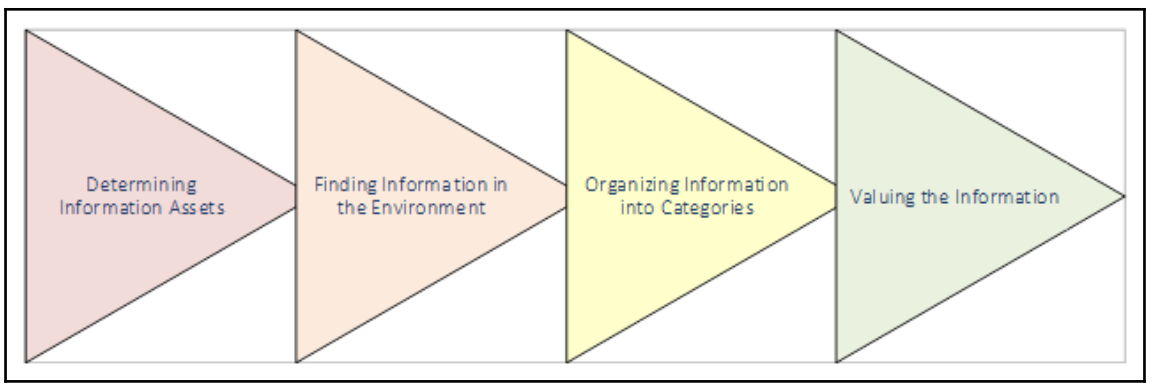
Policy Area	Policy Families	Policy Topic Examples
Technical	Access Control Audit and Accountability Identification and Authentication System and Communications Protection	Account Management End User Device Security Server Security Controls Network Security Controls Web Based Application Controls
Management	Planning Risk Assessment Security Assessment Systems and Services Acquisitions	Information Security Program Establishment of Official Roles Information Security Metrics Conducting Risk Assessments Vulnerability Scanning Penetration Testing Account Rights Reviews
Operational	Awareness and Training Configuration Management Contingency Planning Incident Response Maintenance Media Protection Personnel Security Physical and Environmental Protection System and Information Integrity	Training Topics Expected and Prohibited Behavior Employee Screening Account Termination Business Continuity Planning Disaster Recovery Incident Response Planning Workplace Security Removable Device Security Sensitive Data Security

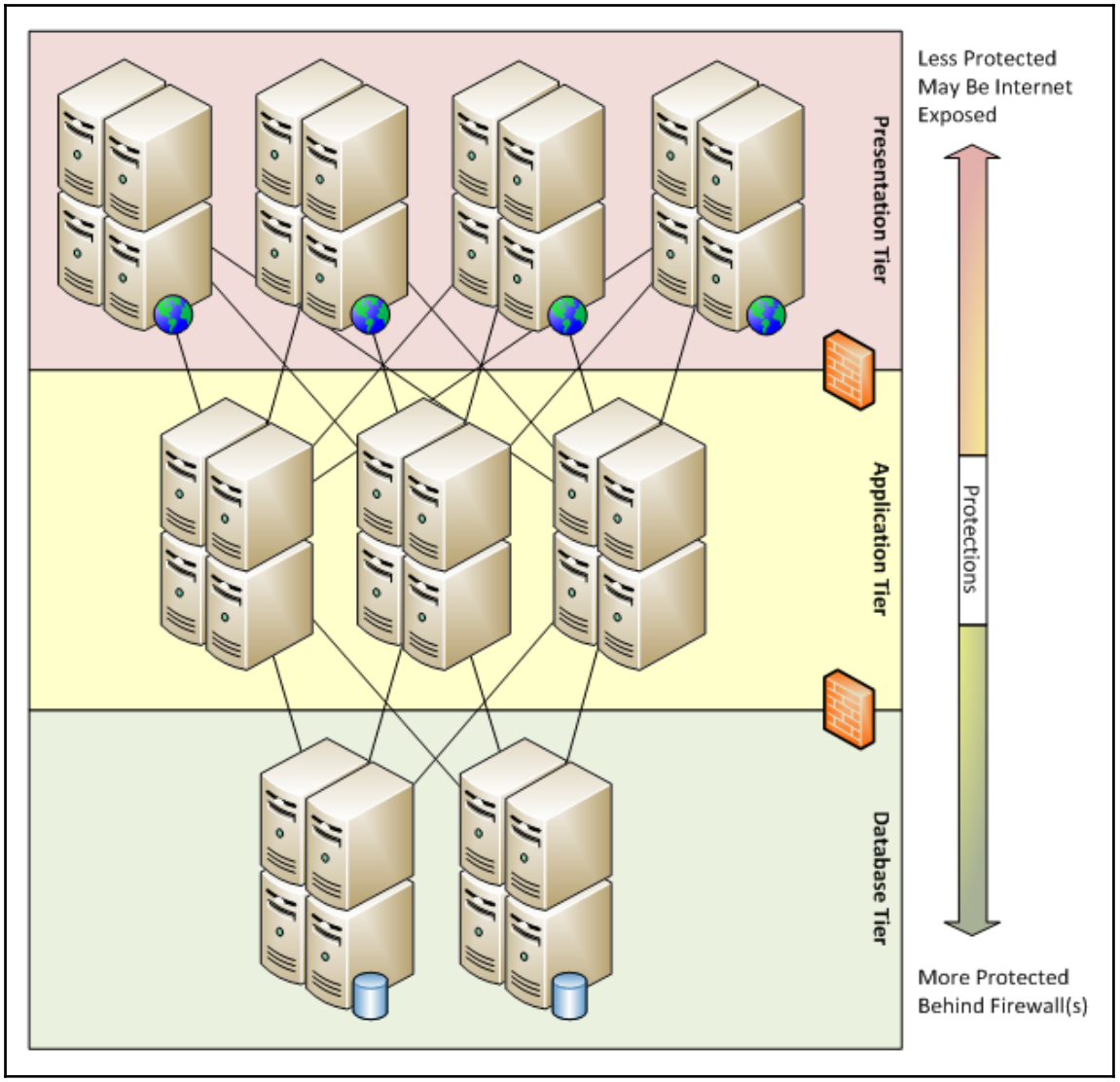
Chapter 4: Information Security Risk Management

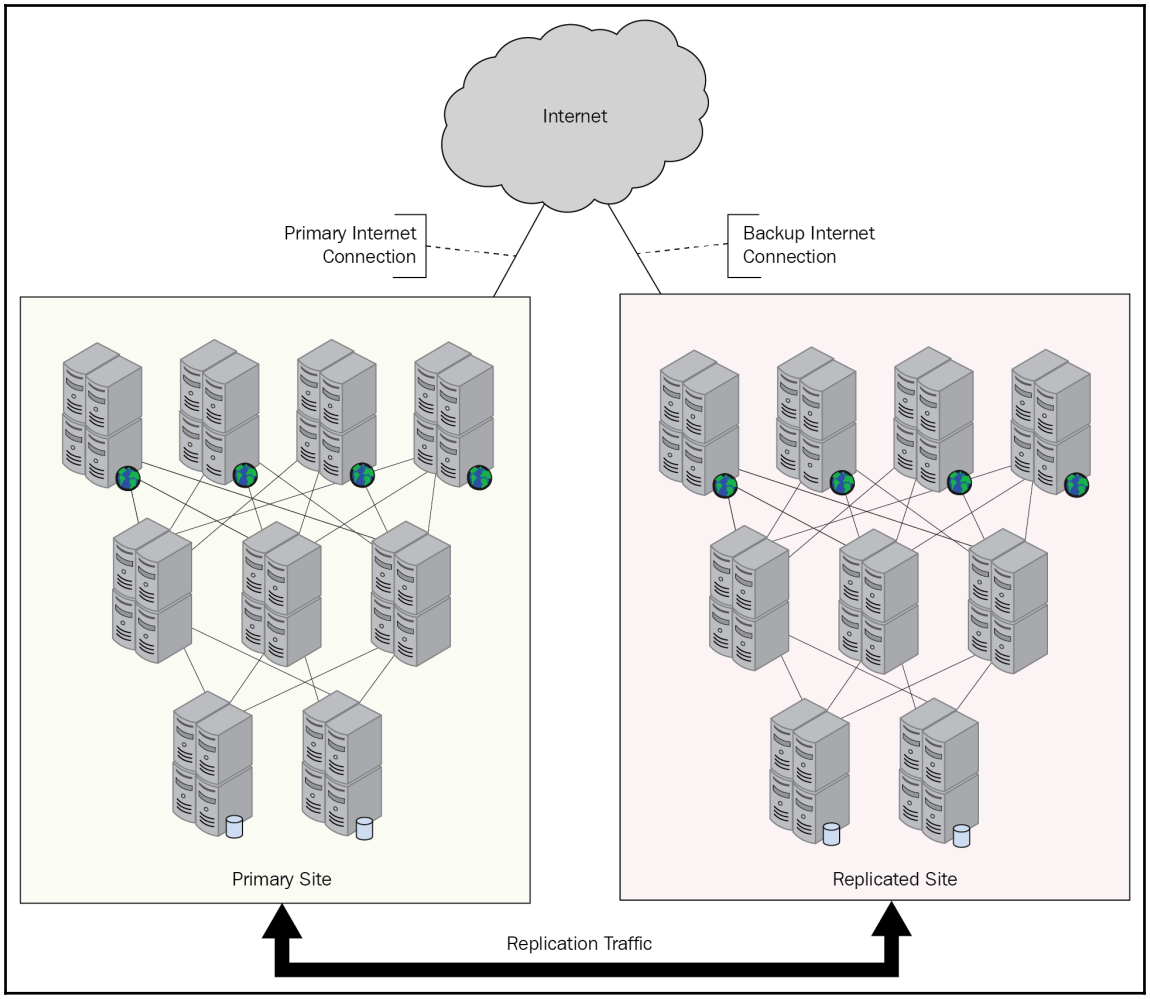


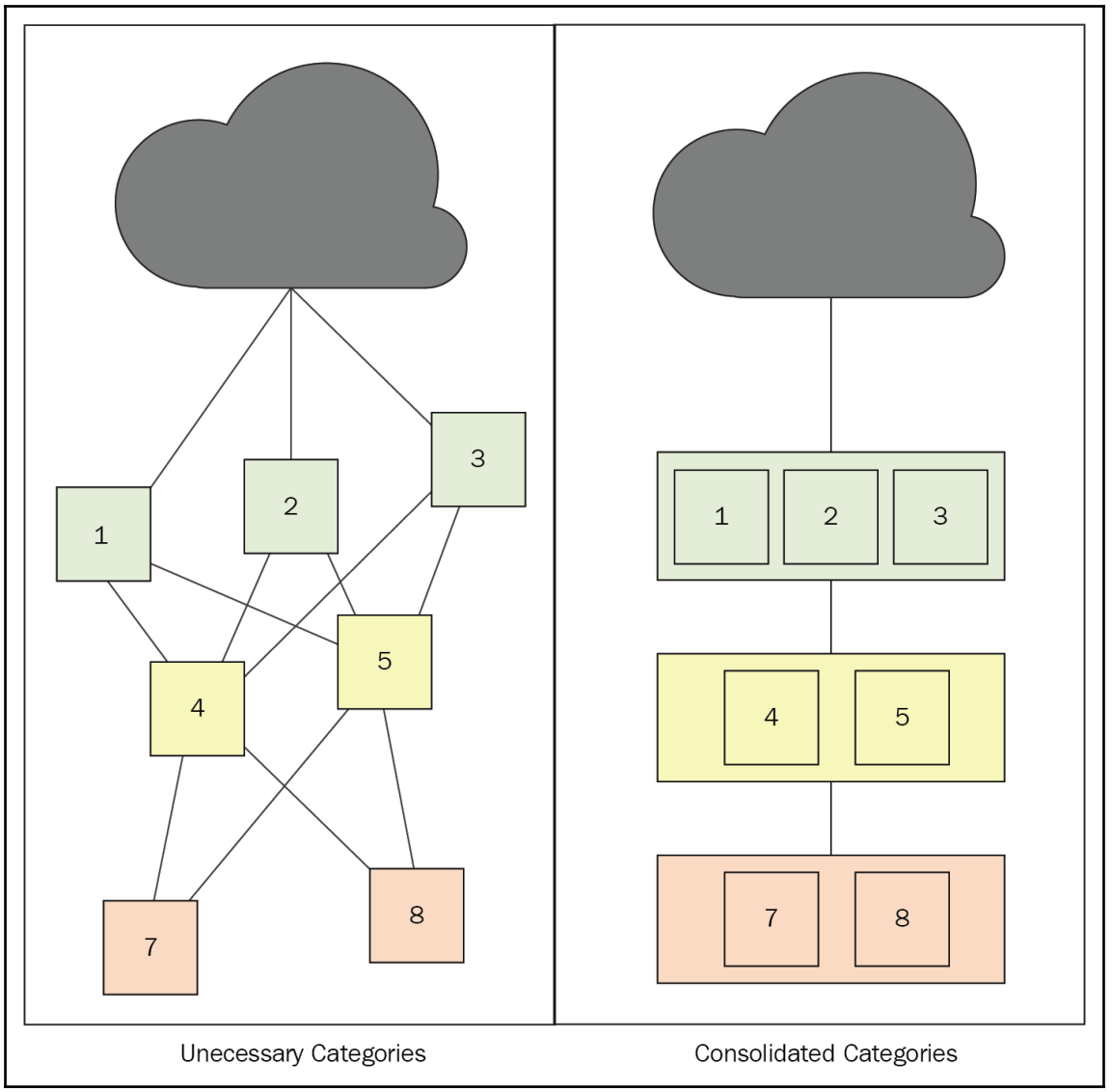

Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries
PROCESS OVERVIEW
Starting Point
Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
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
Security Controls
Step 6
MONITOR
Security Controls
RISK MANAGEMENT FRAMEWORK

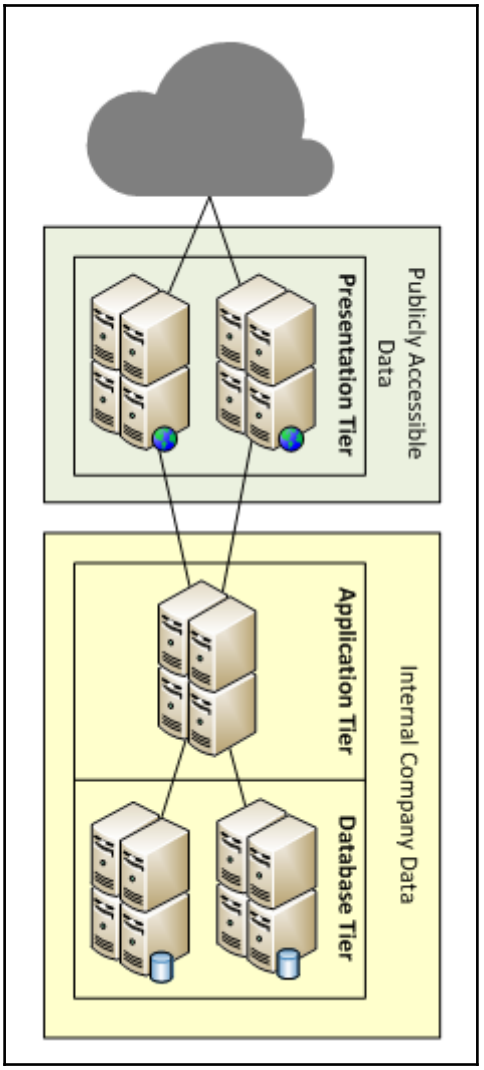

Public Information
Internal Company Information
Confidential Information
Proprietary Information
The further inward you move requires the application of additional data protections.
Additional data protections increase complexity and cost.

