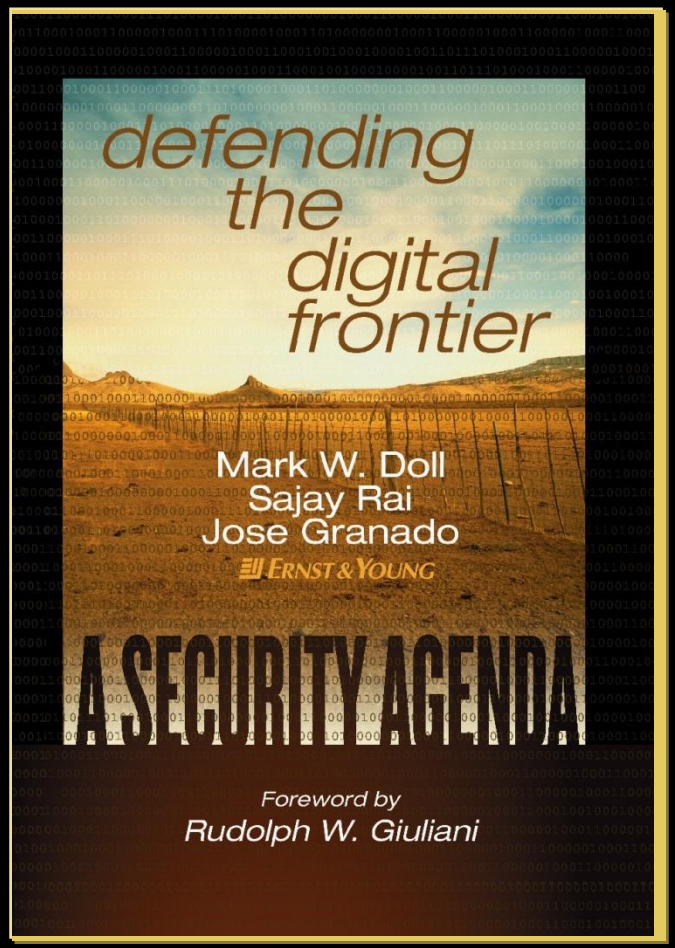
Defending the Digital Frontier



Oakland University
June 11, 2013

What is Information Security?

- Information is one of the most crucial and expensive assets in an organization.
- Mechanisms need to be in place to protect the loss, alteration and/or unauthorized access to this asset.

What is Information Security -definition

Information system security is the science and study of methods of protecting information in computer and communication systems against unauthorized disclosure, transfer, modification and destruction whether accidental or intentional.

SECURITY REQUIREMENTS: 3 Key Areas

1. Types of Information to protect:
   - Company Information / trade secrets
   - Customer Information
   - Credit Card data / Personal Data / IT Infrastructure

2. Threats to protect against:
   - Cyber vandalism
   - Disgruntled employees
   - Industrial spies
   - Negligent system administrators

SECURITY REQUIREMENTS:

(3 key areas)

3. Activities to protect against :
   - Unauthorized data access
   - Intentional or unintentional alteration and/or deletion of data
   - Denial of service (DOS)
   - Fraud

ADVERSARIES

SECURITY ADVERSARIES

- Disgruntled & Snooping Employees (INTERNAL)
- Negligent system administrator (INTERNAL)
- Foreign Governments (EXTERNAL)
- Press & Organized Crime (EXTERNAL)
- Terrorist groupings (EXTERNAL)

TYPE OF ATTACKS OR THREATS

- Fraud and Scams (Financially motivated)
- Destructive Attacks (Virus, Worms, Trojan Horses, Time bombs etc…)
- Identity theft (Impersonation/masquerading)
- Intellectual property/ document theft (Espionage)
- Industrial espionage (Financially motivated)
- Privacy violation and Publicity attacks (Hacking & Defacement)

PILLARS OF INFORMATION SECURITY – CIA and More

- **C**onfidentiality
- **I**ntegrity
- **A**vailability

- Non-Repudiation
- Auditing

CONFIDENTIALITY MECHANISM
(Secret / Secure ?)

- Software Encryption
  - Symmetric encryption: private key (DES).
  - Asymmetric encryption: public key (PKI).

- Hardware Encryption
  - DATA 6, 8, 11 (Line Encryption).

