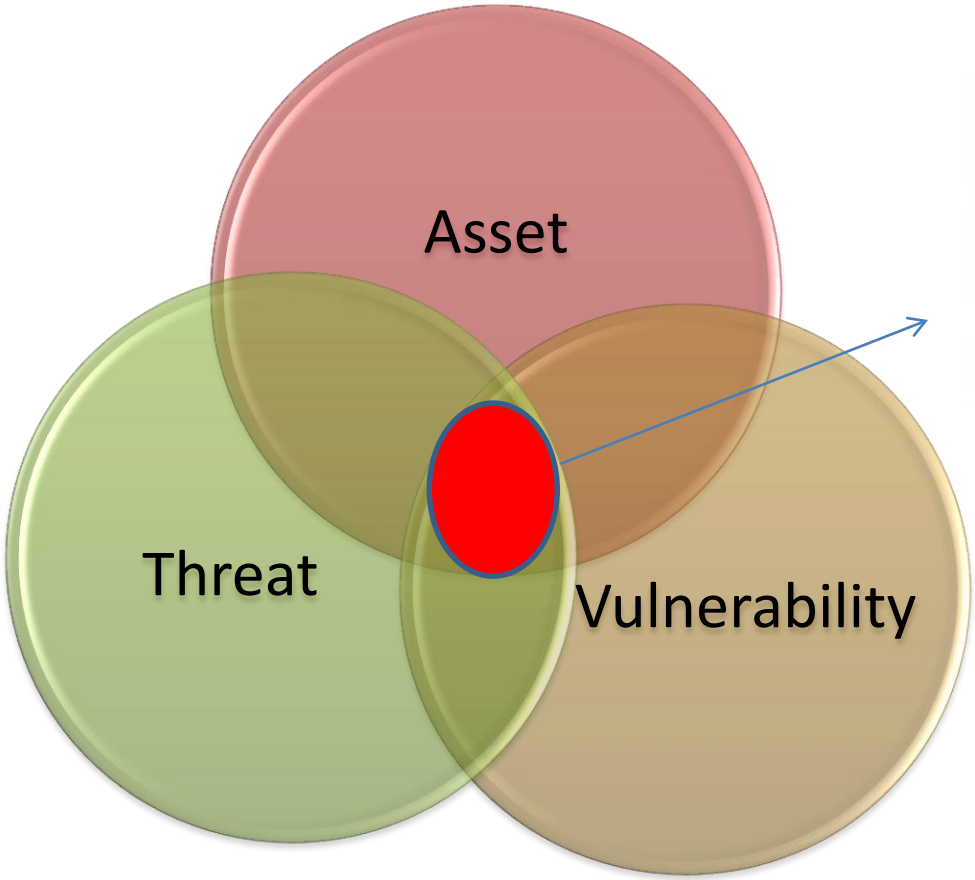
Critical Controls for Cyber Security

www.infogistic.com

Understanding Risk



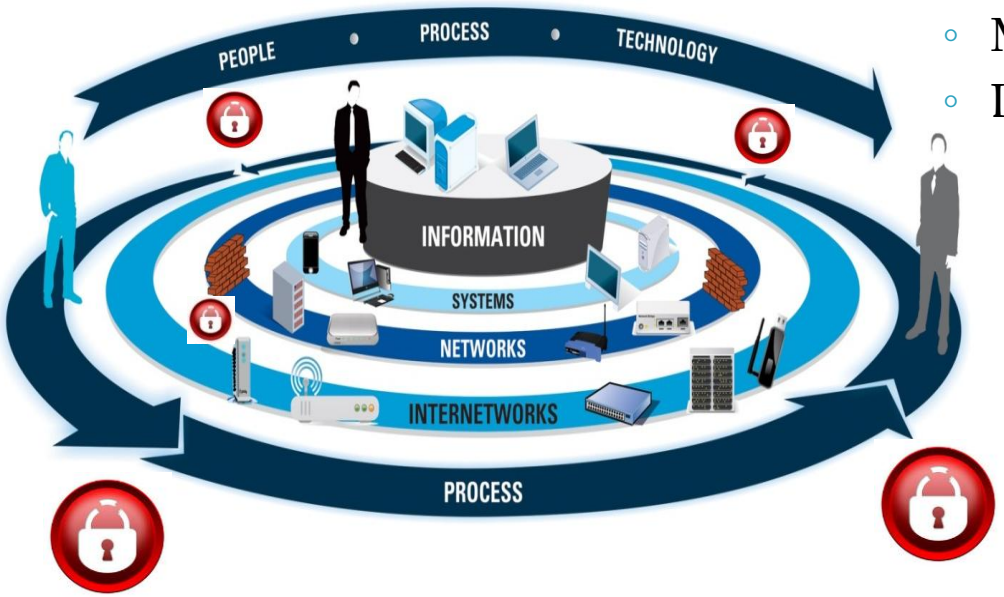
Managing Risks

- Systematic Approach for Managing Risks
  - Identify, characterize threats
  - Assess the vulnerability of critical assets to specific threats
  - Determine the risk
  - Identify/implement controls to reduce risks