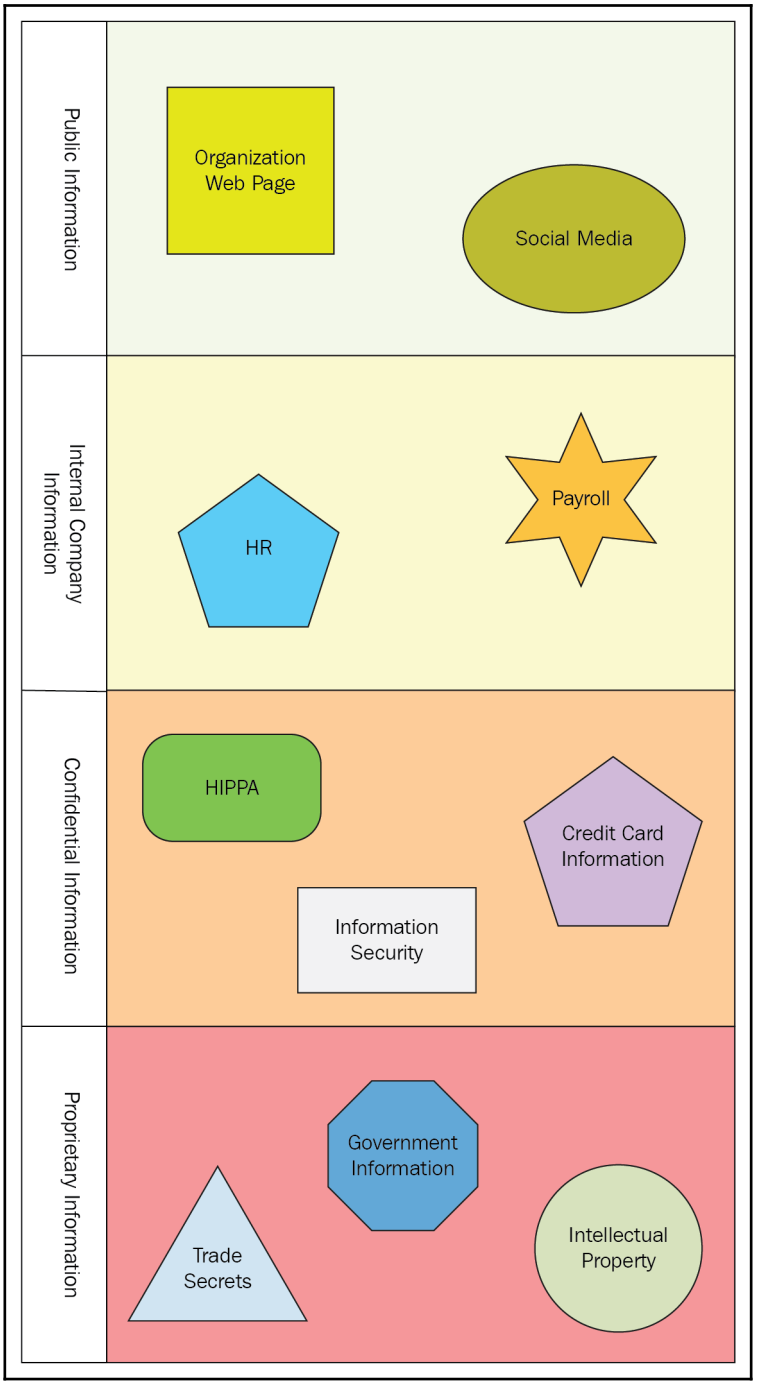

Determining Information Assets
Finding Information in the Environment
Organizing Information into Categories
Valuing the Information


Presentation Tier
Application Tier
Database Tier
Less Protected
May Be Internet
Exposed
Protections
More Protected
Behind Firewall(s)

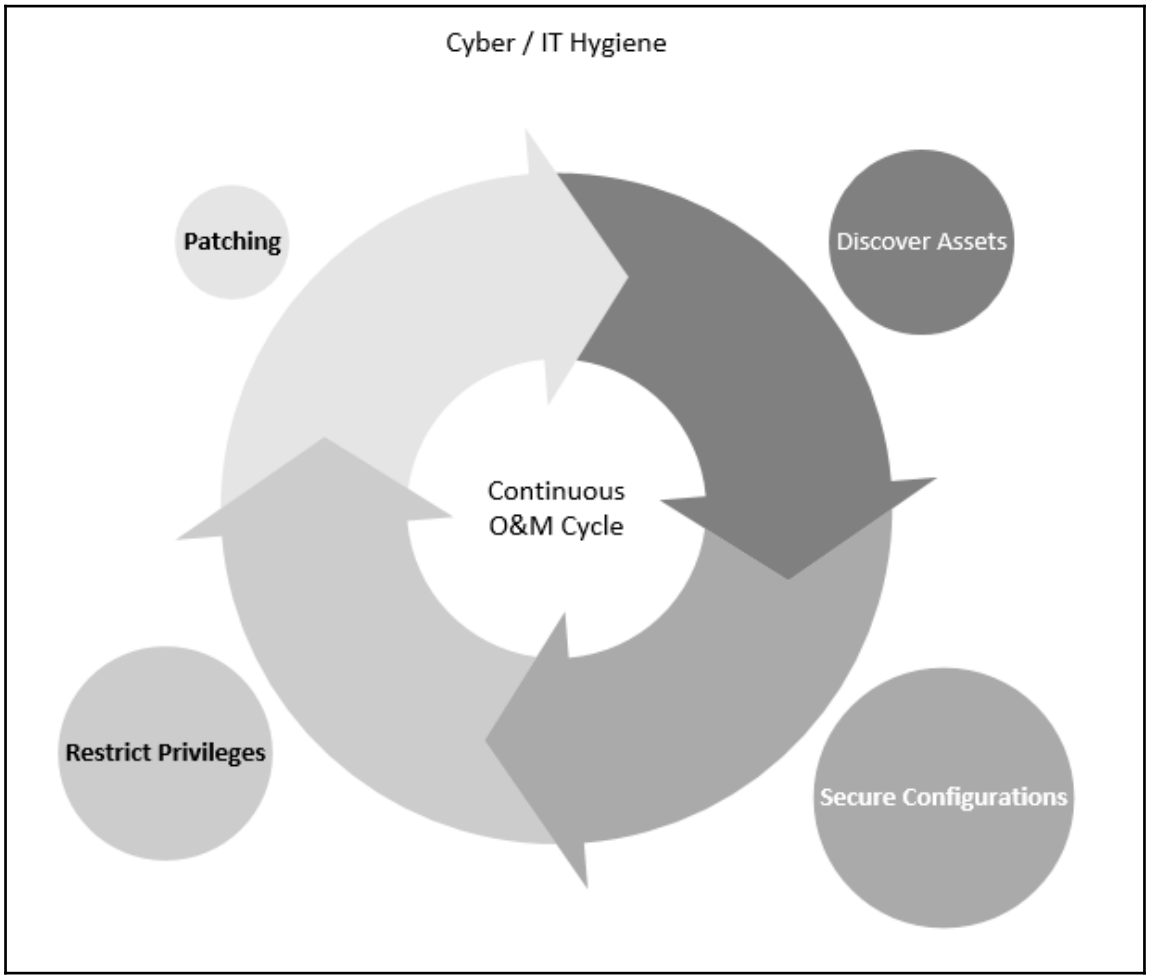

Internet
Primary Internet Connection
Backup Internet Connection
Primary Site
Replicated Site
Replication Traffic

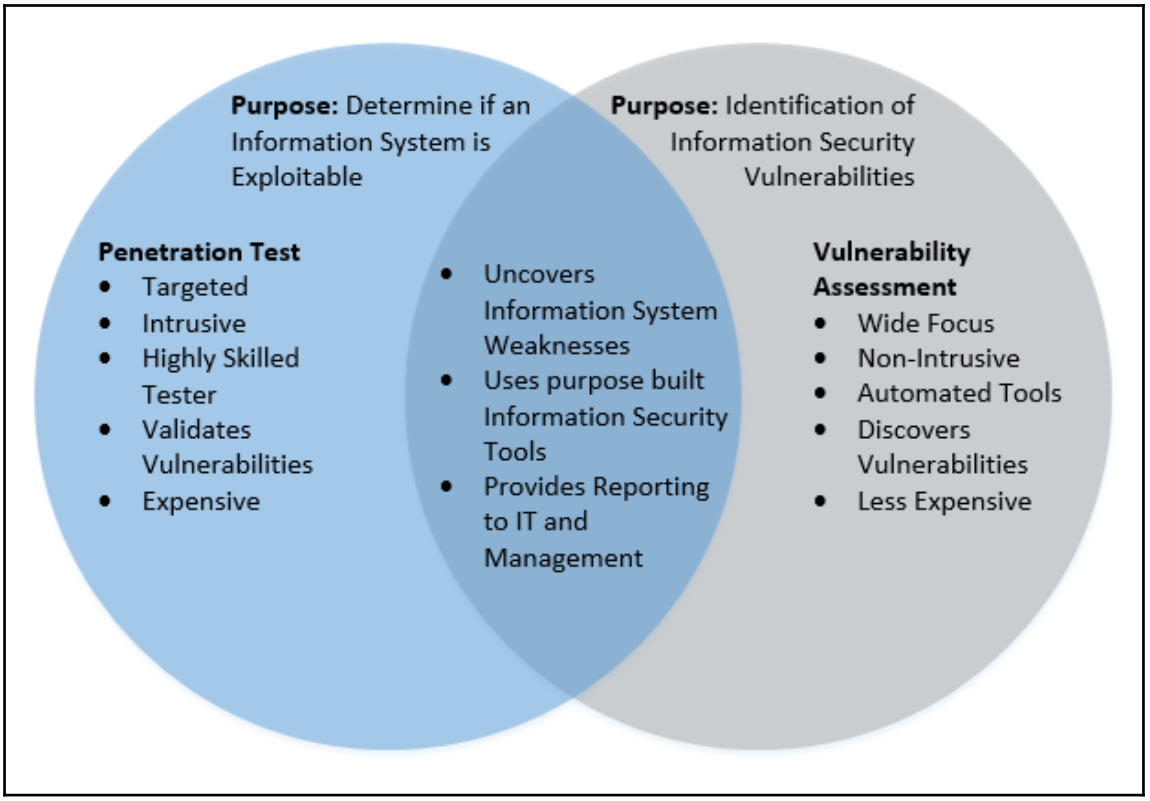

1
2
3
4
5
7
8
1
2
3
4
5
7
8
Unecessary Categories
Consolidated Categories

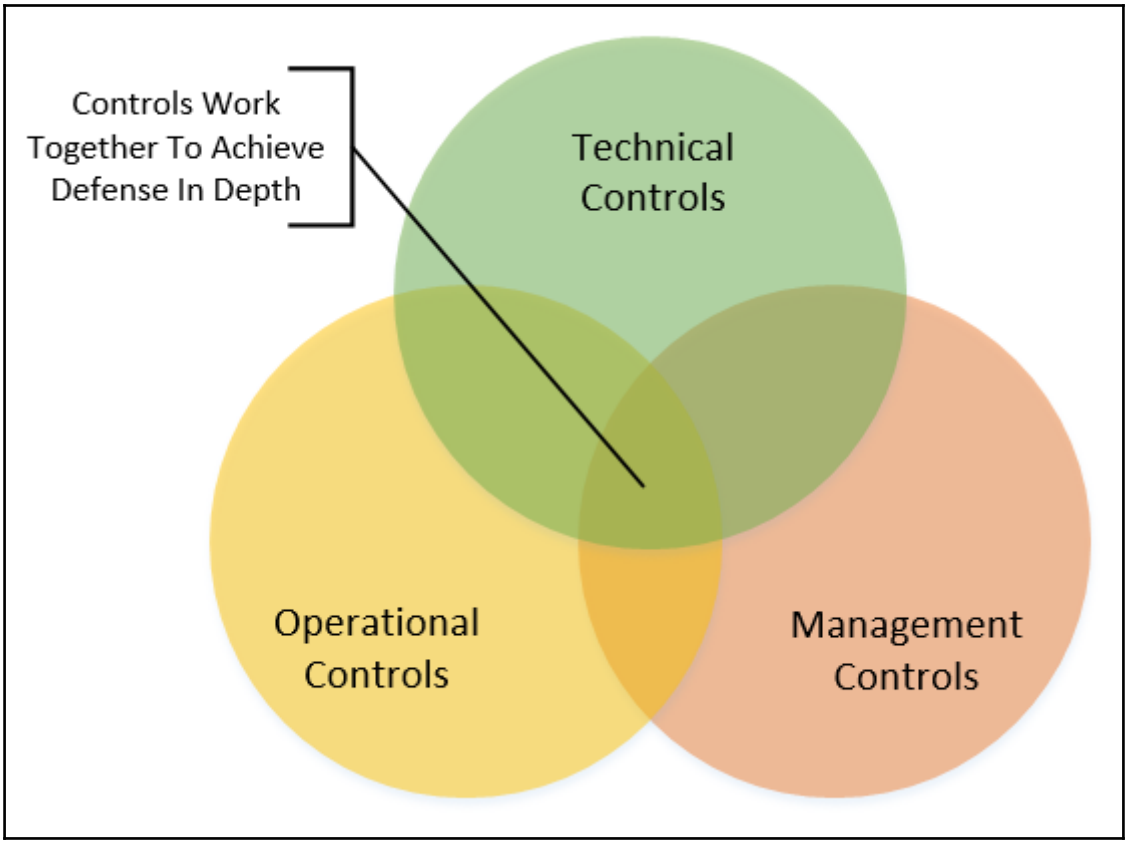

Publicly Accessible Data
Presentation Tier
Internal Company Data
Application Tier
Database Tier

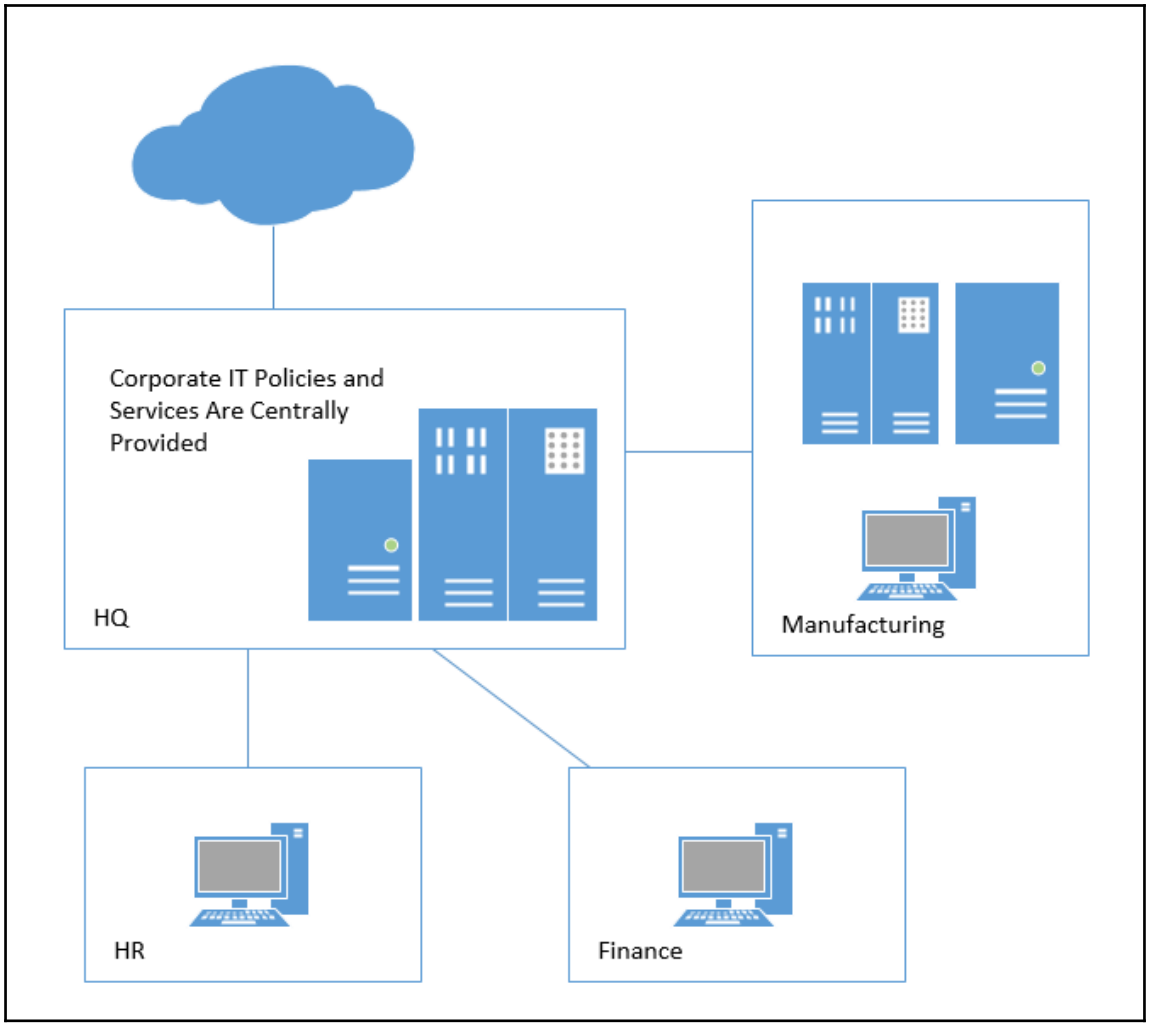

Public Information
Organization Web Page
Social Media
Internal Company Information
HR
Payroll
Confidential Information
HIPPA
Credit Card Information
Information Security
Proprietary Information
Government Information
Trade Secrets
Intellectual Property

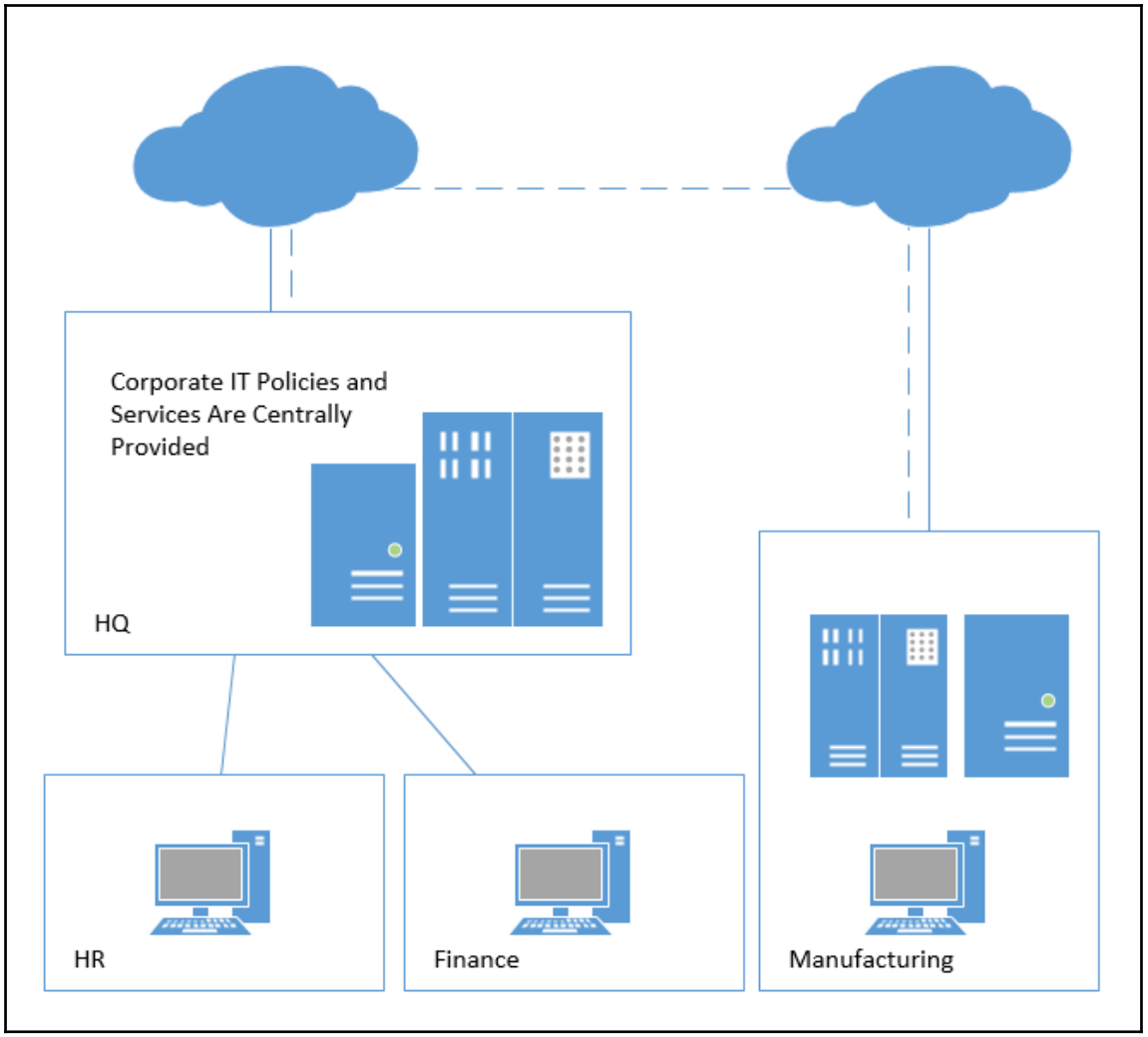
Chapter 5: Developing Your Information and Data Security Plan