INTEGRITY MECHANISMS
(Is it still the same ?)

- Protecting the content of a data packet.
- No changes were made to the data packet.
- Message authentication code (MAC).
- Checksums (Documents).

Example – Integrity MAC

This document contains encrypted text!

In order to check the integrity of the message above we could use the following method:

- Calculate the number of vowels = 10
- Calculate the number of spaces = 4
- Calculate the number of punctuation marks = 1
- Calculate the number of words in total = 5

Our MAC would therefore look like this 10/4/1/5

AVAILABILITY MECHANISM

- Information is available
- Proactive approach to ensure that networks are available
- Email systems are available
- Denial-of-Service (DOS) attacks can be prevented

NON- REPUDIATION MECHANISM

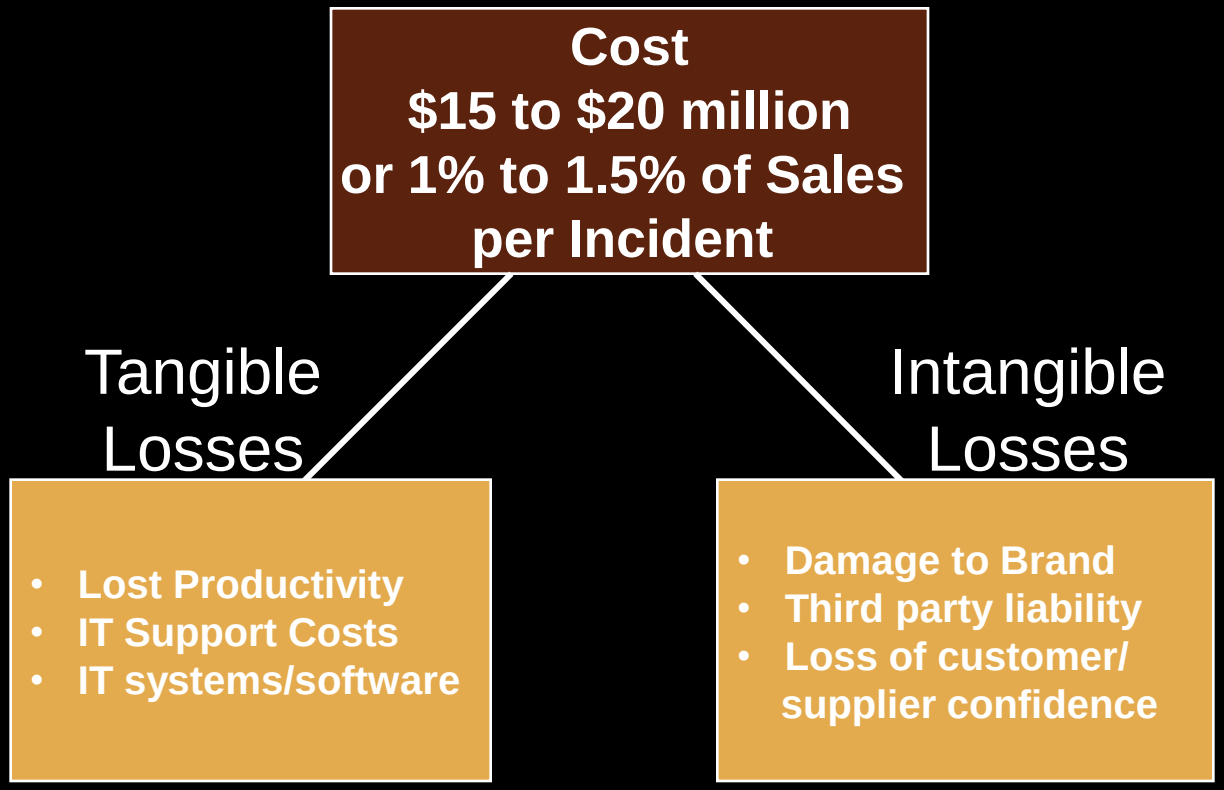
(It Was U !)

