Business Security Strategy

Clinton Thomson

Agenda

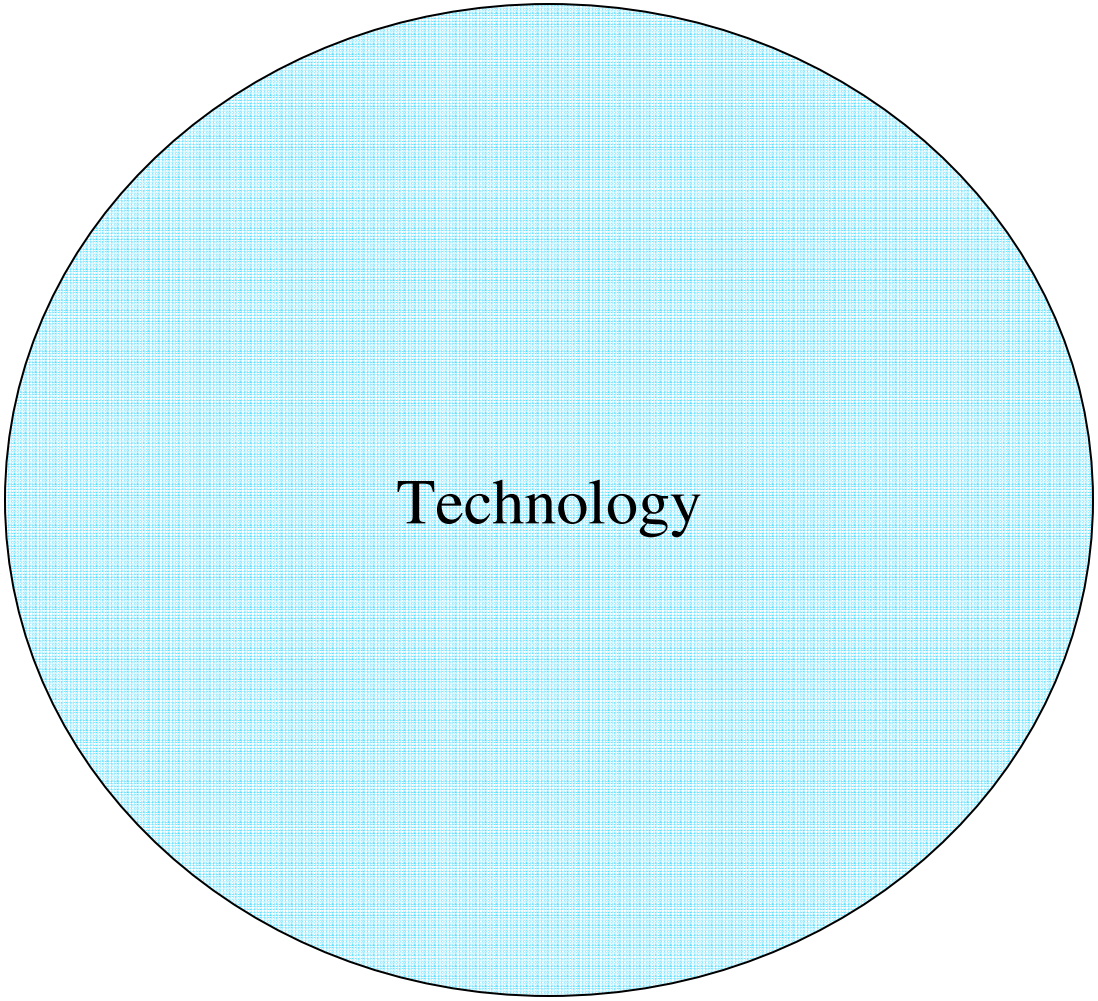
- What's Involved
- Knowing the elements
- Risk Management
- Defence in Depth
- Operations Maturity