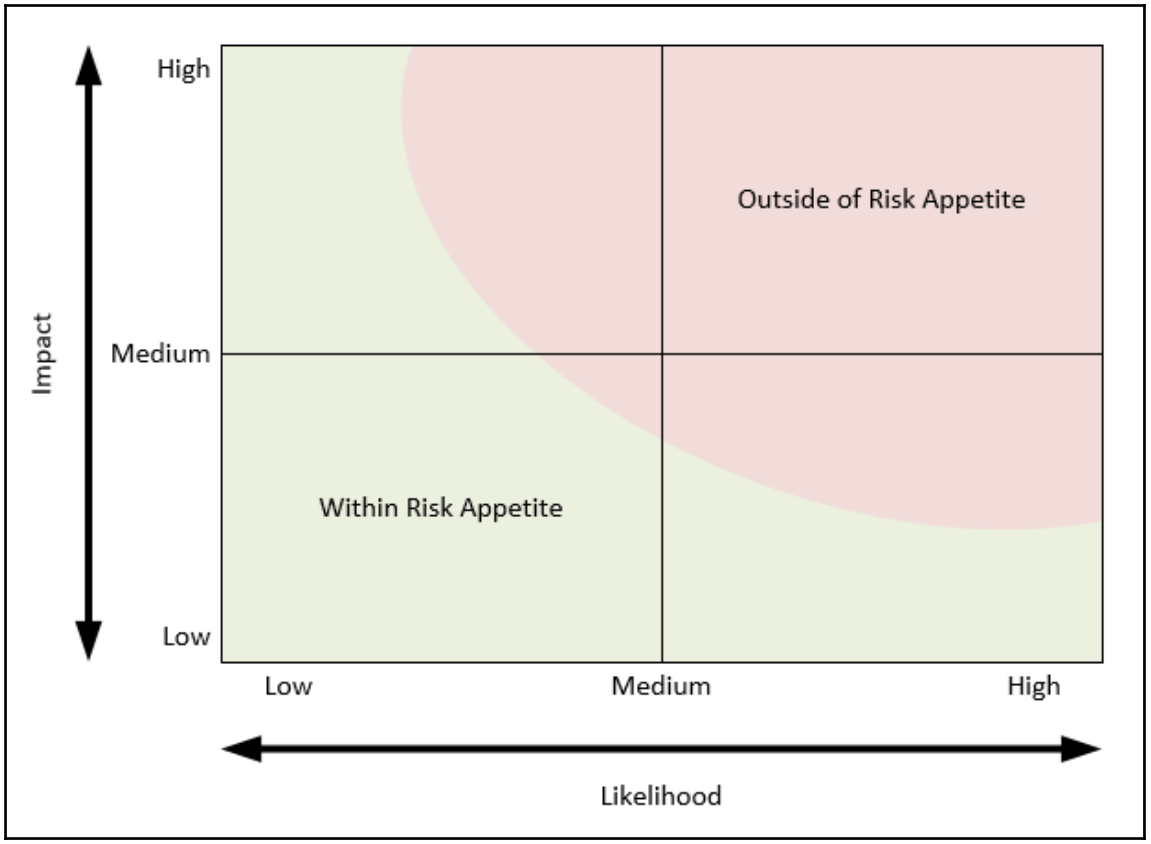



Purpose: Determine if an Information System is Exploitable
Purpose: Identification of Information Security Vulnerabilities
Penetration Test
• Targeted
• Intrusive
• Highly Skilled Tester
• Validates Vulnerabilities
• Expensive
• Uncovers Information System Weaknesses
• Uses purpose built Information Security Tools
• Provides Reporting to IT and Management
Vulnerability Assessment
• Wide Focus
• Non-Intrusive
• Automated Tools
• Discovers Vulnerabilities
• Less Expensive

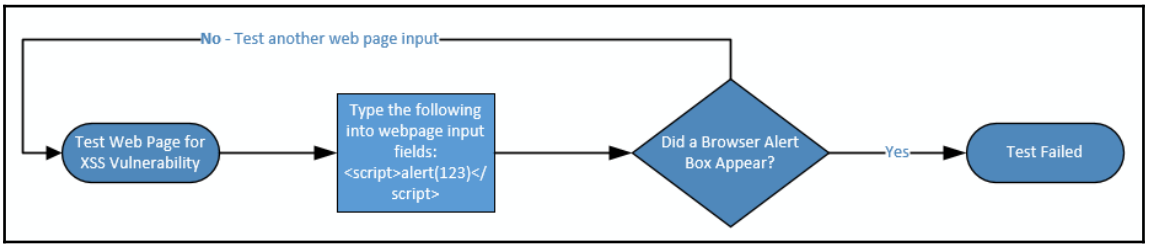

Controls Work Together To Achieve Defense In Depth
Technical Controls
Operational Controls
Management Controls

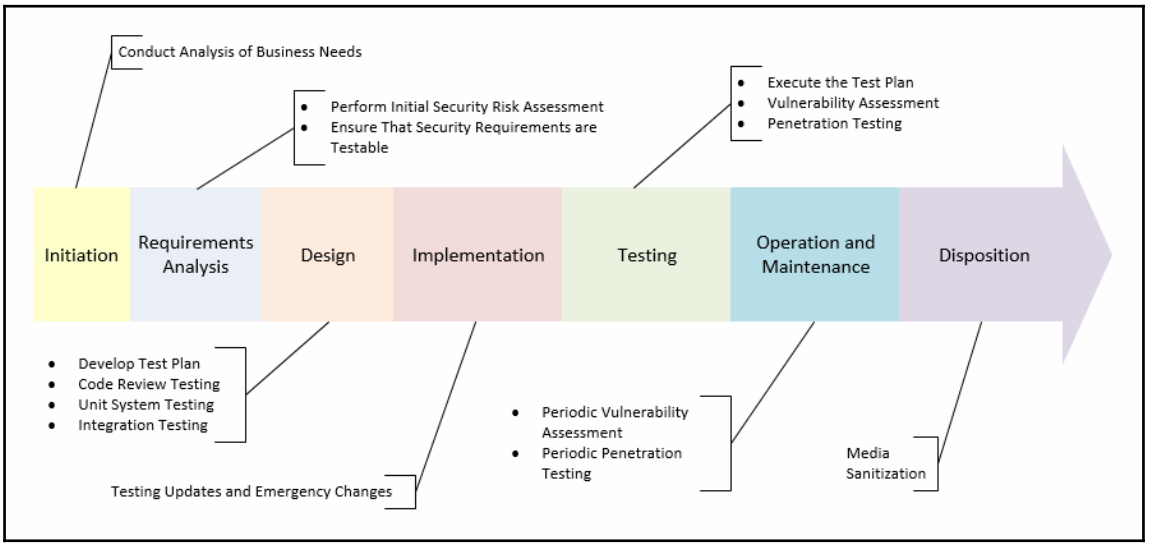

Corporate IT Policies and Services Are Centrally Provided
HQ
Manufacturing
HR
Finance

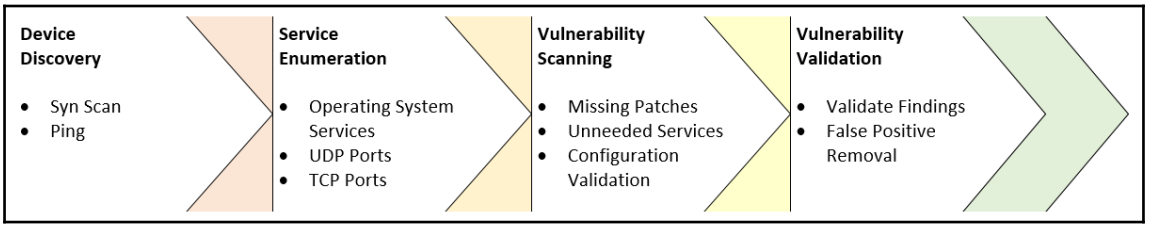

Corporate IT Policies and Services Are Centrally Provided
HQ
HR
Finance
Manufacturing

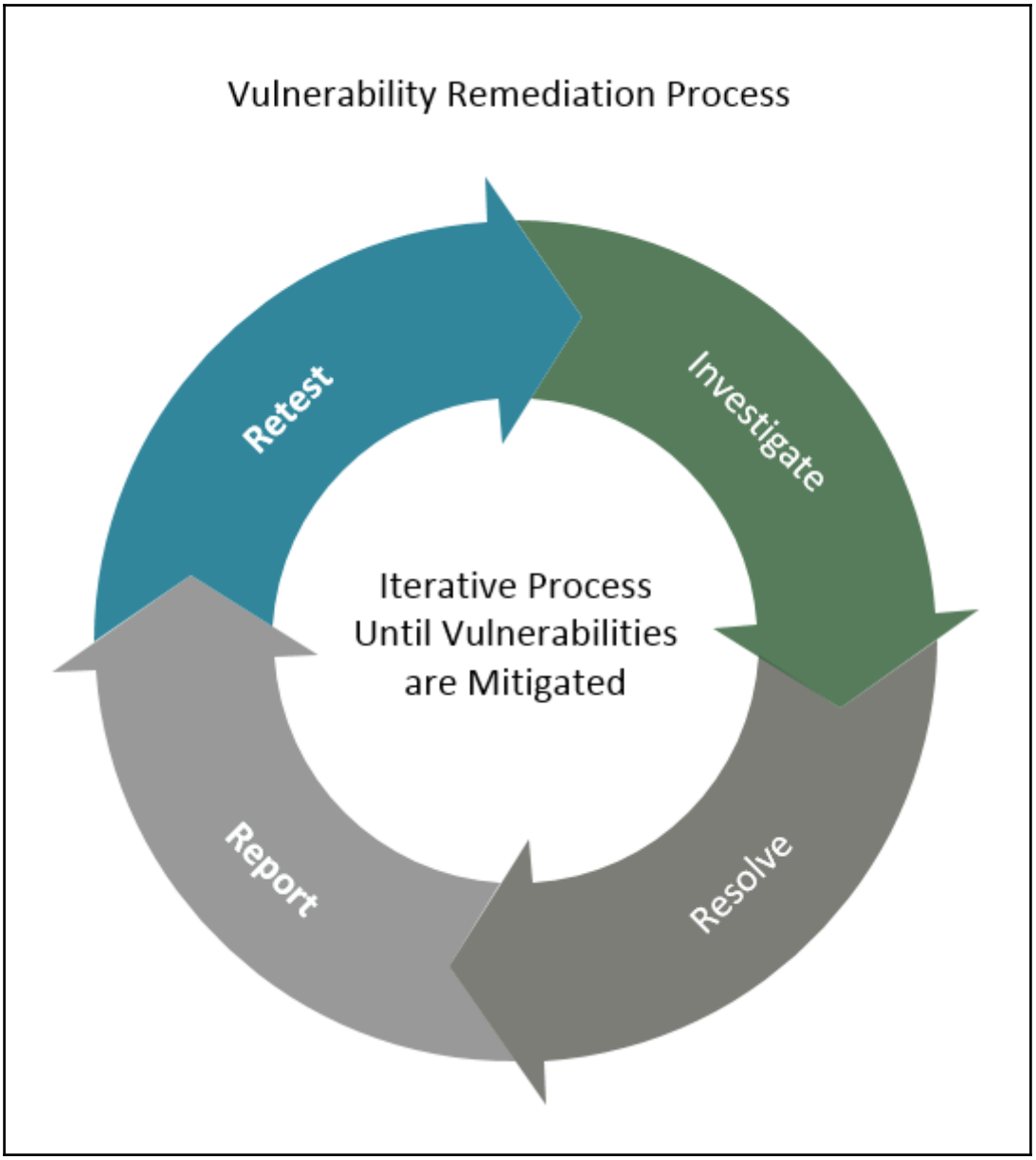

High
Medium
Low
Impact
Outside of Risk Appetite
Within Risk Appetite
Low
Medium
High
Likelihood

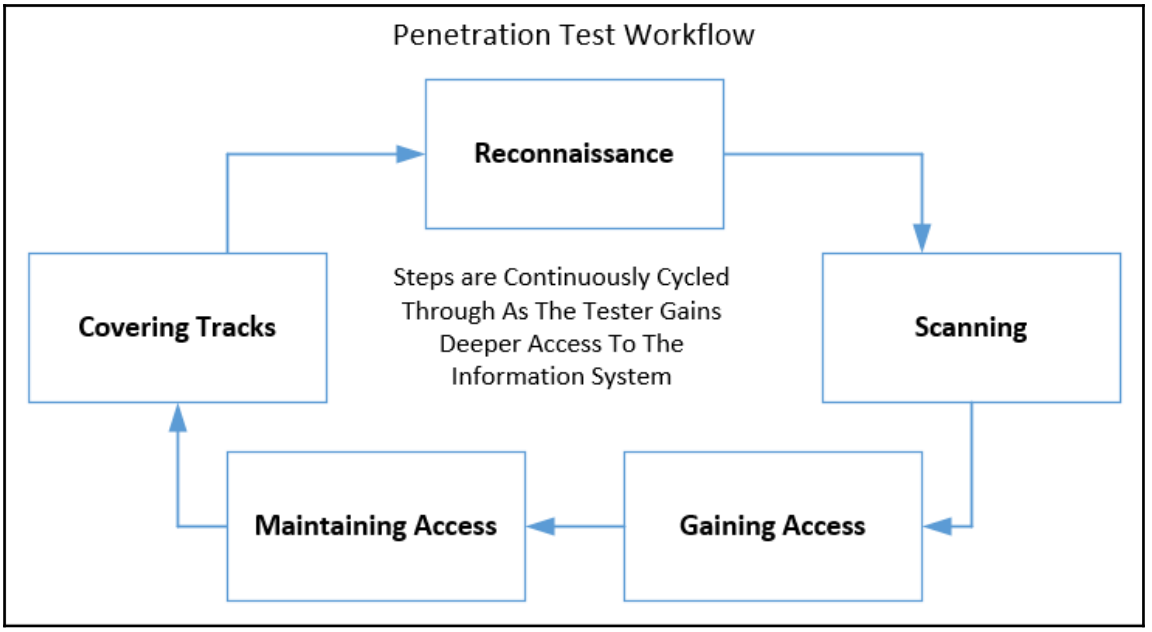
Chapter 6: Continuous Testing and Monitoring