- Accountability for actions
  - Digital Signatures
  - Digital Certificates
- This needs to be kept confidential
- User can not deny

Rudy Giuliani's Call to Action

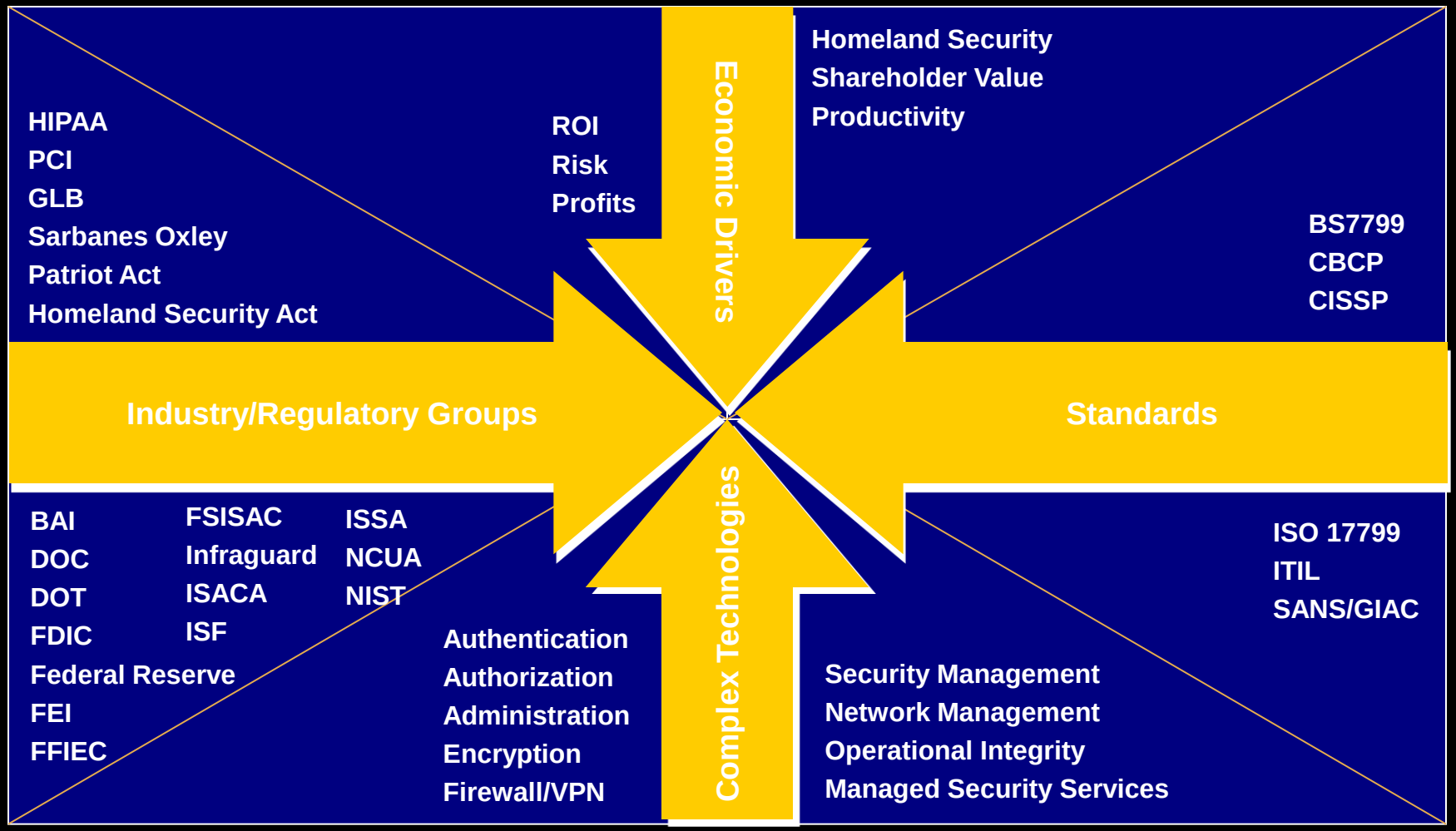
The time has come for senior executives of U.S. corporations to follow the President's lead and make security a mainstream business critical, board-level issue…the time when security-related decisions could be left to persons at a mid-manager level or decided solely upon budgetary considerations has passed. Senior executives must now take the steps to plan, prepare and practice to address their organizational security threats and challenges.