Getting and Staying Secure

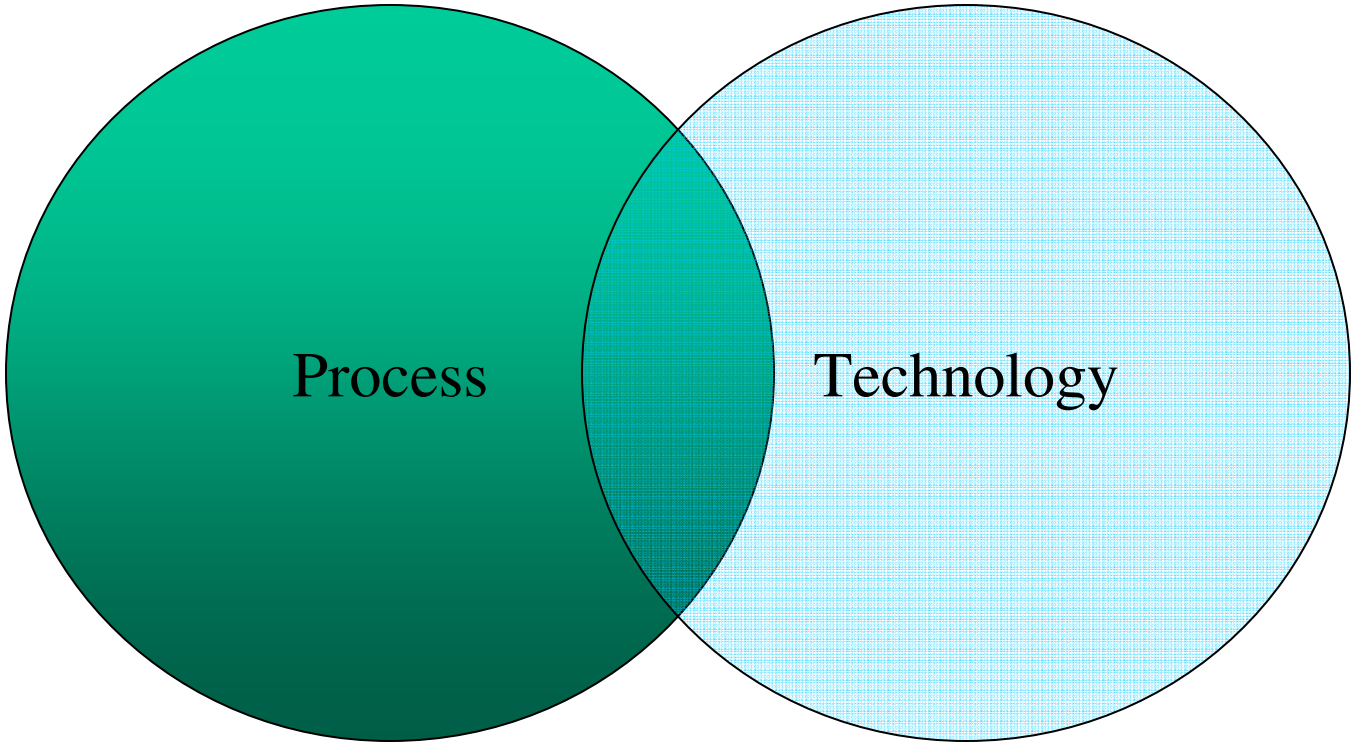
- ⚠ **Develop IT Security Policy**
- ⚠ **Defense in Depth Strategy**
- ⚠ **Server Lockdown**
- ⚠ **Anti-Virus**
- ⚠ **Backup and Restore**
- ⚠ **Patch Management**
- ⚠ **Audit and Intrusion Detection**
- ⚠ **Incident Response Plan**