Enterprise IT Infrastructure

- Social Engineering
- Insider Threats
- Vendors & Employees

- Key Loggers
- Hacking
- Weak Algorithms
- Malicious code
- Denial of Service

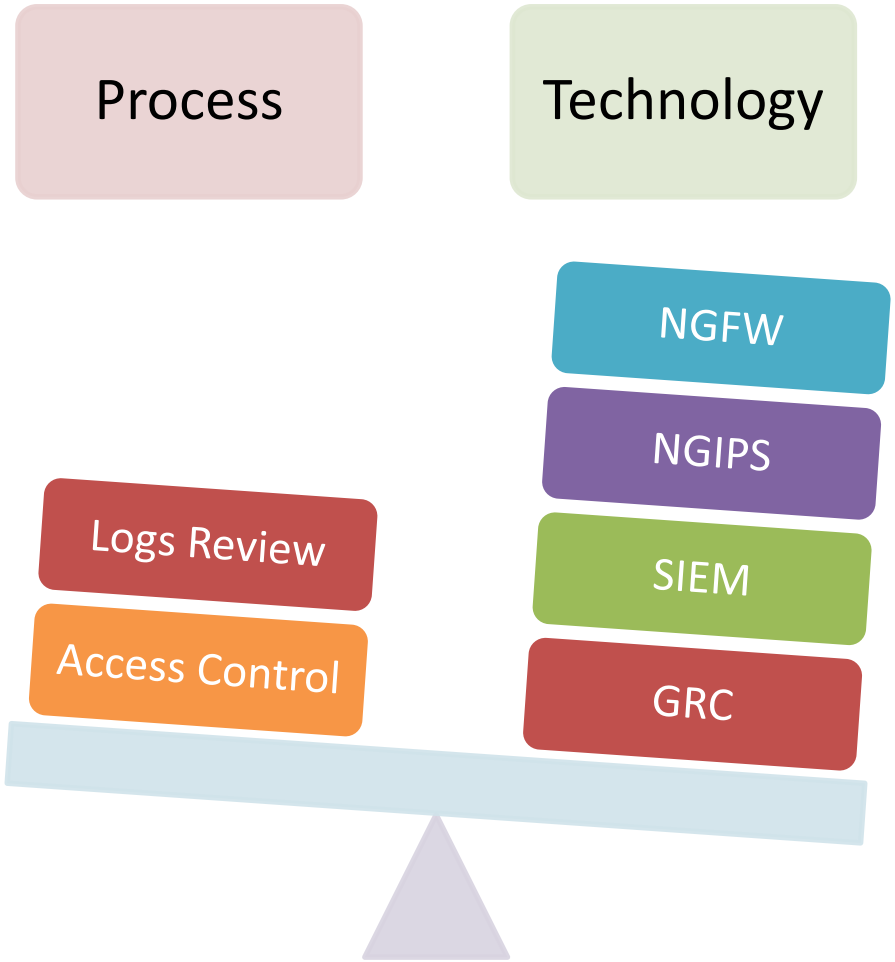


- Natural Disasters
- Access Controls

Implementation of Controls

- Controls are identified and applied to reduce the risk
- Controls can be of two types
  - Technology Based
  - Process Based
- Can be categorized across
  - Technical (IPS, IDS, Firewall, DLP, IAM, SIEM, etc)
  - Physical (Bio Metrics, Electronic Locks etc, Barriers etc)
  - Administrative (Policies, Procedures, Manuals)

Balance of Technology & Process



20 Critical Controls for Cyber Security

- Background
- Joint Efforts of
  - US Department of Defense
  - Nuclear Laboratories of US Department of Energy
  - US CERT
  - US Department of Homeland Security
  - Defense Signal Directorate – Australia
  - Centre for Protection of Critical Infrastructure – UK
  - National Institute of Standards & Technology (NIST)
  - SANS Institute
- Leading to “Consortium for Cyber Security Action”

20 Critical Controls for Cyber Security

- Critical Control 1: Inventory of Authorized and Unauthorized Devices
- Critical Control 2: Inventory of Authorized and Unauthorized Software
- Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Critical Control 4: Continuous Vulnerability Assessment and Remediation
- Critical Control 5: Malware Defenses
- Critical Control 6: Application Software Security
- Critical Control 7: Wireless Device Control
- Critical Control 8: Data Recovery Capability
- Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps
- Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
- Critical Control 12: Controlled Use of Administrative Privileges
- Critical Control 13: Boundary Defense
- Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs
- Critical Control 15: Controlled Access Based on the Need to Know
- Critical Control 16: Account Monitoring and Control
- Critical Control 17: Data Loss Prevention