Digital Security Breach: The True Cost



The greatest loss as a result of an IT security breach is the intangible impact

Security drivers in Today's complex environment



Multiple Drivers Are Bringing Digital Security to the Boardroom

Triple Witching Event

Homeland Defense
(Homeland Security Act, USA Patriot Act)

Privacy/Fraud
(CA1386, GLB, HIPAA)

Sarbanes-Oxley

IT Executives are increasingly focused on controls

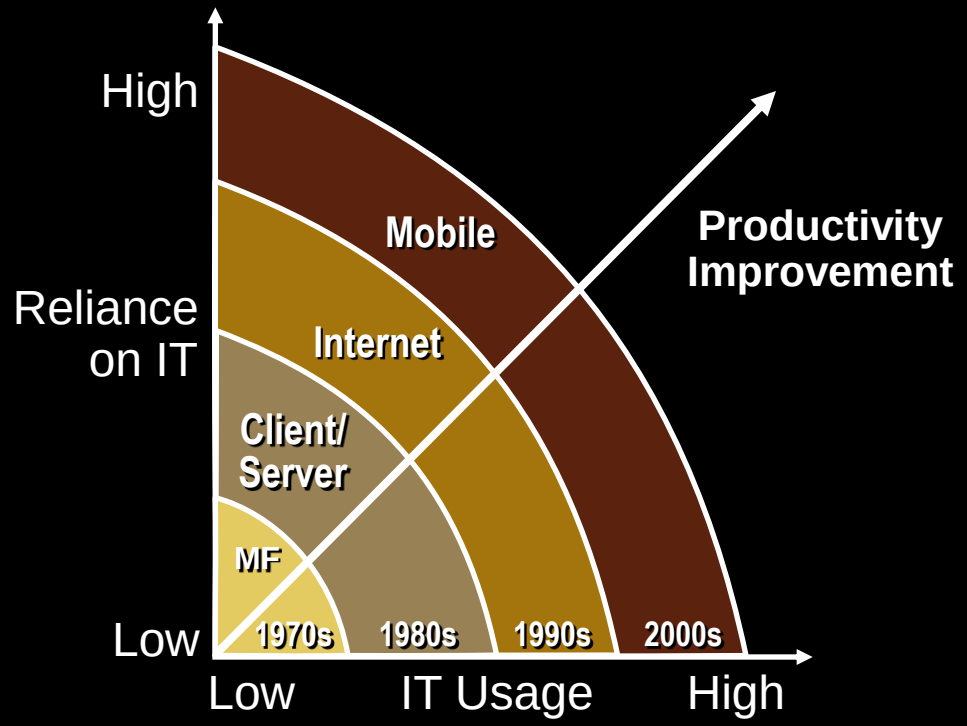
- Feature
- Productivity
- Reliability

- Security
- Predictability
- Stability

Technical Advances & Increasing Regulation

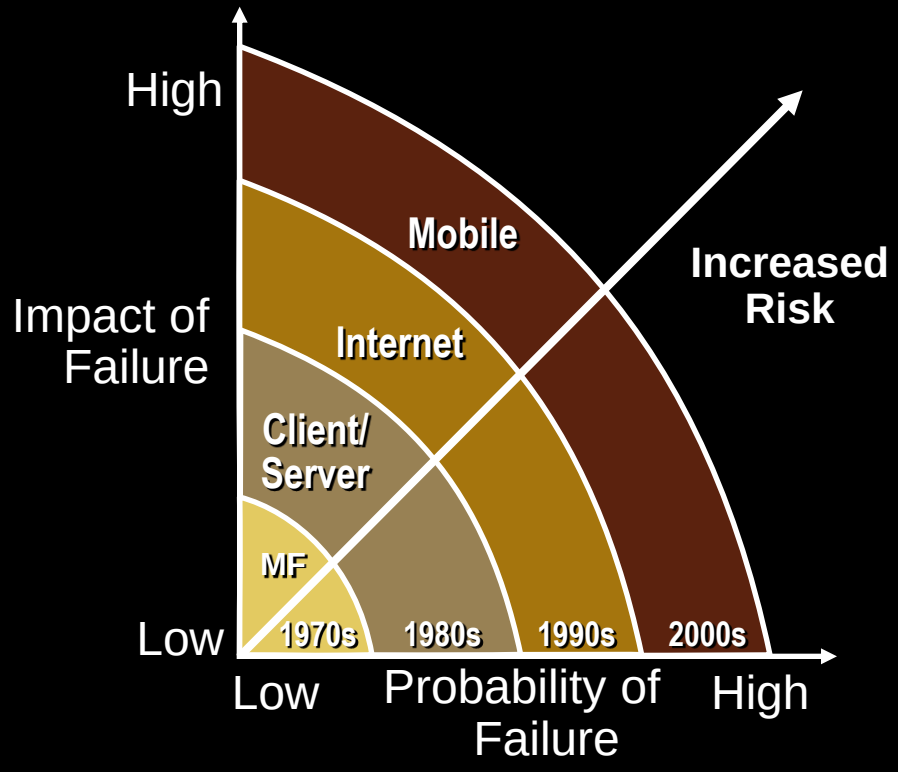
What is the Digital Frontier?