Knowing the elements…

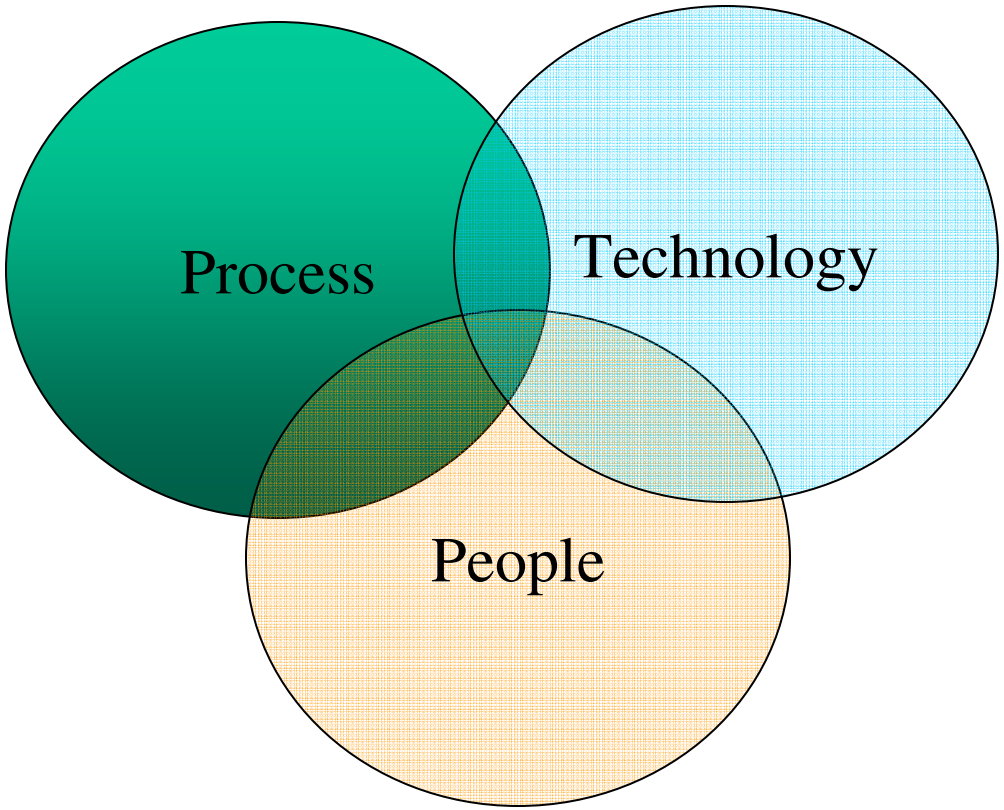
Knowing the elements…



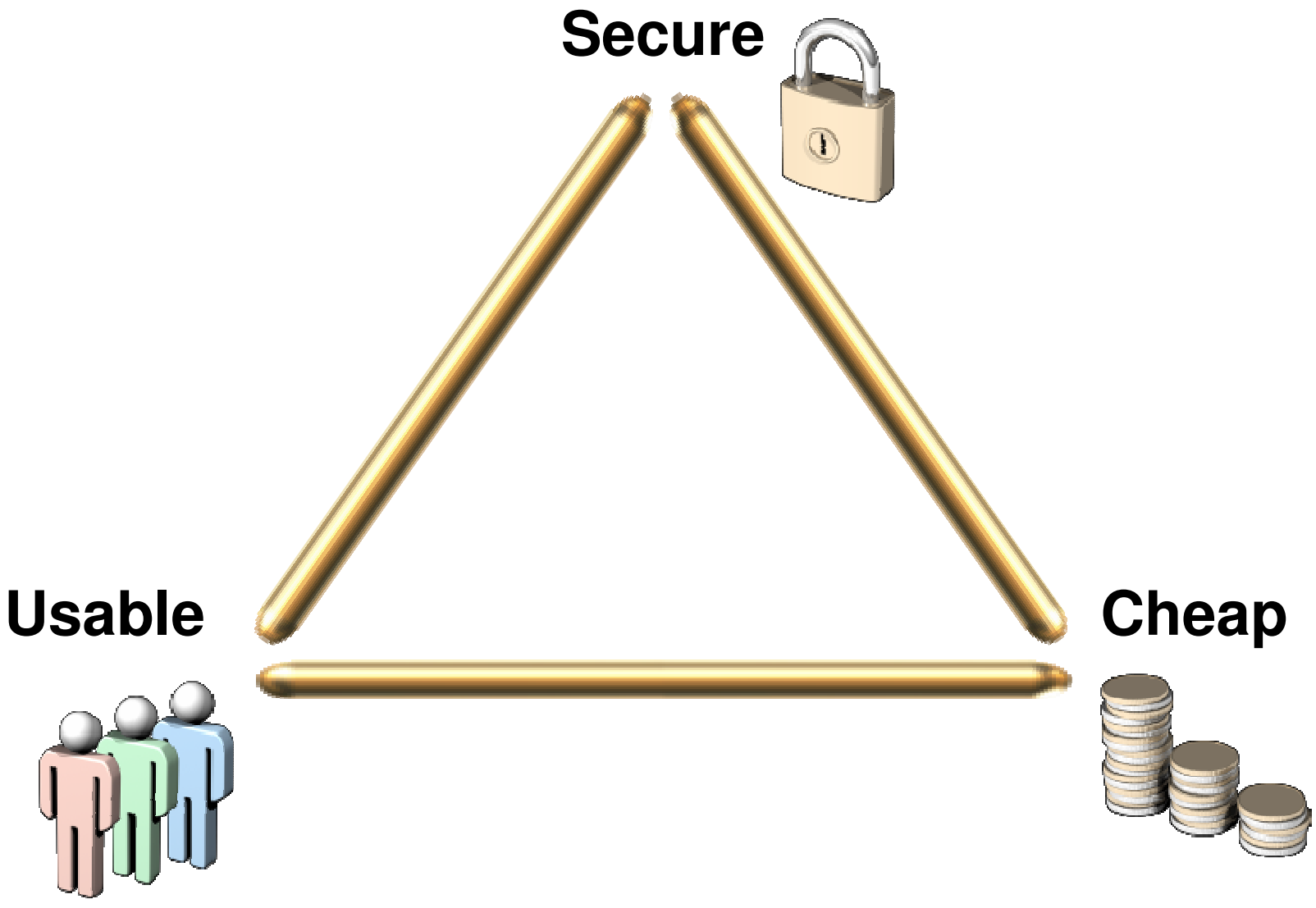
Knowing the elements…



Knowing the elements…



Knowing the elements…



Risk Management

Risk Management

- **Resources**
  - People, Applications, Hardware

Risk Management

- **Resources**
  - People, Applications, Hardware
- **Threats**
  - Natural & Physical, Unintentional, Intentional