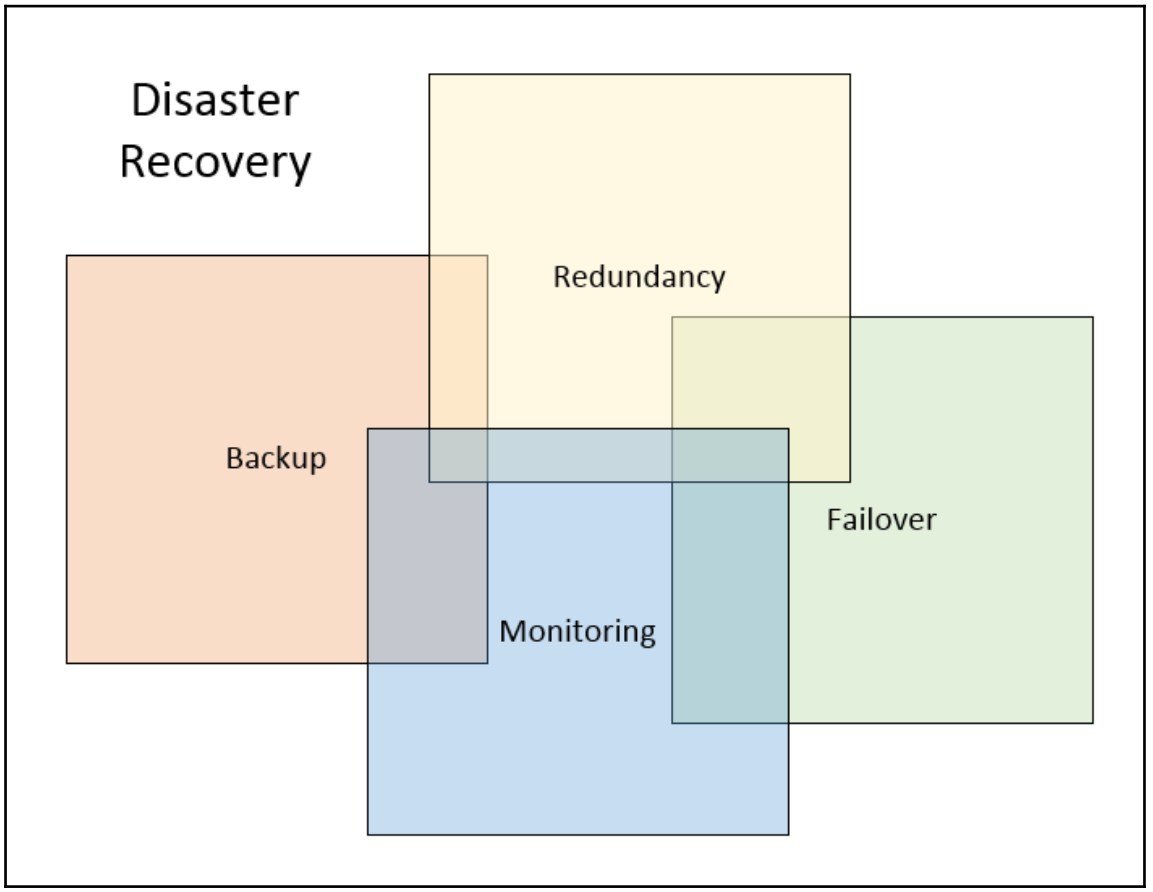


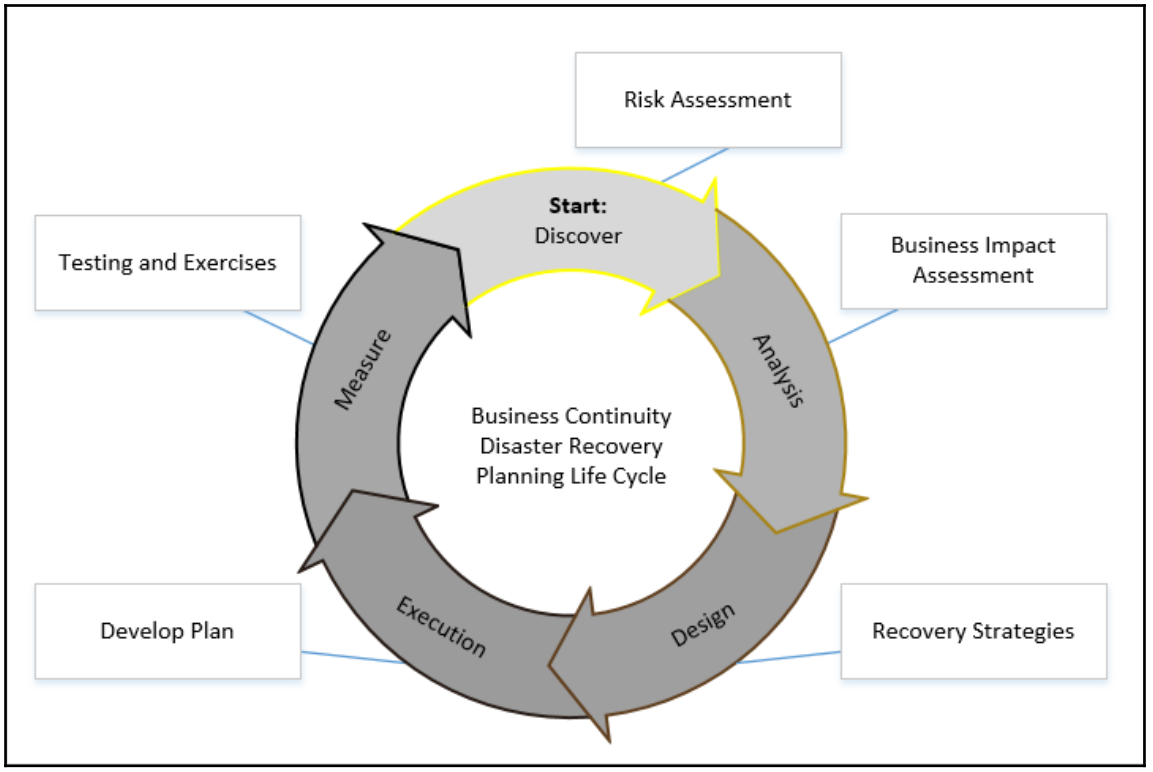


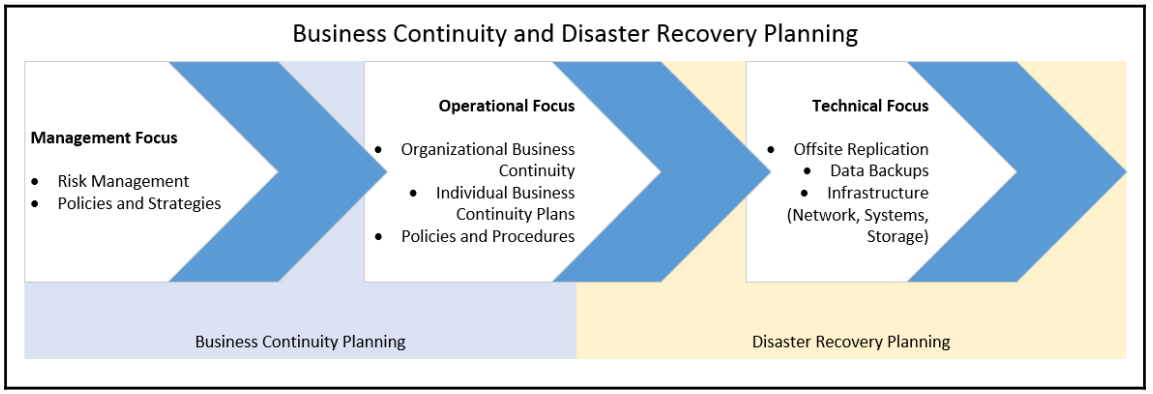

Vulnerability Remediation Process
Retest
Investigate
Iterative Process
Until Vulnerabilities
are Mitigated
Report
Resolve

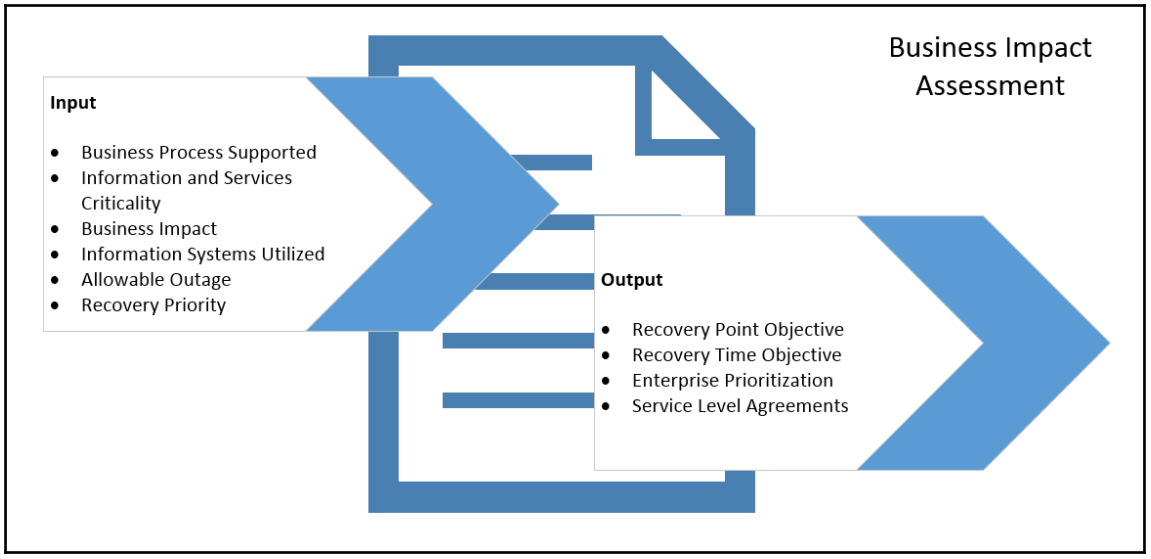

Penetration Test Workflow
Reconnaissance
Scanning
Gaining Access
Maintaining Access
Covering Tracks
Steps are Continuously Cycled Through As The Tester Gains Deeper Access To The Information System

Chapter 7: Business Continuity/Disaster Recovery Planning

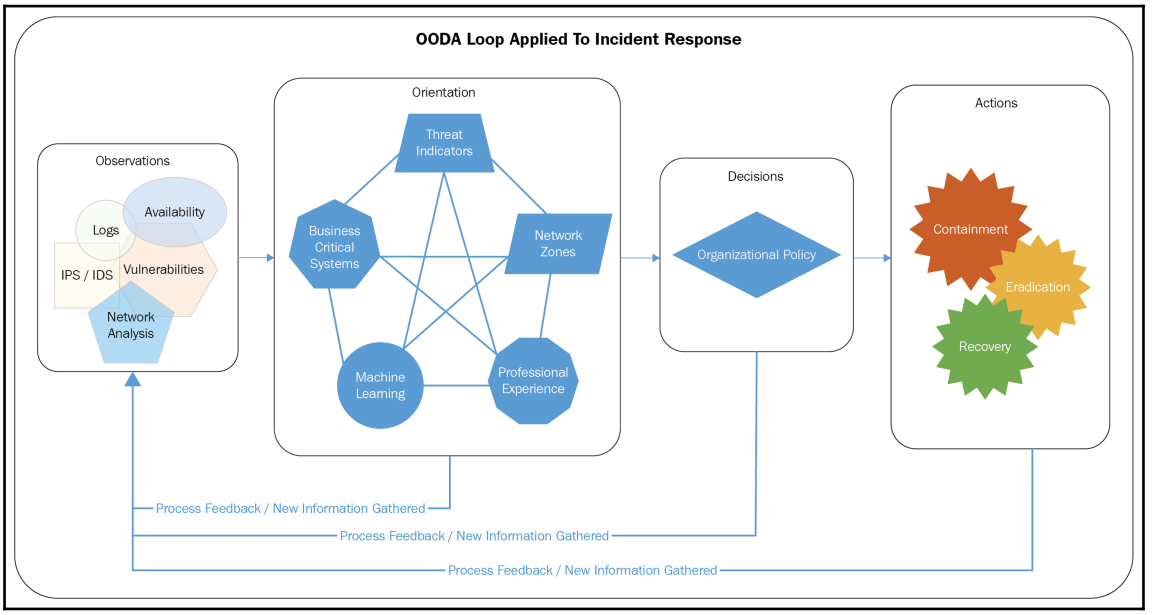


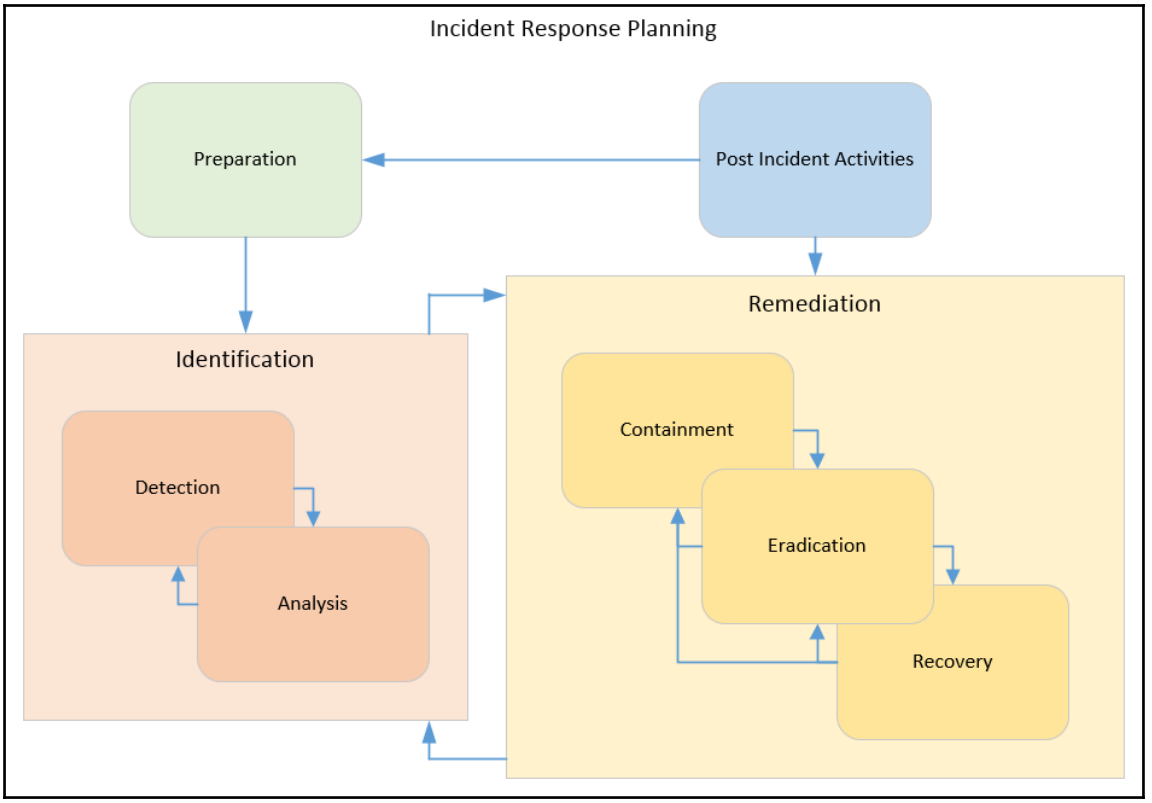

Risk Assessment
Start:
Discover
Business Impact Assessment
Testing and Exercises
Measure
Analysis
Business Continuity
Disaster Recovery
Planning Life Cycle
Develop Plan
Execution
Design
Recovery Strategies


Business Continuity and Disaster Recovery Planning
Management Focus
Risk Management
Policies and Strategies
Operational Focus
Organizational Business Continuity
Individual Business Continuity Plans
Policies and Procedures
Technical Focus
Offsite Replication
Data Backups
Infrastructure (Network, Systems, Storage)
Business Continuity Planning
Disaster Recovery Planning

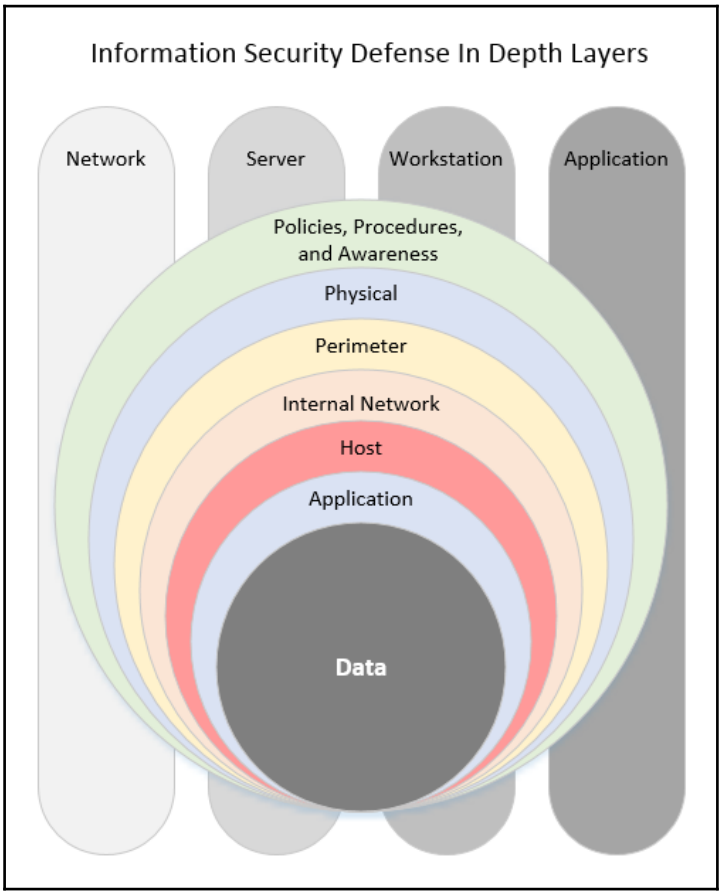

Business Impact Assessment
Input
Business Process Supported
Information and Services Criticality
Business Impact
Information Systems Utilized
Allowable Outage
Recovery Priority
Output
Recovery Point Objective
Recovery Time Objective
Enterprise Prioritization
Service Level Agreements