- Critical Control 18: Incident Response and Management
- Critical Control 19: Secure Network Engineering
- Critical Control 20: Penetration Tests and Red Team Exercises

Categorizing Critical Controls

Control	Process	Technology
Inventory of Authorized and Unauthorized Devices		
Inventory of Authorized and Unauthorized Software		
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers		
Continuous Vulnerability Assessment and Remediation		
Malware Defenses		
Application Software Security		
Wireless Device Control		

Categorizing Critical Controls

Control	Process	Technology
Data Recovery Capability		
Security Skills Assessment and Appropriate Training to Fill Gaps		
Secure Configurations for Network Devices such as Firewalls, Routers, and Switches		
Limitation and Control of Network Ports, Protocols, and Services		
Controlled Use of Administrative Privileges		
Boundary Defense		
Maintenance, Monitoring, and Analysis of Audit Logs		

Categorizing Critical Controls

Control	Process	Technology
Controlled Access Based on the Need to Know		
Account Monitoring and Control		
Data Loss Prevention		
Incident Response and Management		
Secure Network Engineering		
External Penetration Tests & Contextual Risk Management		

Vulnerability Assessment & Continuous Remediation

Technology

- Acquire and Implement a Vulnerability Scanning Tool
- Emphasis on database, networks, web , servers, applications, SCADA(if applicable)

Process

- Frequency of scanning
- Reporting Mechanism
- Action Plans
- Contingency planning for patch management
- Compare results with previous scans
- Strict Monitoring/Auditing of Access

Application Software Security

Technology

- For Web Applications install Web Application Firewall
- For other applications have a Next Generation Firewall

Process

- In-house developed applications must be tested for security and code review.
- Test in-house-developed and third-party-procured web and other application software for coding errors and malware insertion,