Risk Management

- **Resources**
  - People, Applications, Hardware
- **Threats**
  - Natural & Physical, Unintentional, Intentional
- **Vulnerabilities**
  - Poor Access Control, Human Elements, Communications, Hardware and Software

Risk Management Cont…

- **Exploits**
  - Penetration, Data Mining, Social Eng

Risk Management Cont…

- **Exploits**
  - Penetration, Data Mining, Social Eng
- **Result of Exploit**
  - Confidentiality, Integrity, Availability

Risk Management Cont…

- **Exploits**
  - Penetration, Data Mining, Social Eng
- **Result of Exploit**
  - Confidentiality, Integrity, Availability
- **Countermeasures**
  - Intrusion Detection, Firewalls, Audit, Patching, Lockdown, Process and Procedure, Training and Awareness

Defense in Depth

- **People Issue**
- **Technology Does not work here**
- **Path of least resistance**

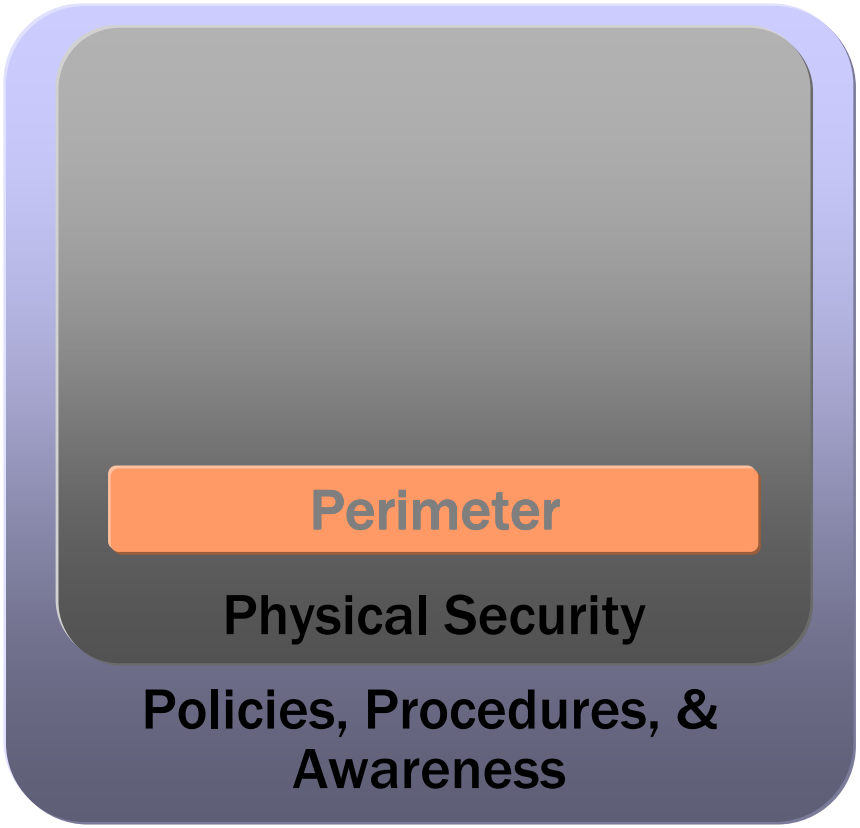
Defense in Depth

- People Issue
- Technology Does not work here
- Path of least resistance

Defense in Depth

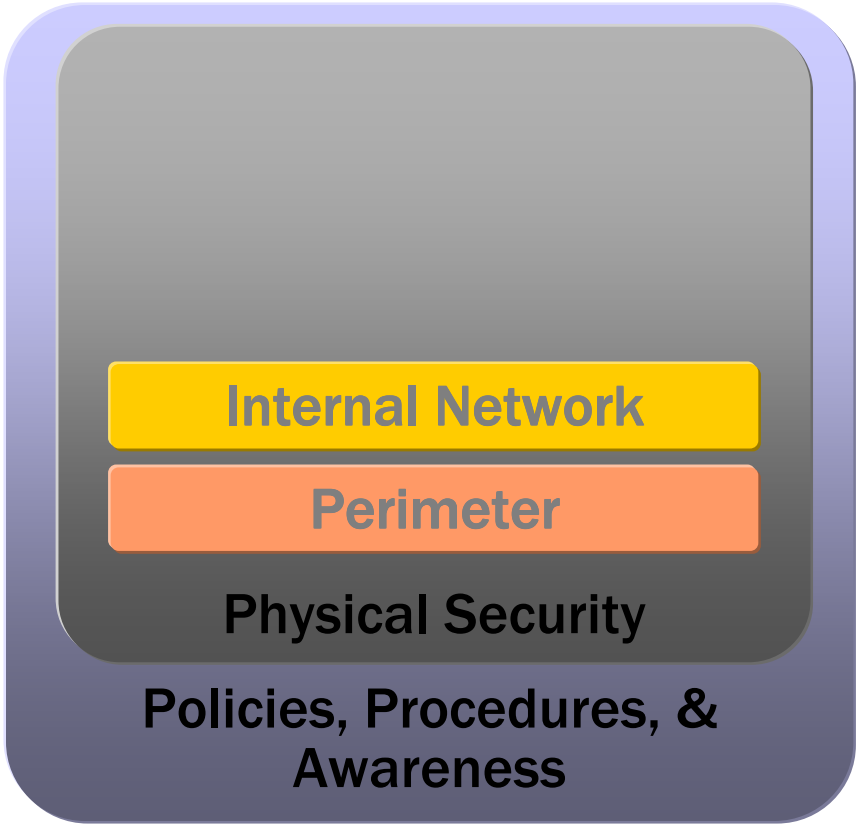
- **Physical Security**
  - Guard
  - Access Control
  - Camera Systems
  - Alarms

Defense in Depth



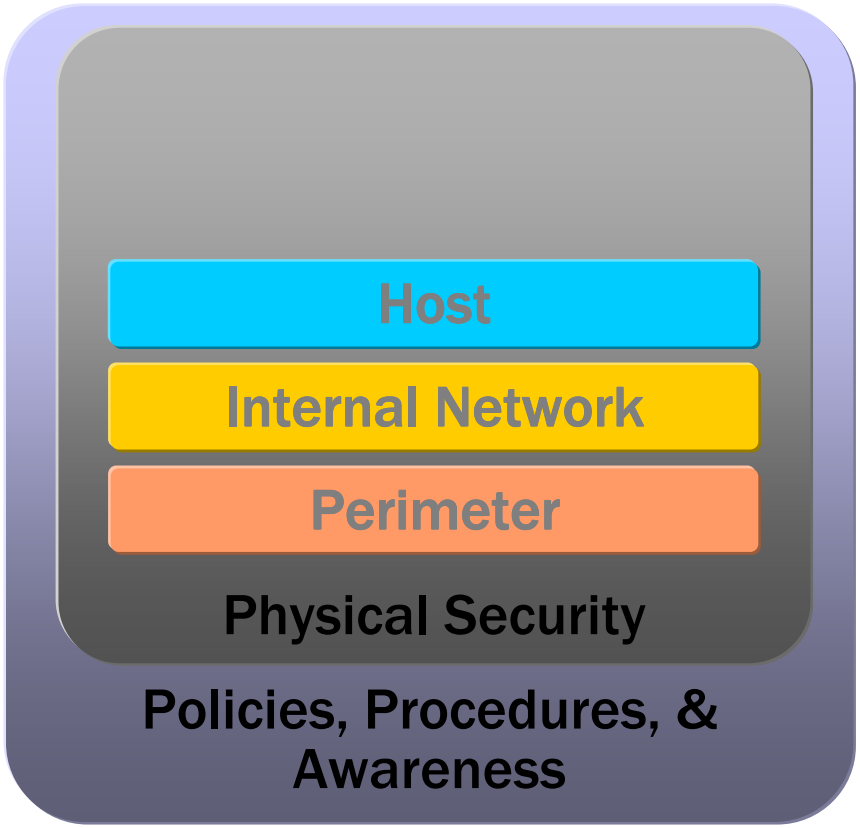
- **Perimeter**
  - IDS now IPS
  - Firewalls
  - Content\Application Filtering
  - Quarantine