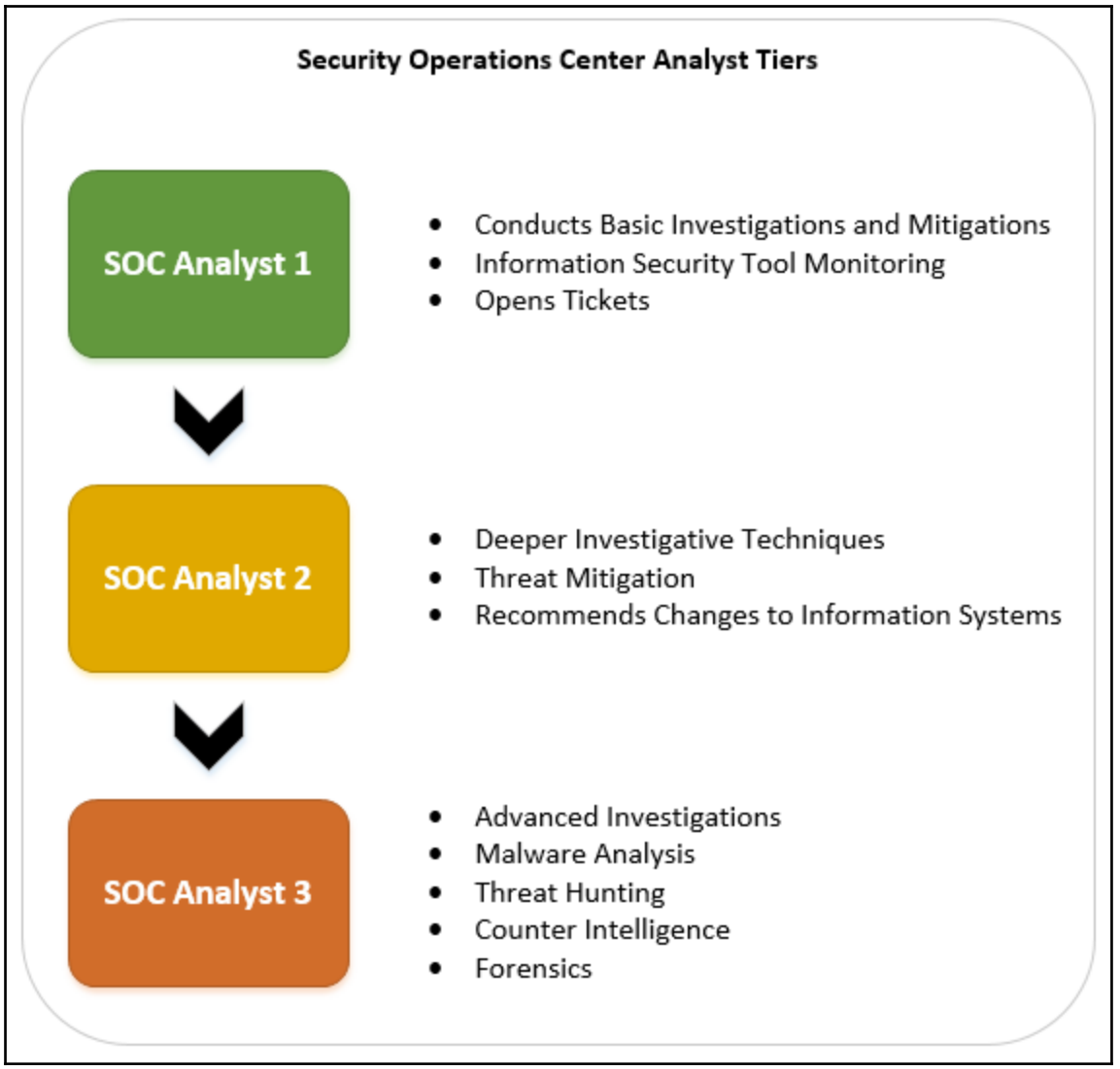
Chapter 8: Incident Response Planning

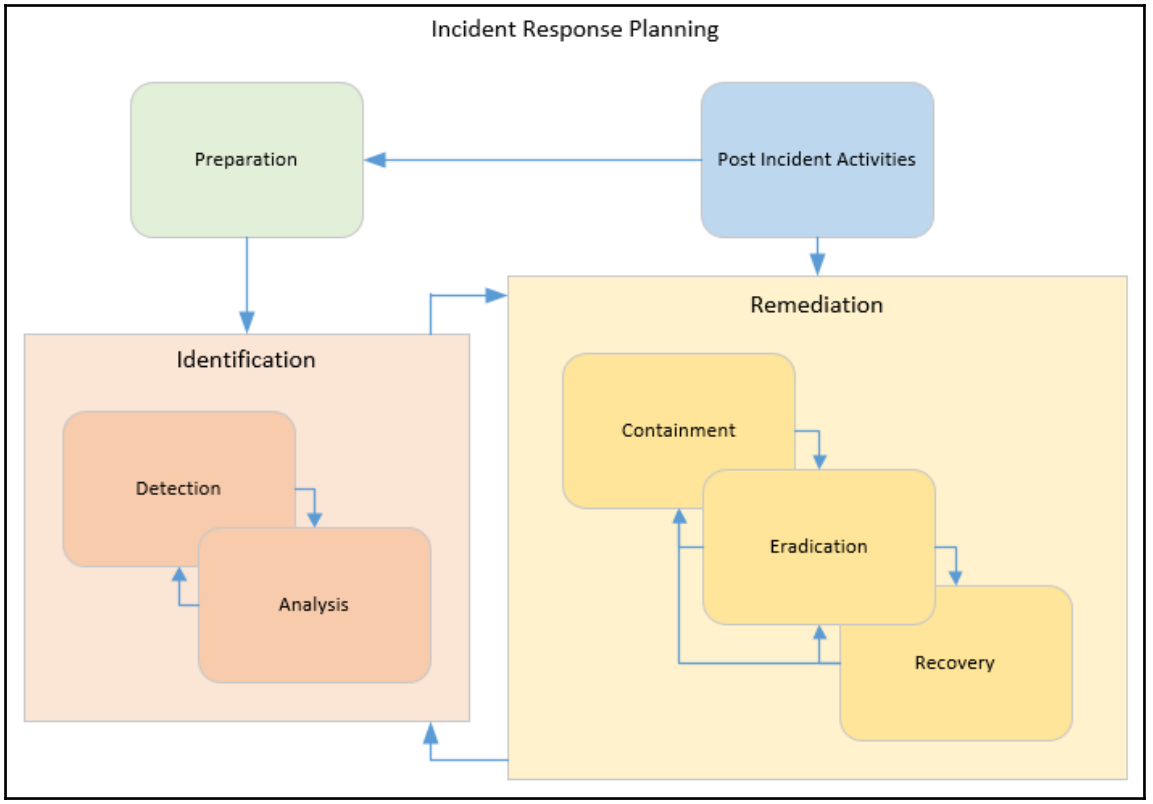


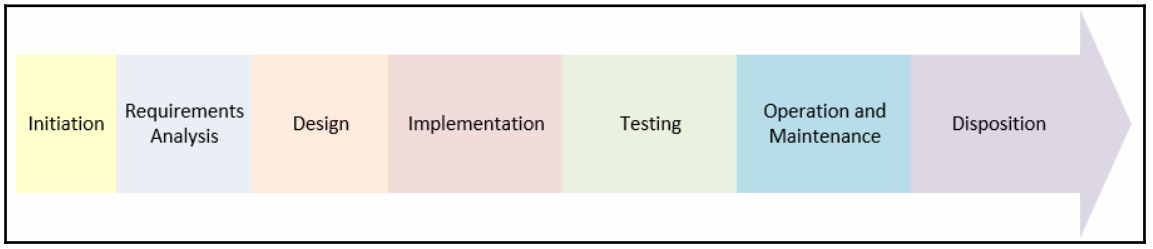

Incident Response Planning
Preparation
Post Incident Activities
Identification
Detection
Analysis
Remediation
Containment
Eradication
Recovery

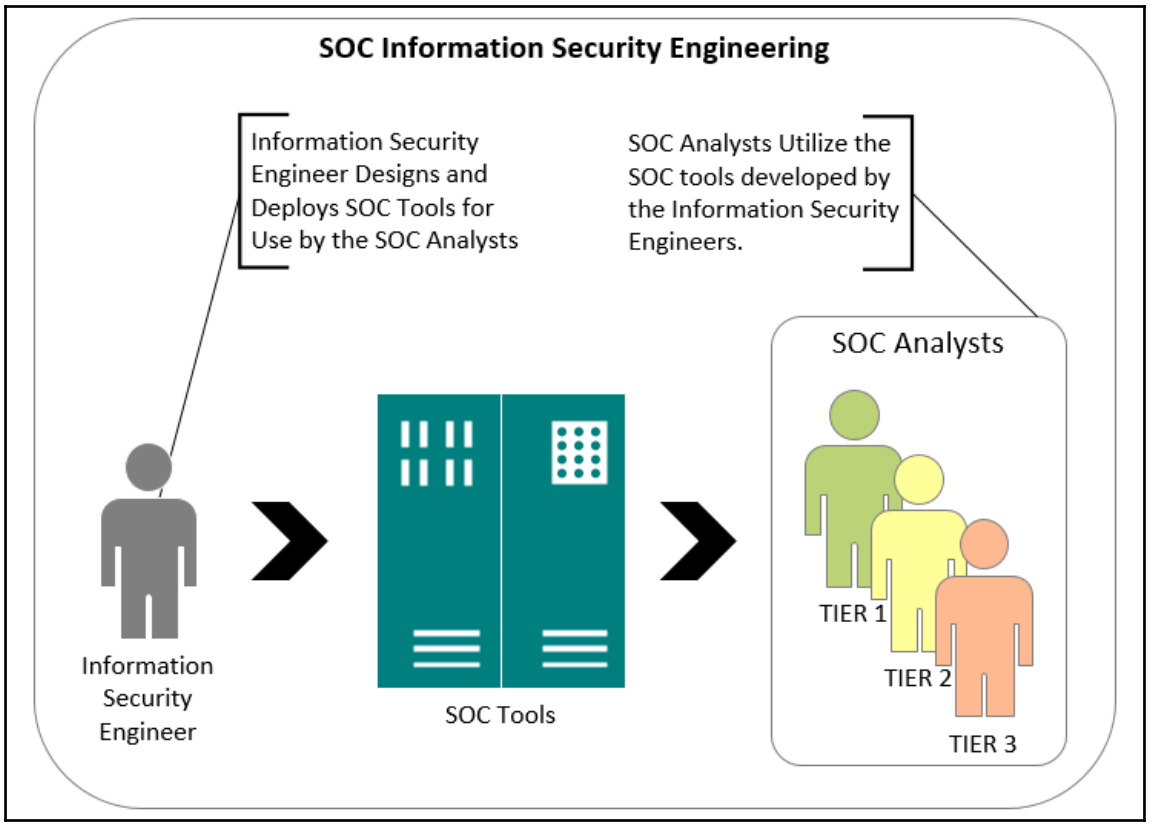
Chapter 9: Developing a Security Operations Center

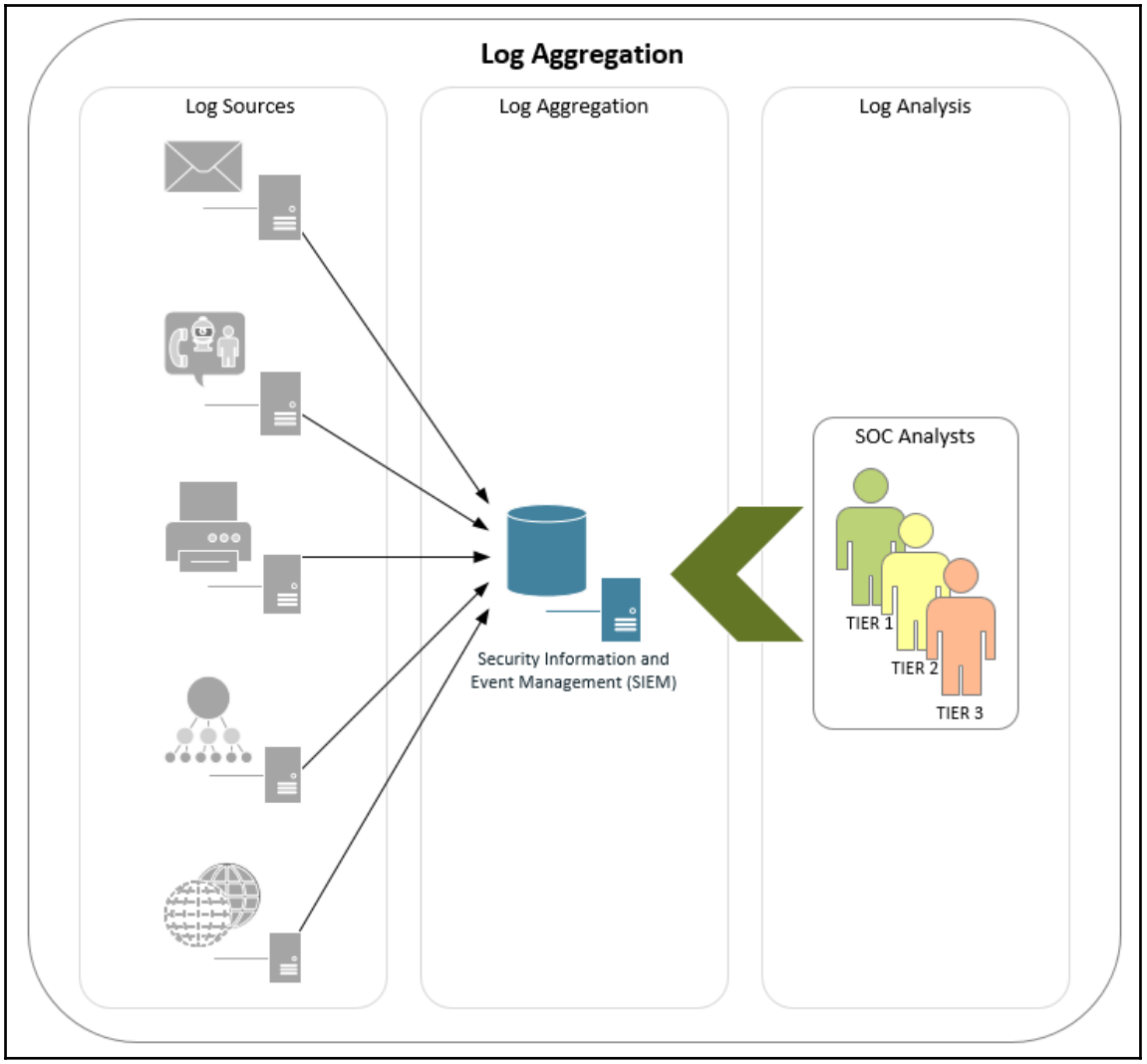


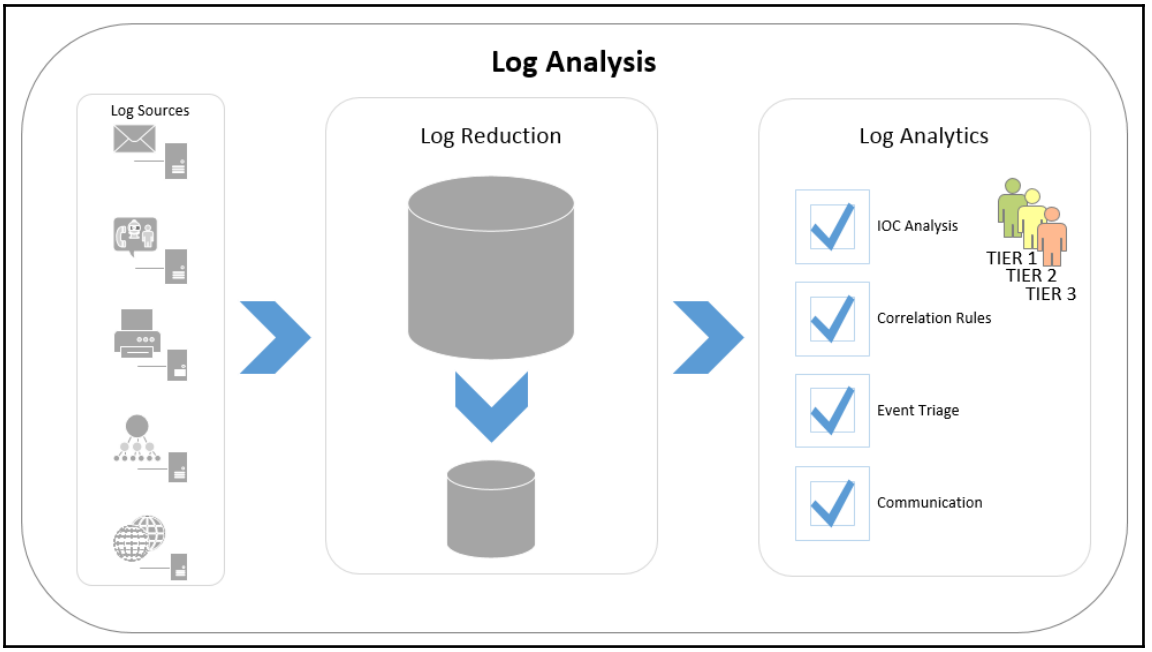

Security Operations Center Analyst Tiers
SOC Analyst 1
Conducts Basic Investigations and Mitigations
Information Security Tool Monitoring
Opens Tickets
SOC Analyst 2
Deeper Investigative Techniques
Threat Mitigation
Recommends Changes to Information Systems
SOC Analyst 3
Advanced Investigations
Malware Analysis
Threat Hunting
Counter Intelligence
Forensics


Incident Response Planning
Preparation
Post Incident Activities
Identification
Detection
Analysis
Remediation
Containment
Eradication
Recovery