Security Skills Assessment

Technology

- Online Training Programs for Security Awareness

Process

- Develop a Security Awareness Program at all levels
- KPI must be defined
- Security awareness must be enforced through HR
- Capability and Capacity Development

Data Loss Prevention

Technology

- Install and implement a Data Loss Prevention Solution

Process

- Policies and Procedures
- Classification of Information
- Business Work Flow
- Incident Management

Governance Risk & Compliance

Technology

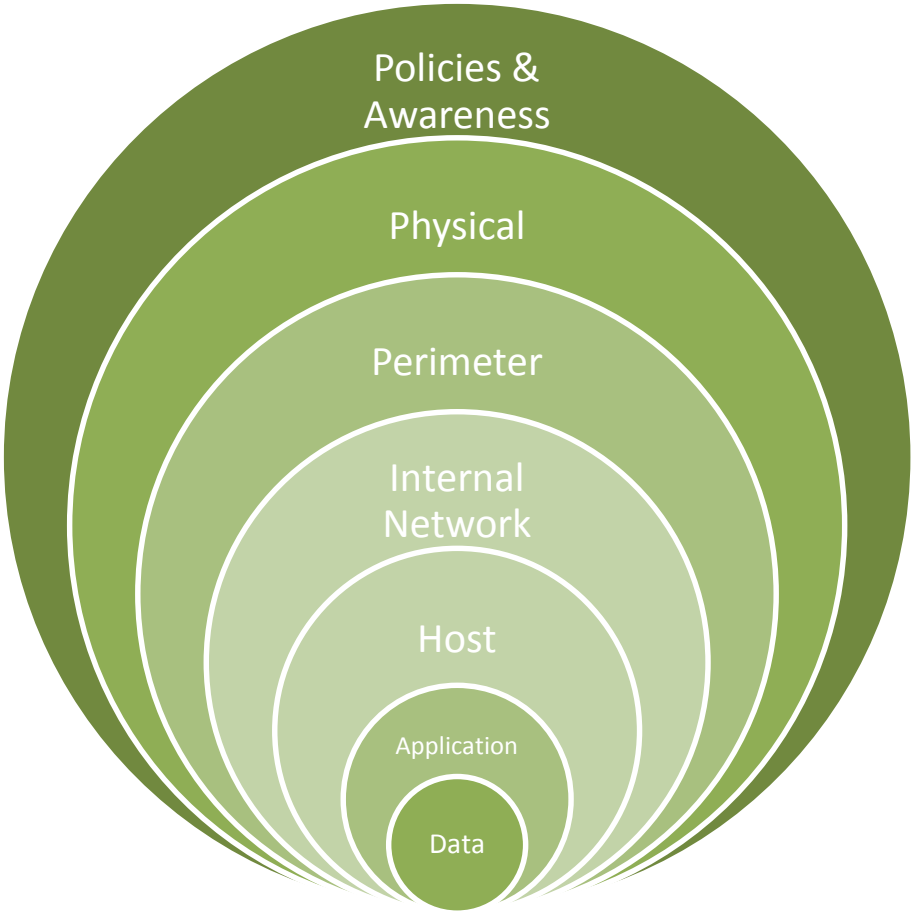
- Implement a GRC suite
- Modules may include
  - Policy Management
  - Risk Management
  - Incident Management
  - Vendor Management
  - Audit Management

Process

- Business Process Mapping
- Risk Management
- Work Flow Definitions
- Integrity Monitoring

Furnishing Technology

Security Analytics
Smart ID
Email Security
IAM
Malware Analysis
Vulnerability Scanning
Encryption



GRC
BMS
NGIPS
NGFW
Host Based Protection
X factor Authentication
DLP

Symptoms of Vulnerable Organizations

- I understand process, I understand technology, but how to integrate them?
- Which best practices suit my organization?
- There are too many, I am confused?
- We are too busy in our day to day security operations?
- No one follows the process here?
- Frequently change the security technology in place?

Answer

Enterprise Security Framework