Defense in Depth



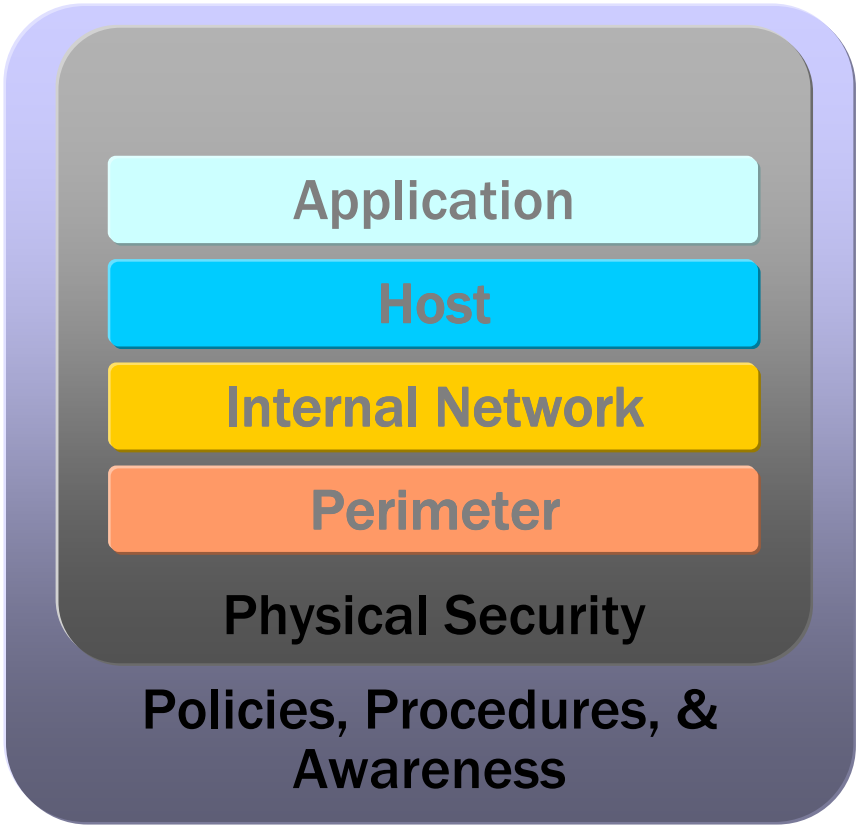
- **Internal Network**
  - VLANs
  - Firewalls
  - ACLs
  - NAC\NAP
  - Audit
  - Event Management
  - Config Management

Defense in Depth



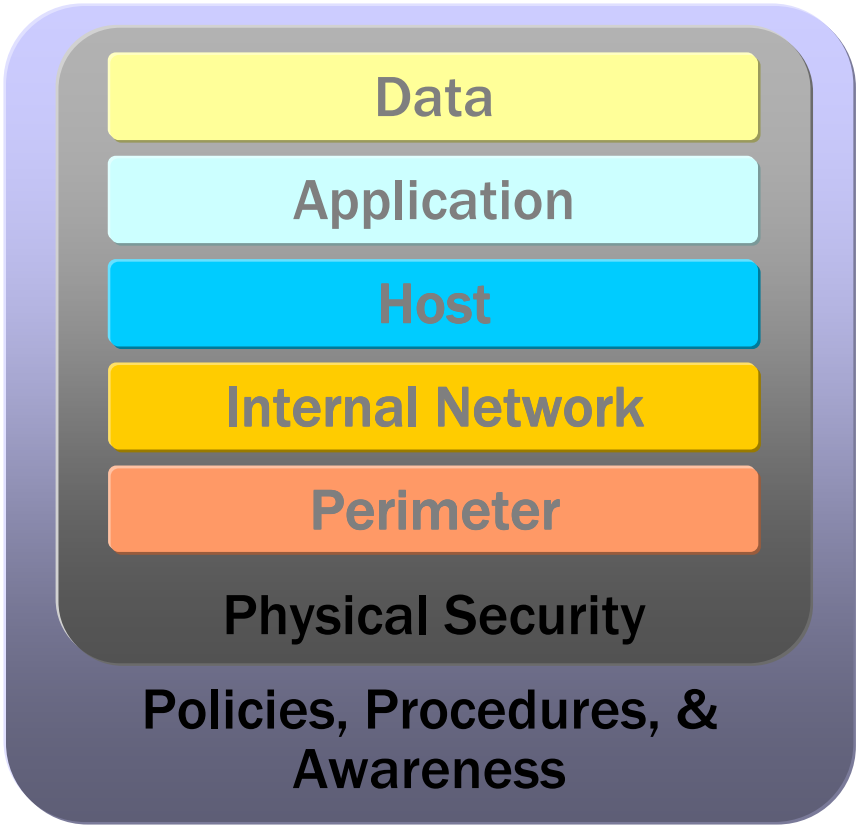
- **Host**
  - HIDs
  - Server Isolation
  - Auditing
  - Event Management
  - Hardening
  - Firewall
  - Anti Virus
  - Patch Management
  - Configuration Management

Defense in Depth



- **Application**
  - Auditing
  - Authentication
  - Anti Virus
  - Patch Management
  - Hardening or Secure Apps
  - Configuration Management
  - Backups
  - Business Continuity