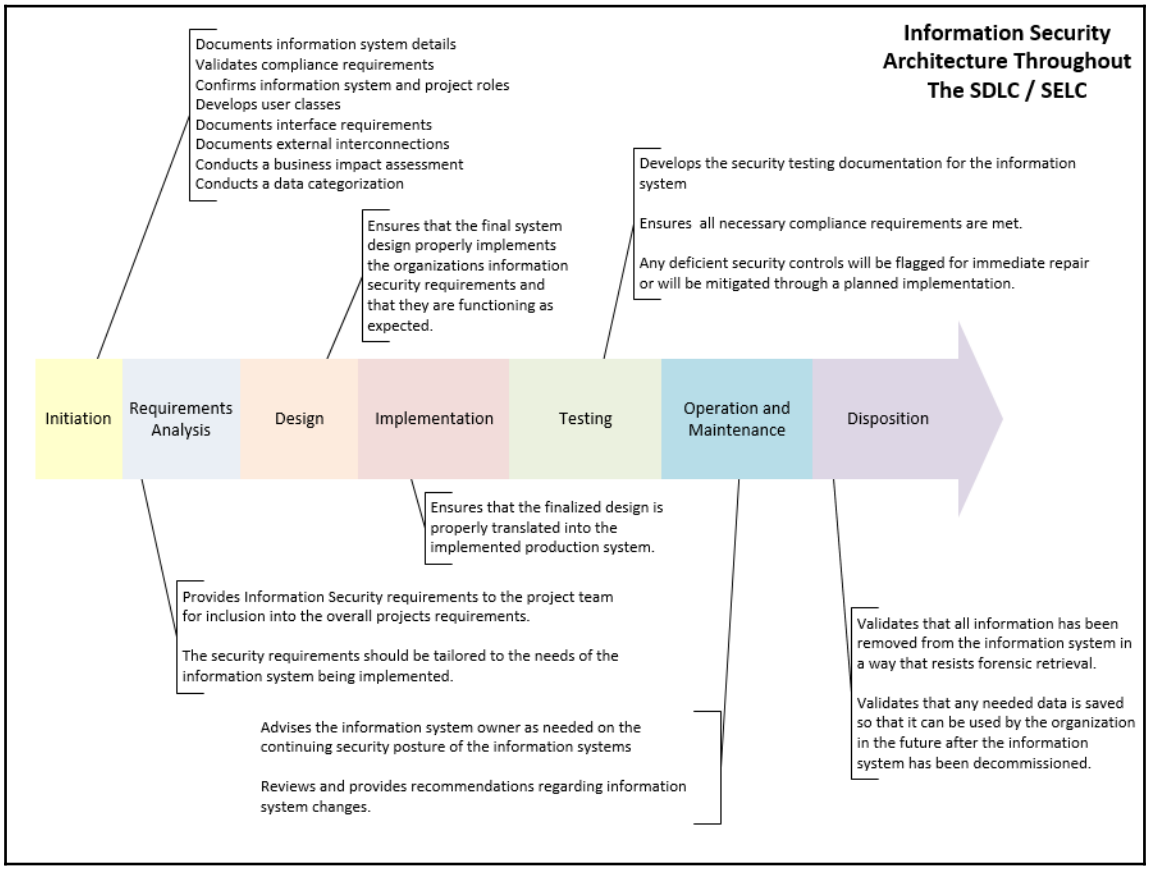

Initiation
Requirements Analysis
Design
Implementation
Testing
Operation and Maintenance
Disposition

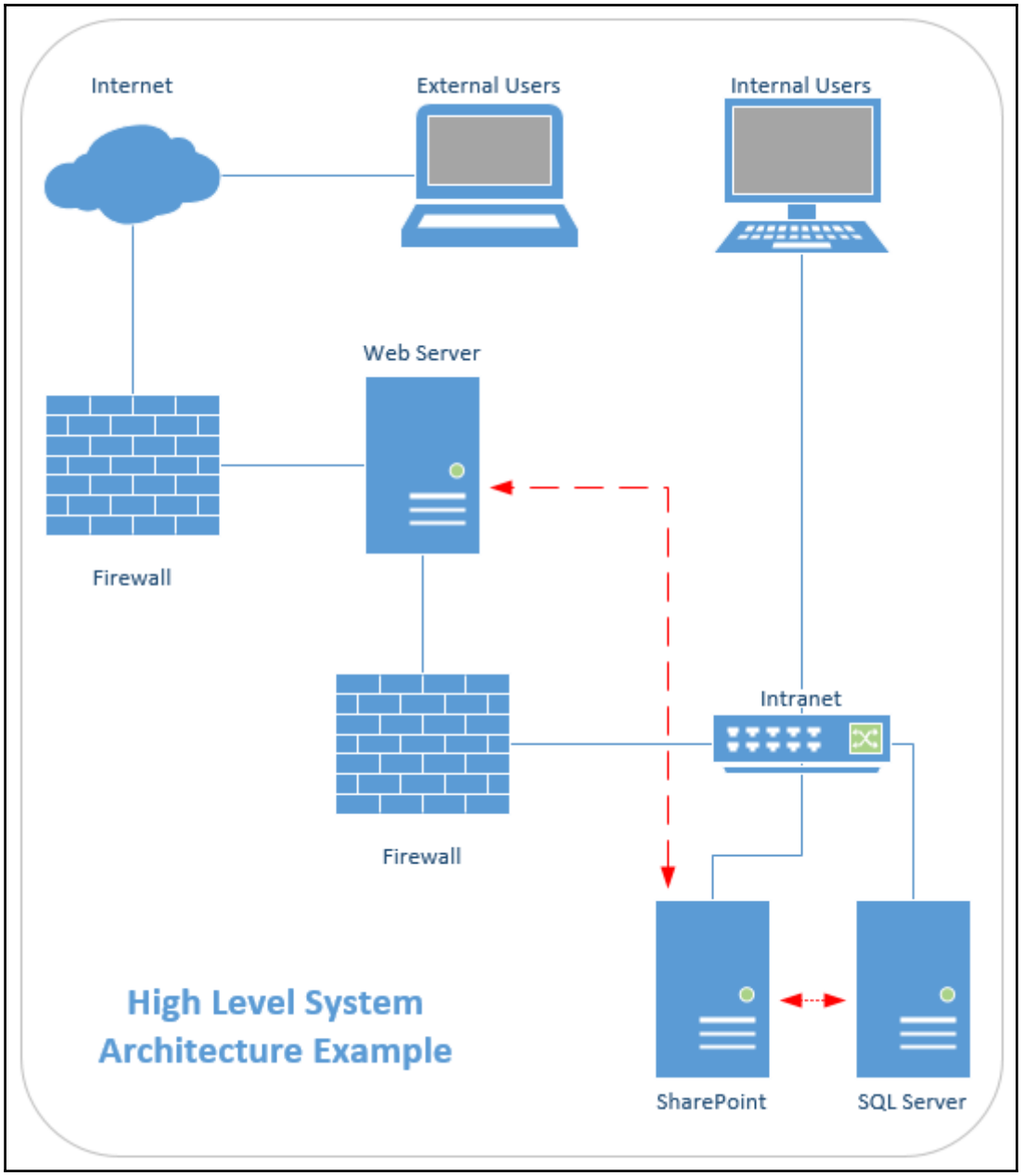

SOC Information Security Engineering
Information Security Engineer Designs and Deploys SOC Tools for Use by the SOC Analysts
SOC Analysts Utilize the SOC tools developed by the Information Security Engineers.
Information Security Engineer
SOC Tools
SOC Analysts
TIER 1
TIER 2
TIER 3


Log Aggregation
Log Sources
Log Aggregation
Log Analysis
SOC Analysts
TIER 1
TIER 2
TIER 3
Security Information and
Event Management (SIEM)

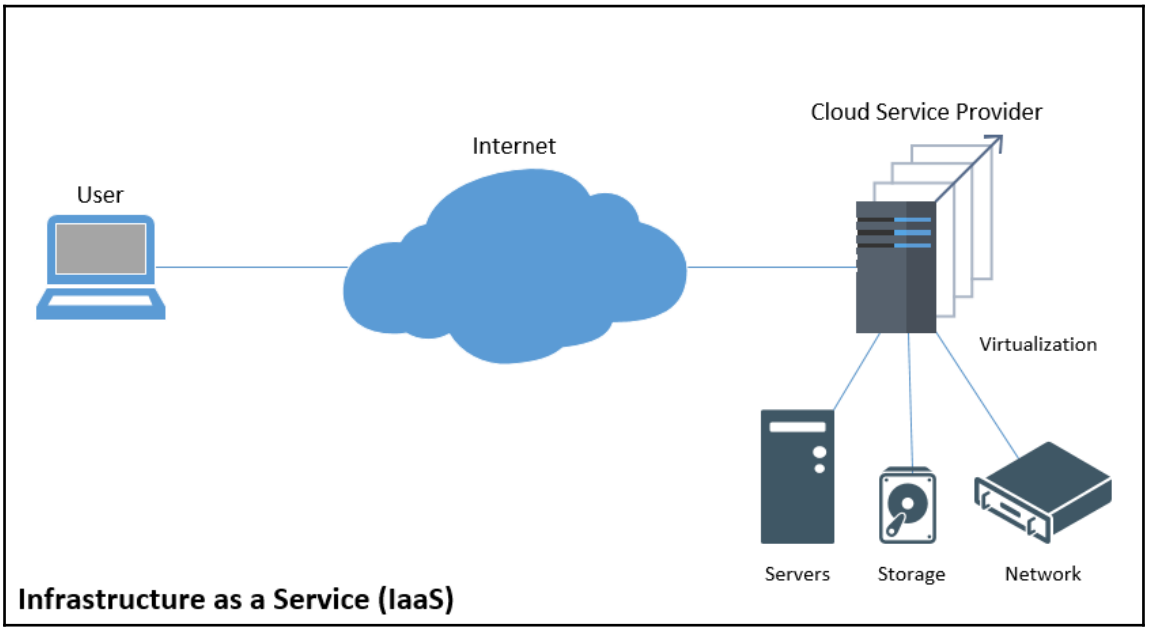

Log Analysis
Log Sources
Log Reduction
Log Analytics
IOC Analysis
Correlation Rules
Event Triage
Communication
TIER 1
TIER 2
TIER 3

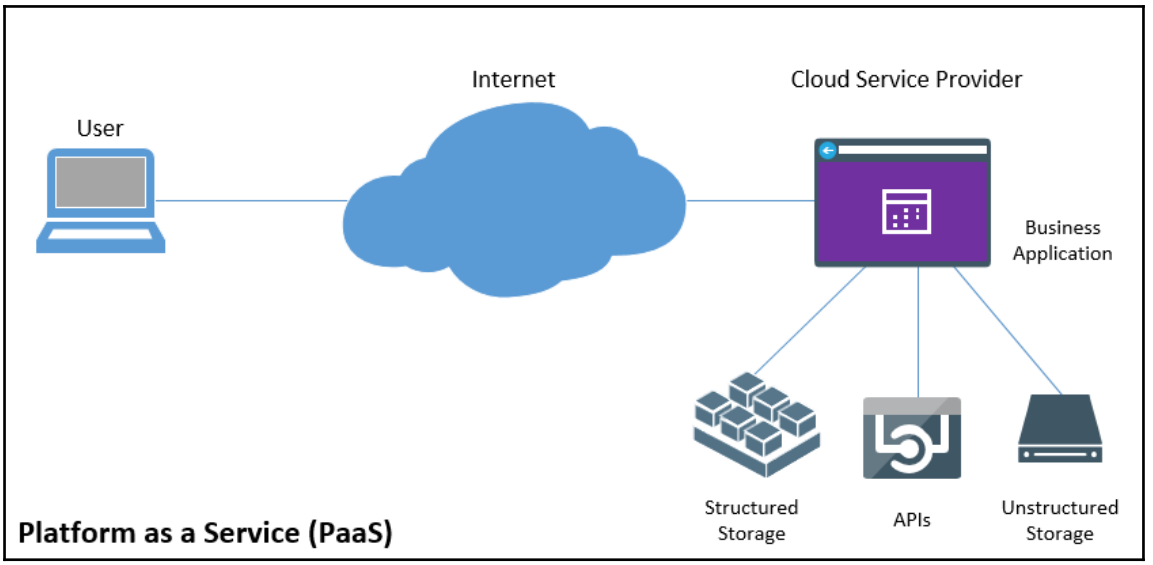
Chapter 10: Developing an Information Security Architecture Program

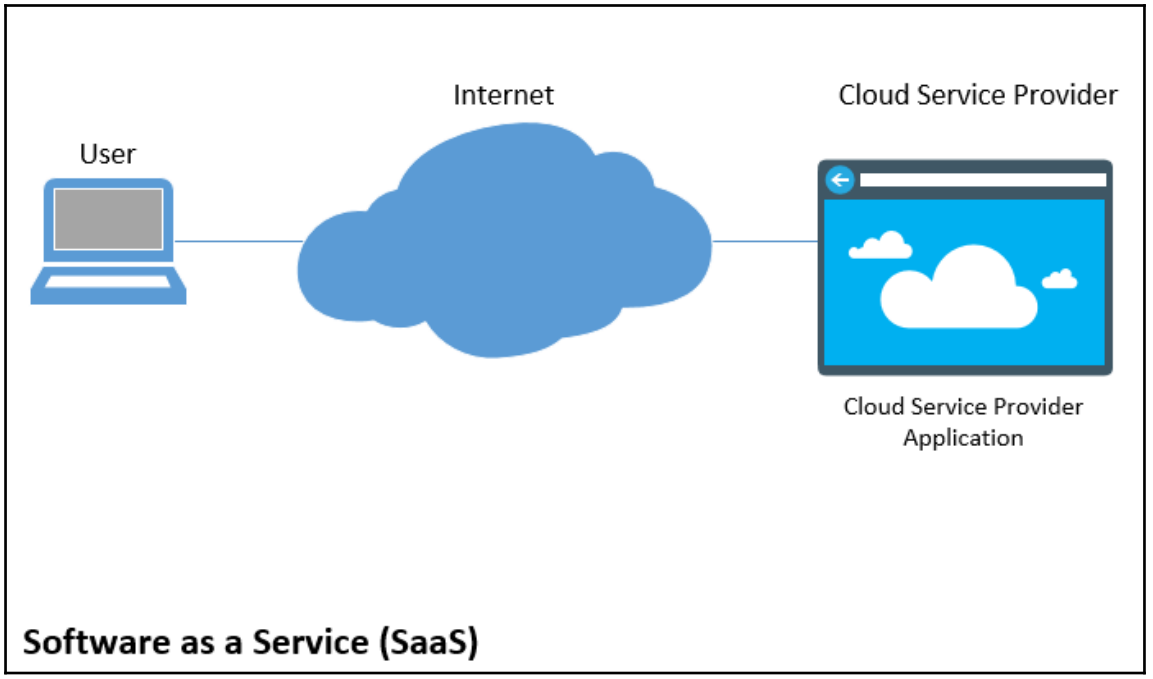


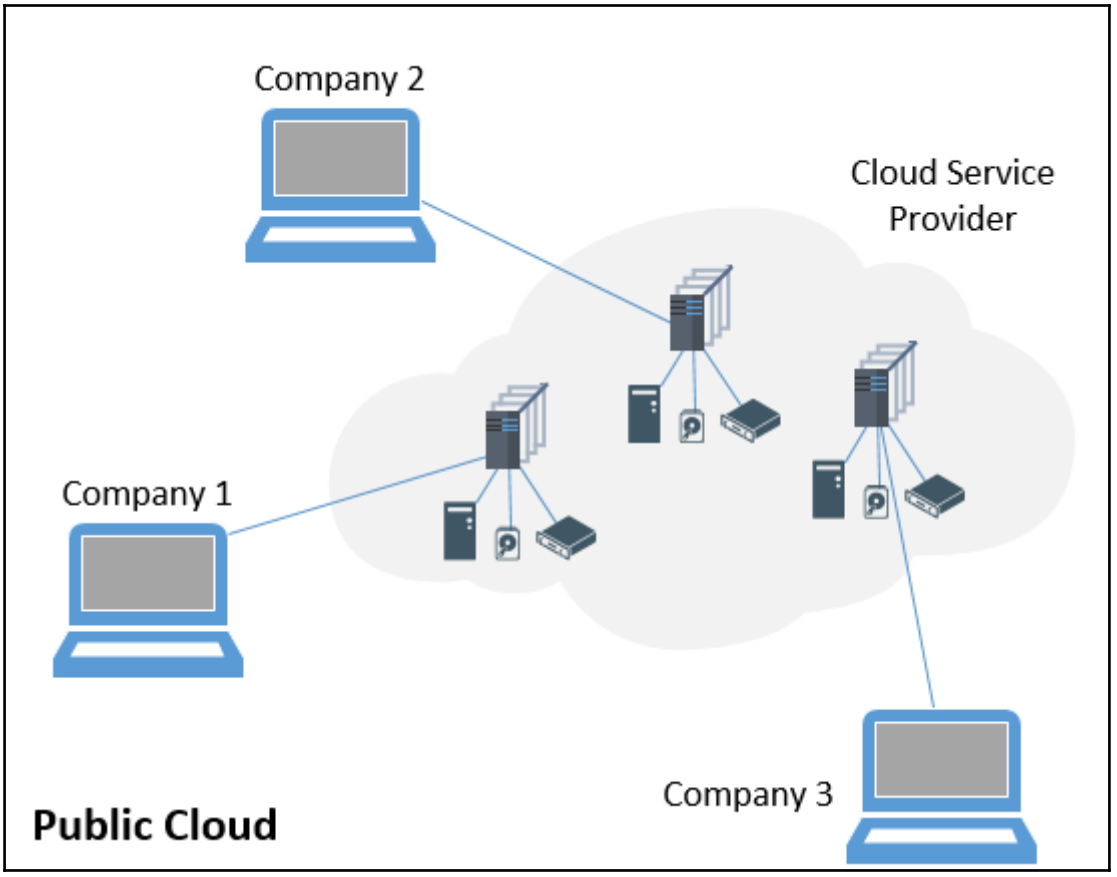

Internet
External Users
Internal Users
Web Server
Firewall
Firewall
Intranet
High Level System
Architecture Example
SharePoint
SQL Server