Defense in Depth



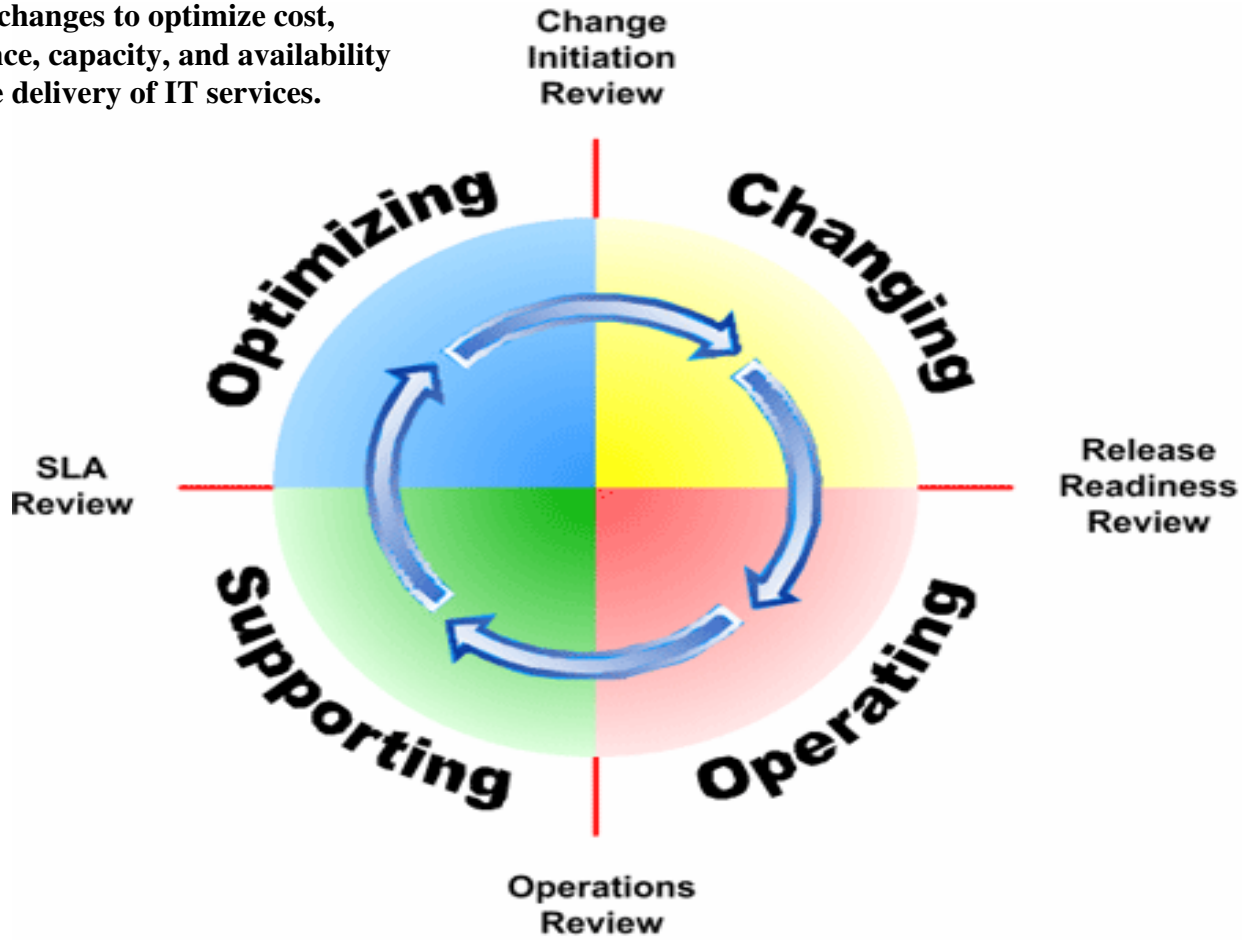
- **Data**
  - Encryption\Hashing
  - ACLs
  - Anti Virus
  - Secure App Coding
  - Backups
  - Business Continuity

Microsoft Operations Framework

www.microsoft.com/mof

Microsoft Operations Framework

Drive changes to optimize cost, performance, capacity, and availability in the delivery of IT services.