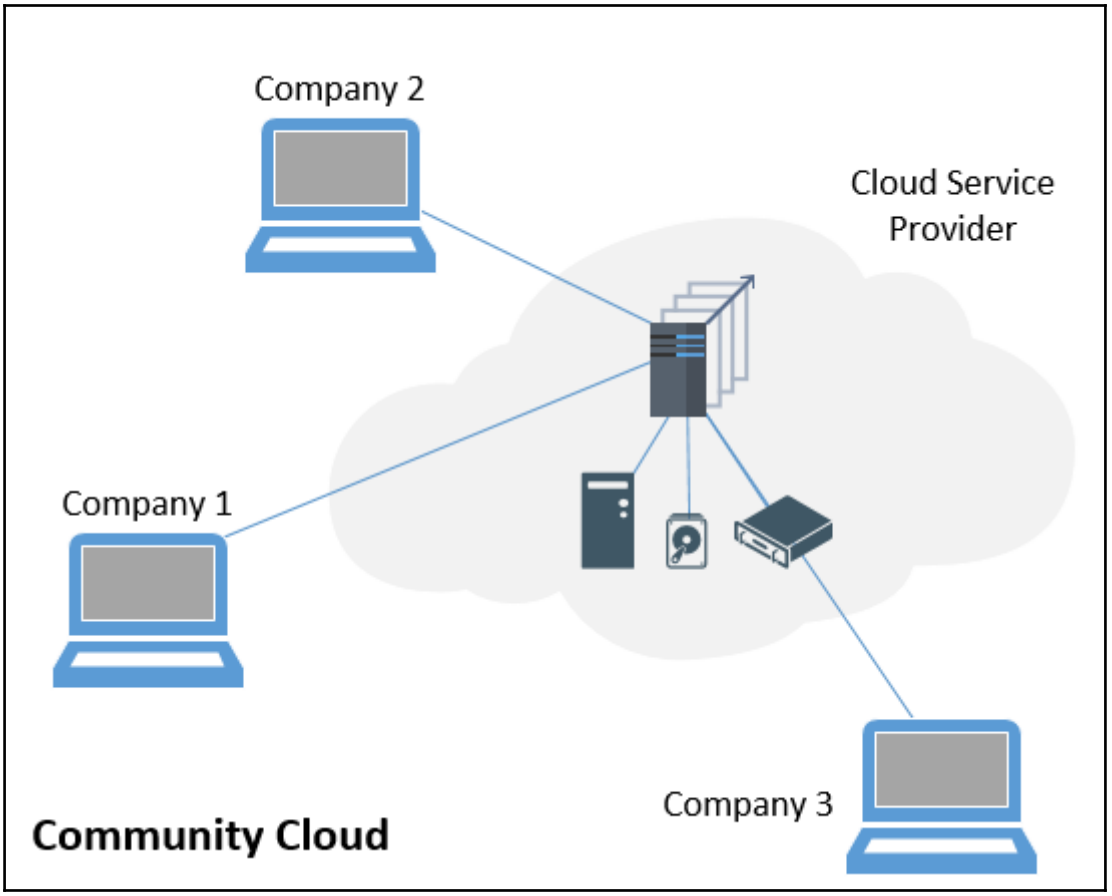
Chapter 11: Cloud Security Consideration

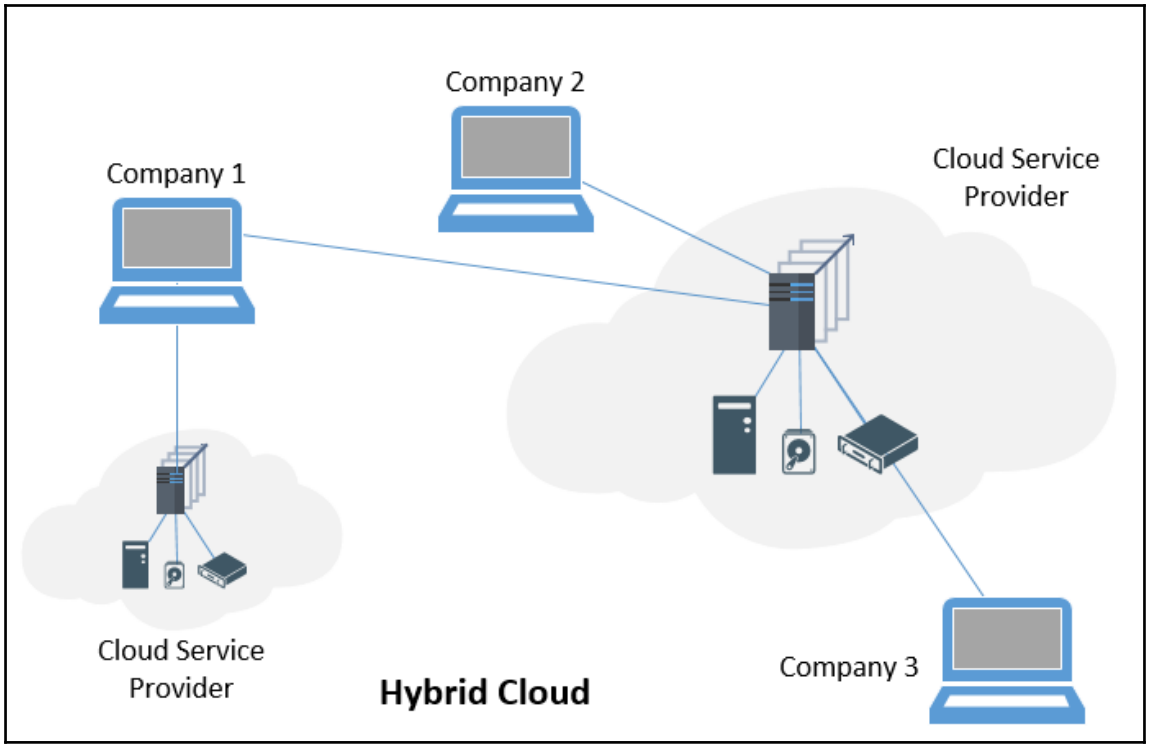


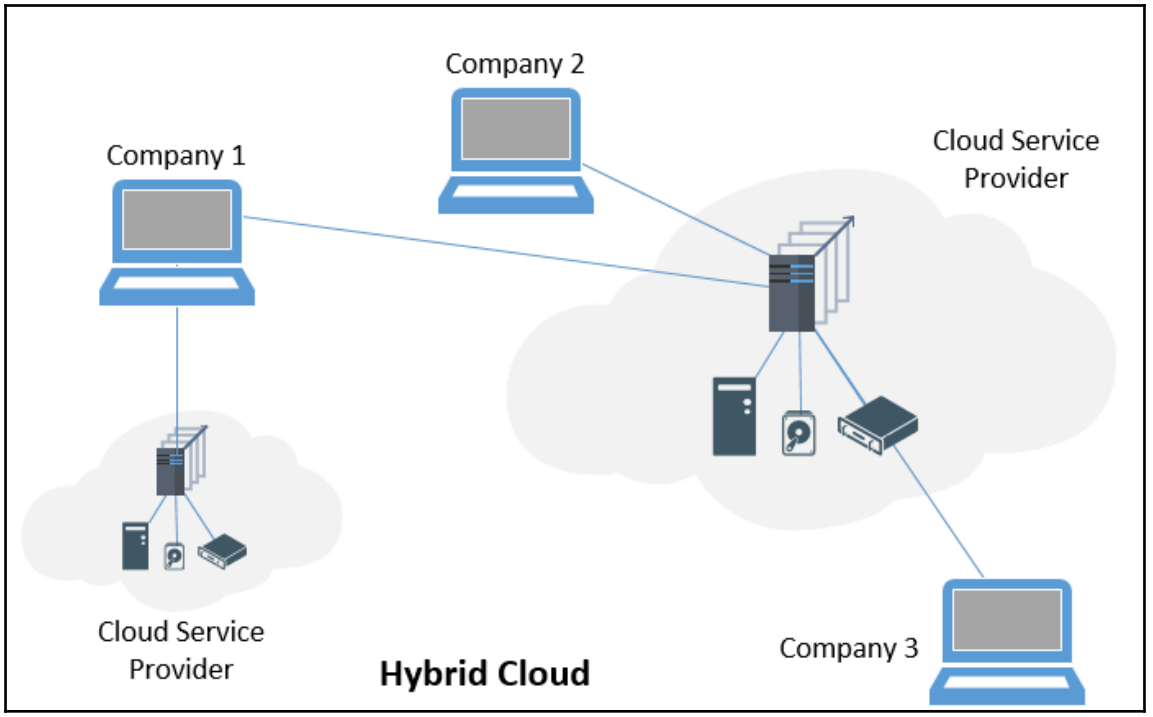


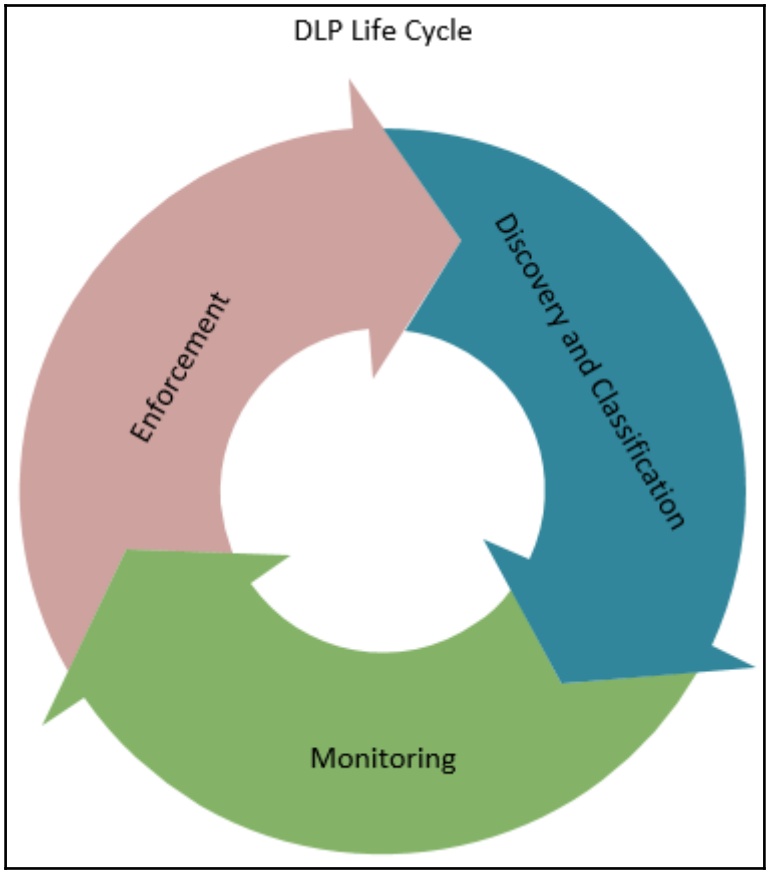

Internet
Cloud Service Provider
User
Cloud Service Provider
Application
Software as a Service (SaaS)

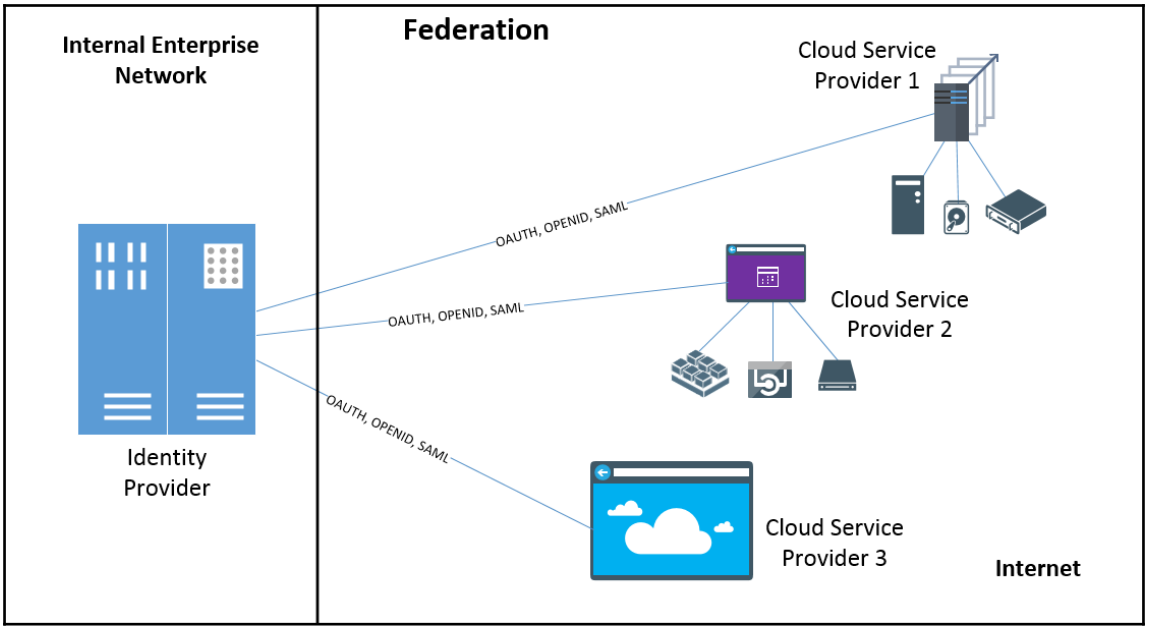

Company 2
Cloud Service Provider
Company 1
Company 3
Public Cloud

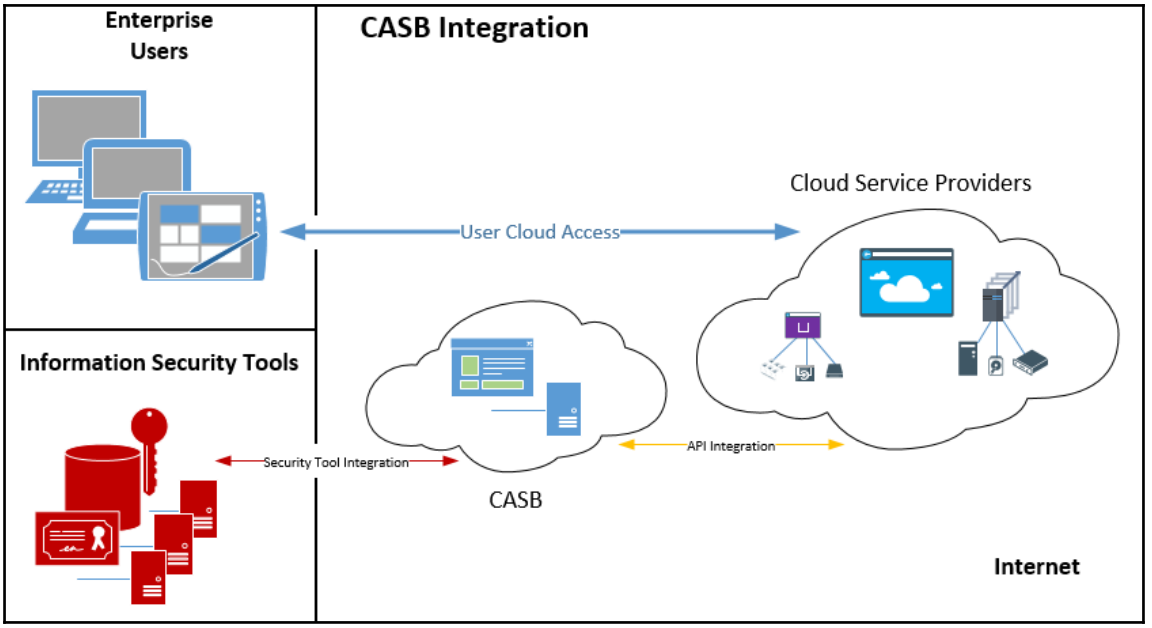

Company 2
Cloud Service Provider
Company 1
Company 3
Community Cloud


Company 2
Company 1
Cloud Service
Provider
Cloud Service
Provider
Company 3
Hybrid Cloud

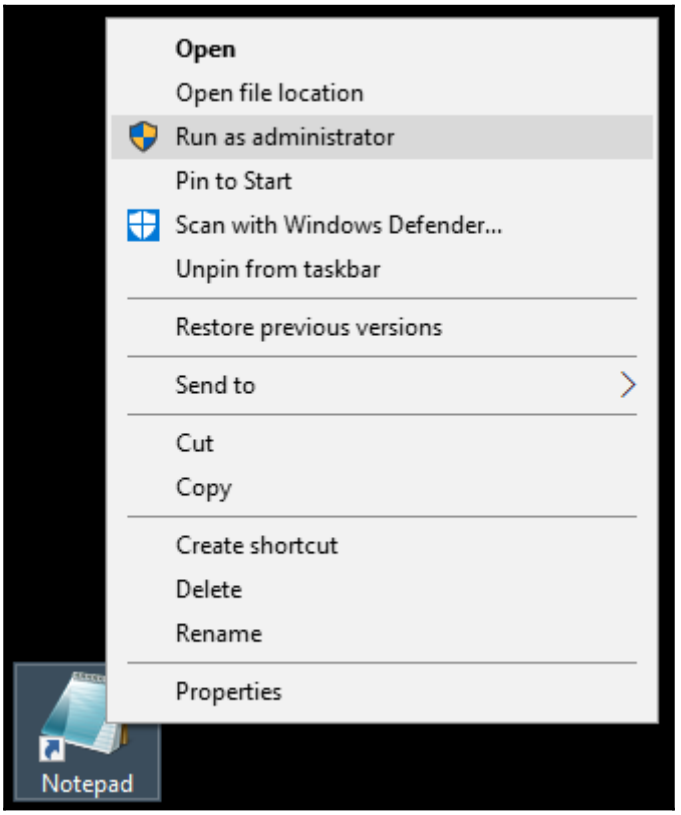

Company 2
Company 1
Cloud Service
Provider
Cloud Service
Provider
Hybrid Cloud
Company 3