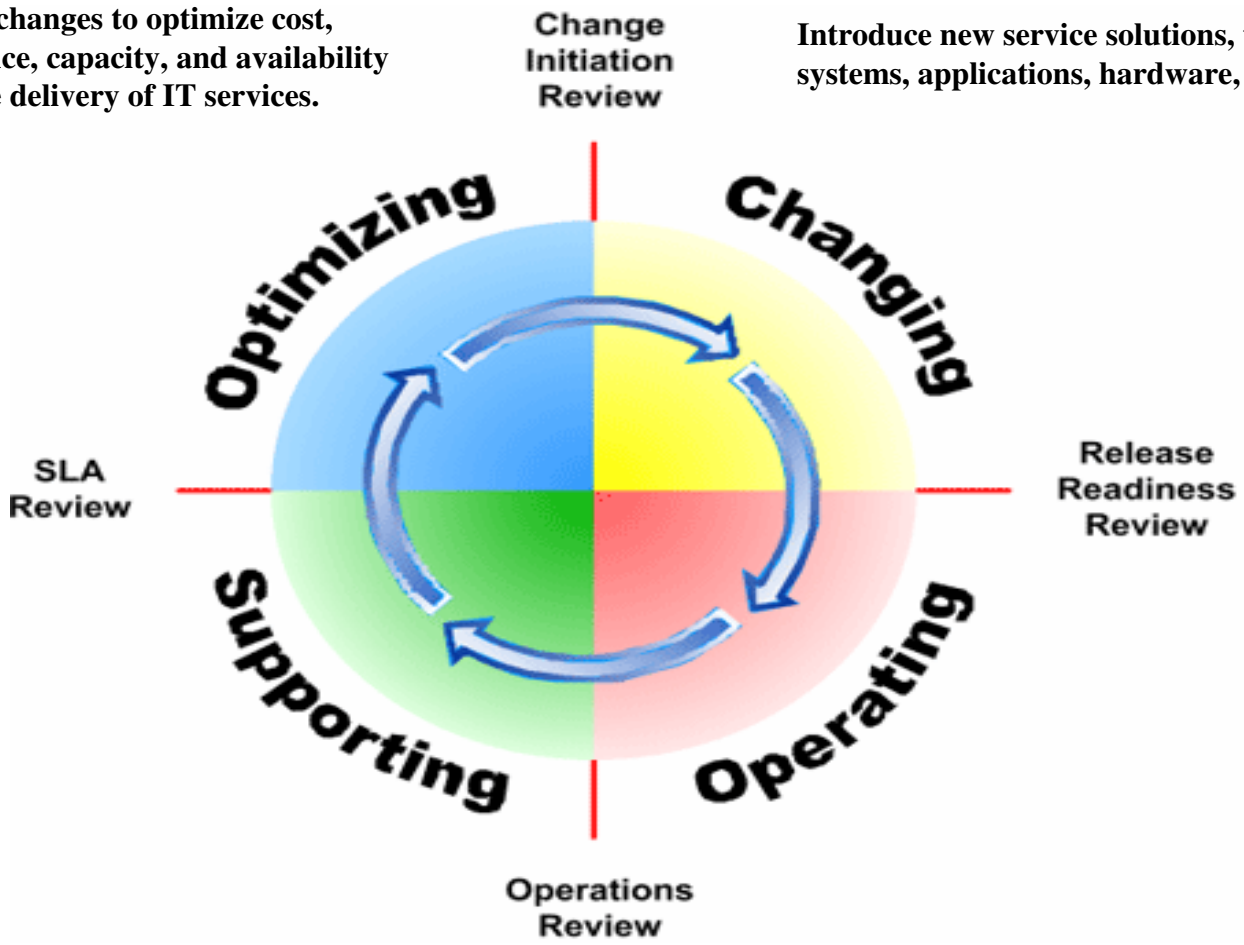


www.microsoft.com/mof

Microsoft Operations Framework

Drive changes to optimize cost, performance, capacity, and availability in the delivery of IT services.

Introduce new service solutions, technologies, systems, applications, hardware, and processes.



www.microsoft.com/mof

Microsoft Operations Framework

Drive changes to optimize cost, performance, capacity, and availability in the delivery of IT services.

Introduce new service solutions, technologies, systems, applications, hardware, and processes.

Execute day-to-day tasks effectively and efficiently.

www.microsoft.com/mof

Microsoft Operations Framework

Drive changes to optimize cost, performance, capacity, and availability in the delivery of IT services.

Introduce new service solutions, technologies, systems, applications, hardware, and processes.

Resolve incidents, problems, and inquiries quickly.

Execute day-to-day tasks effectively and efficiently.

www.microsoft.com/mof

Review

- Lots of thinking! Consider all aspects of technology, process, people, cost, functionality and security
- Technology is the easy part, people are a little harder to control
- Iterative defence in depth, caveat of top heavy dependant layers
- Consider the evolving business

Questions?

References

- **Security Operations Guide**
  - http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=9989D151-5C55-4BD3-A9D2-B95A15C73E92
- **Microsoft Operations Framework**
  - http:///www.microgsoft.com/mof
- **Microsoft Security Centre**
  - http://www.microsoft.com/security/guidance/default.mspx
- **Microsoft Patterns and Practices**
  - http://msdn.microsoft.com/practices
- **Microsoft IT Showcase**
  - http://www.microsoft.com/itshowcase

- **Added Items**
  - Jericho Forum - http://www.opengroup.org/jericho/
  - How to help your employees develop better security habits http://www.microsoft.com/midsizebusiness/securityrisk.mspx