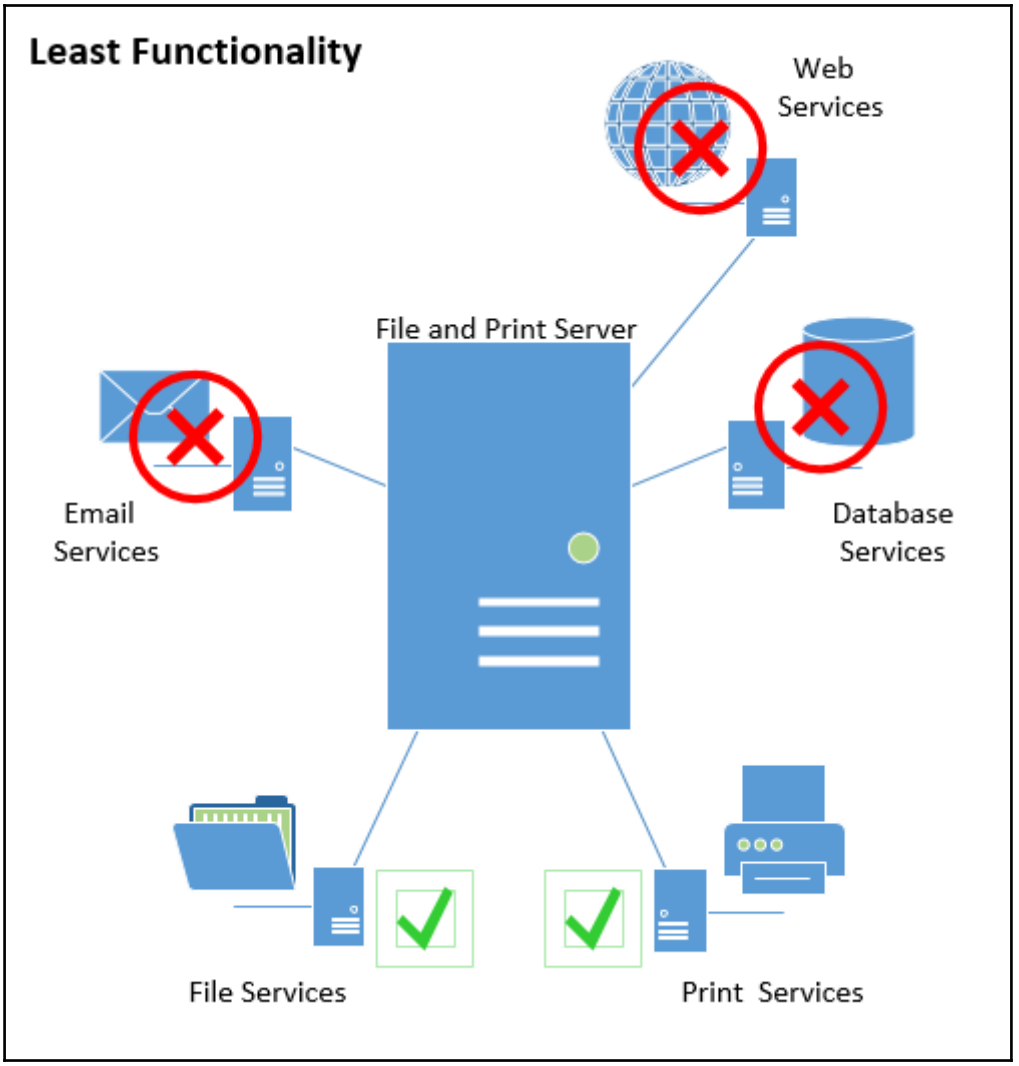

DLP Life Cycle
Enforcement
Discovery and Classification
Monitoring

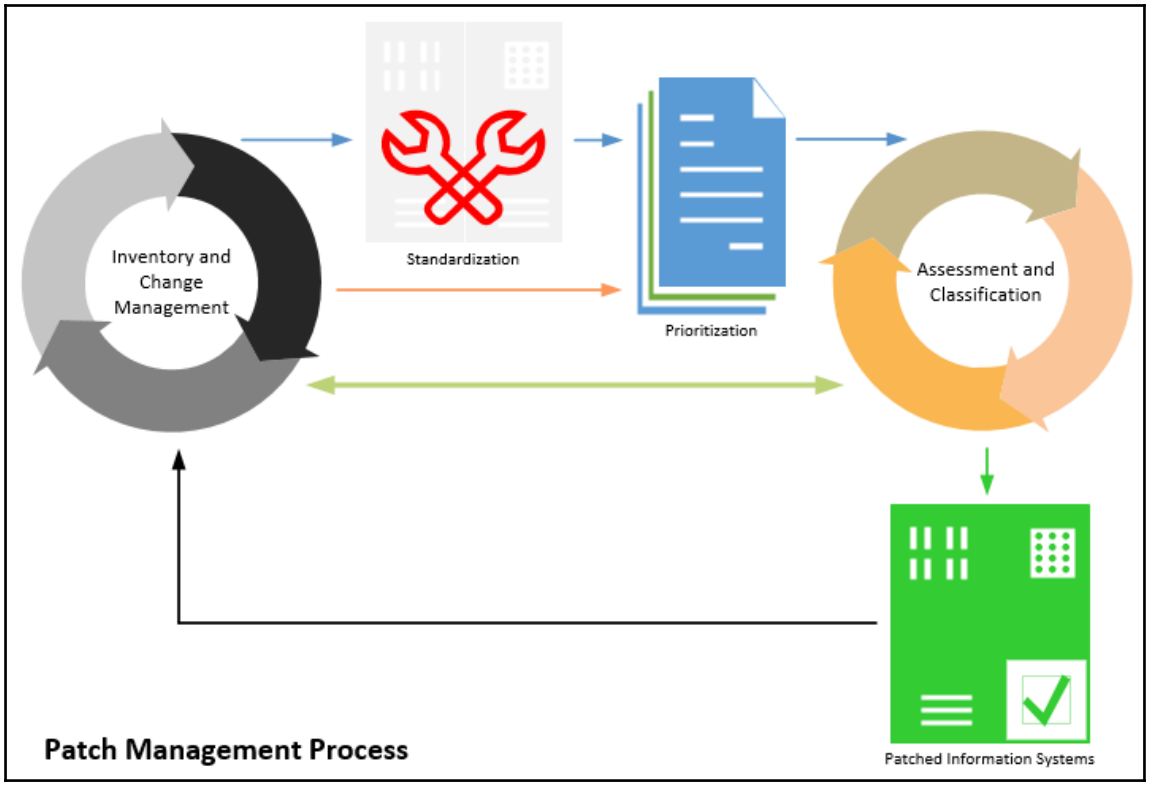

Internal Enterprise Network
Federation
Cloud Service Provider 1
OAUTH, OPENID, SAML
OAUTH, OPENID, SAML
Cloud Service Provider 2
OAUTH, OPENID, SAML
Identity Provider
Cloud Service Provider 3
Internet

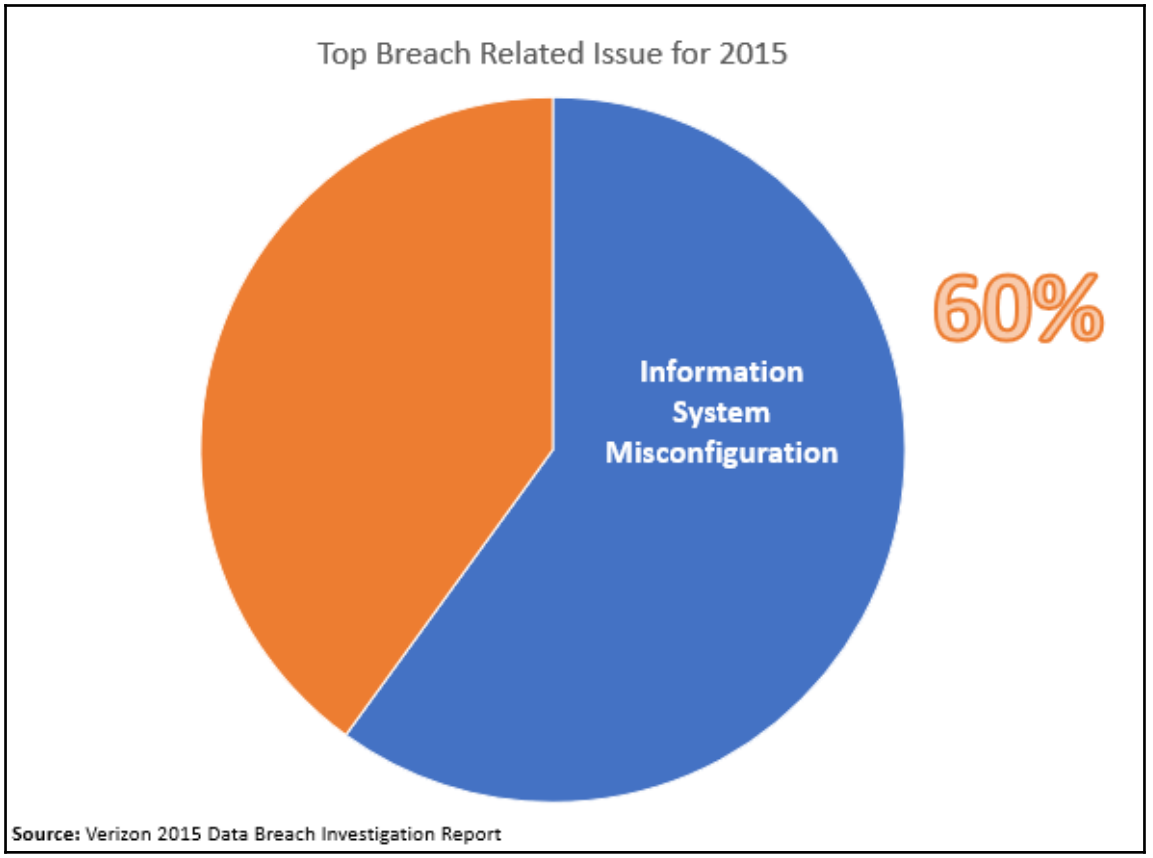

Enterprise Users
CASB Integration
Cloud Service Providers
User Cloud Access
Information Security Tools
Security Tool Integration
API Integration
CASB
Internet

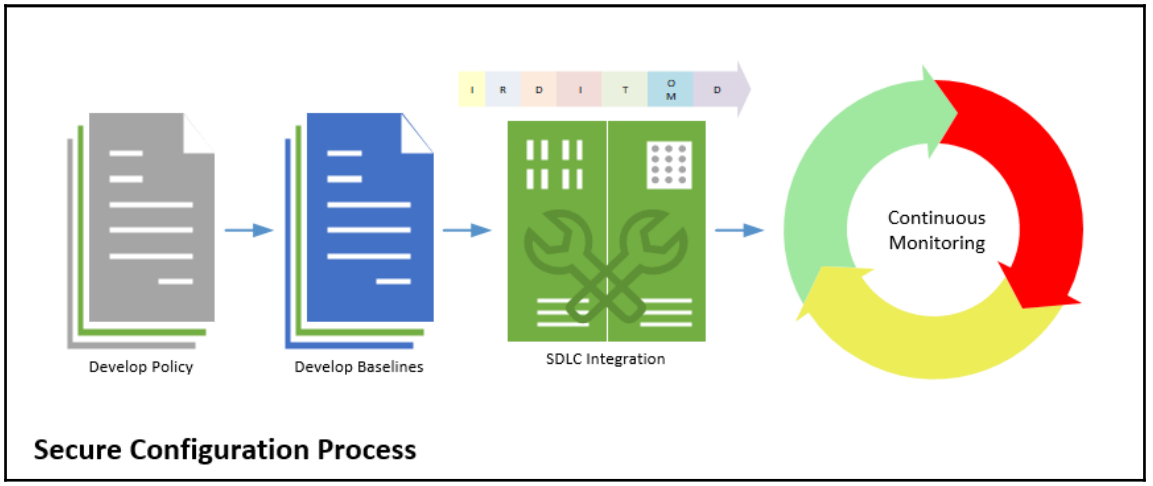
Chapter 12: Information and Data Security Best Practices

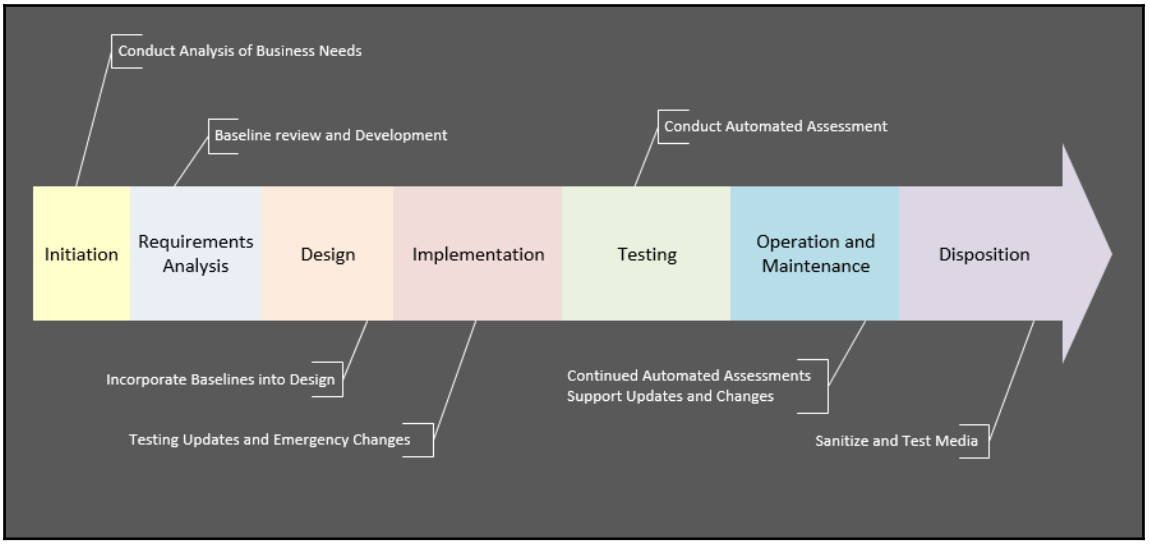


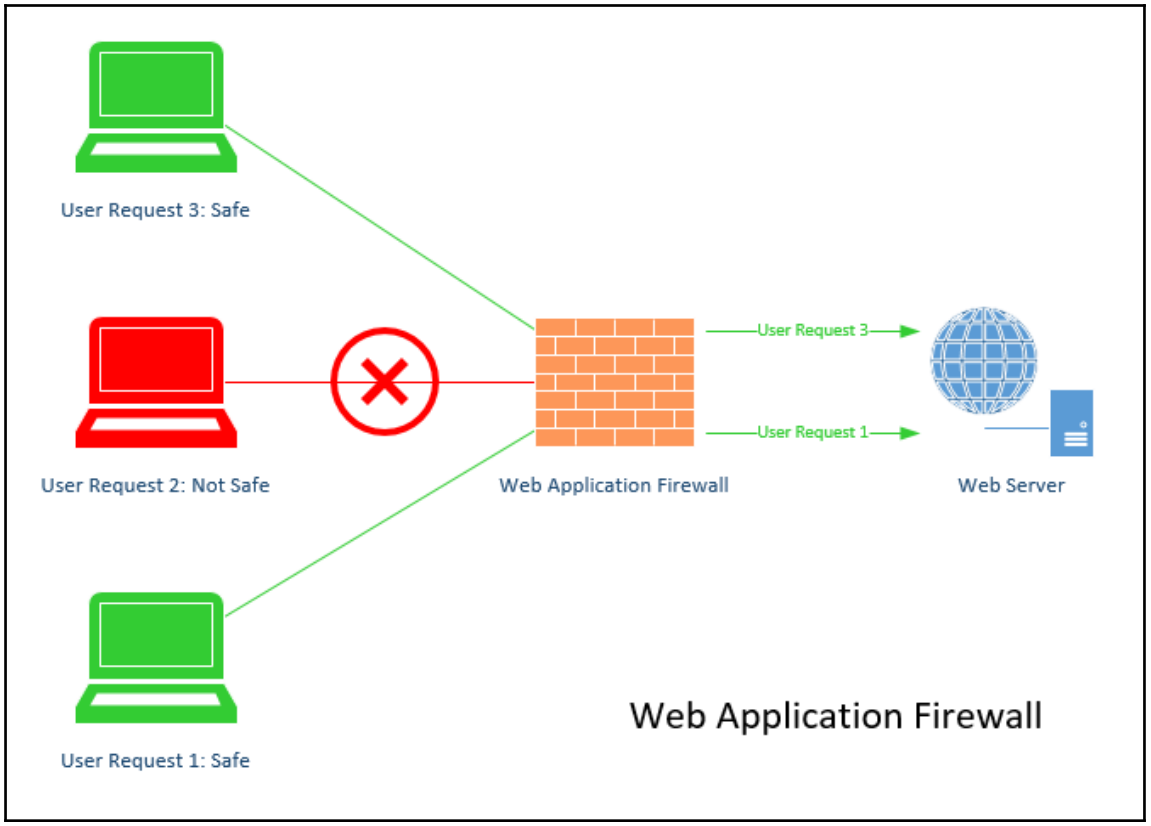

Least Functionality
Web
Services
File and Print Server
Email
Services
Database
Services
File Services
Print Services


Inventory and Change Management
Standardization
Prioritization
Assessment and Classification
Patched Information Systems
Patch Management Process


Top Breach Related Issue for 2015
Information System Misconfiguration
60%
Source: Verizon 2015 Data Breach Investigation Report


I R D I T O M D
Develop Policy
Develop Baselines
SDLC Integration
Continuous Monitoring
Secure Configuration Process


Conduct Analysis of Business Needs
Baseline review and Development
Conduct Automated Assessment
Initiation
Requirements Analysis
Design
Implementation
Testing
Operation and Maintenance
Disposition
Incorporate Baselines into Design
Testing Updates and Emergency Changes
Continued Automated Assessments
Support Updates and Changes
Sanitize and Test Media


User Request 3: Safe
User Request 2: Not Safe
User Request 1: Safe
Web Application Firewall
User Request 3
User Request 1
Web Server
Web Application Firewall