The digital frontier is the forward edge of technological ***impact*** with respect to organizations' ***usage*** of technology and their ***reliance*** upon it for productivity improvements.



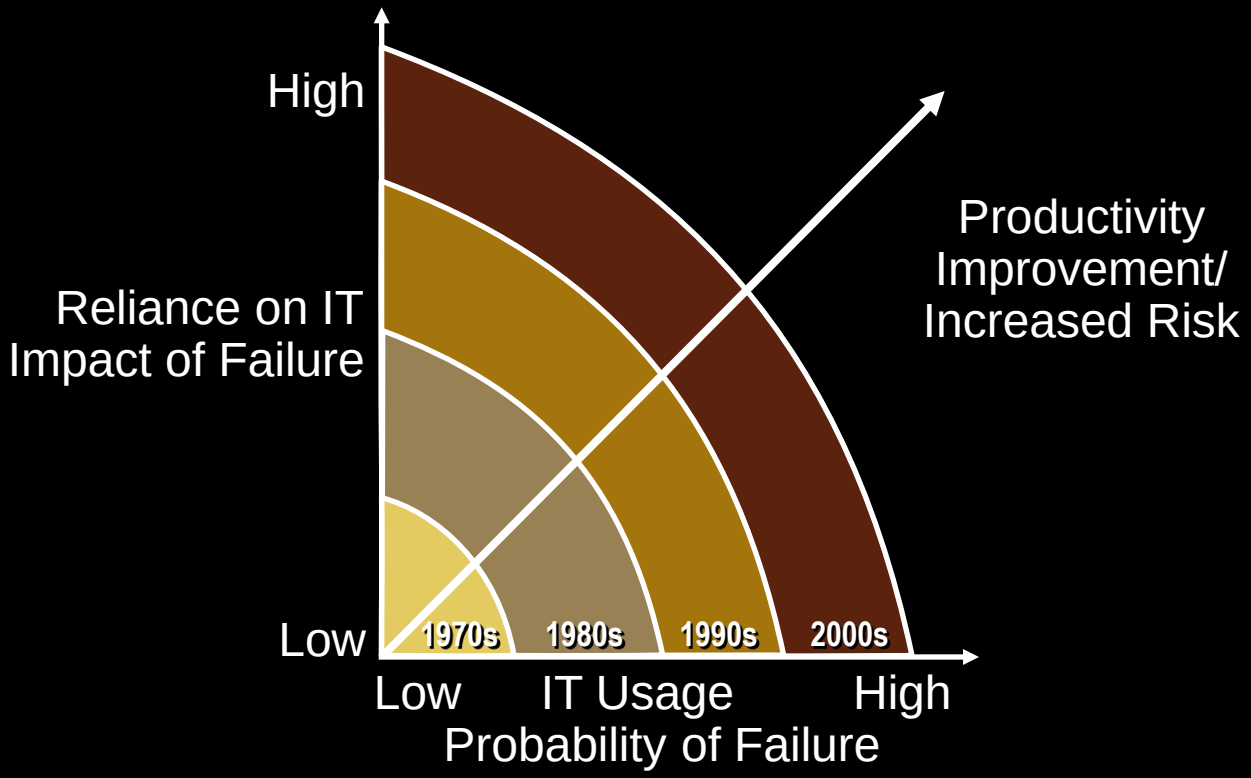
Increase Security Risks

As organizations invest for productivity improvement to the edge of digital frontier they also encounter increased security risks via a greater ***impact*** of and ***probability*** of technology failures.



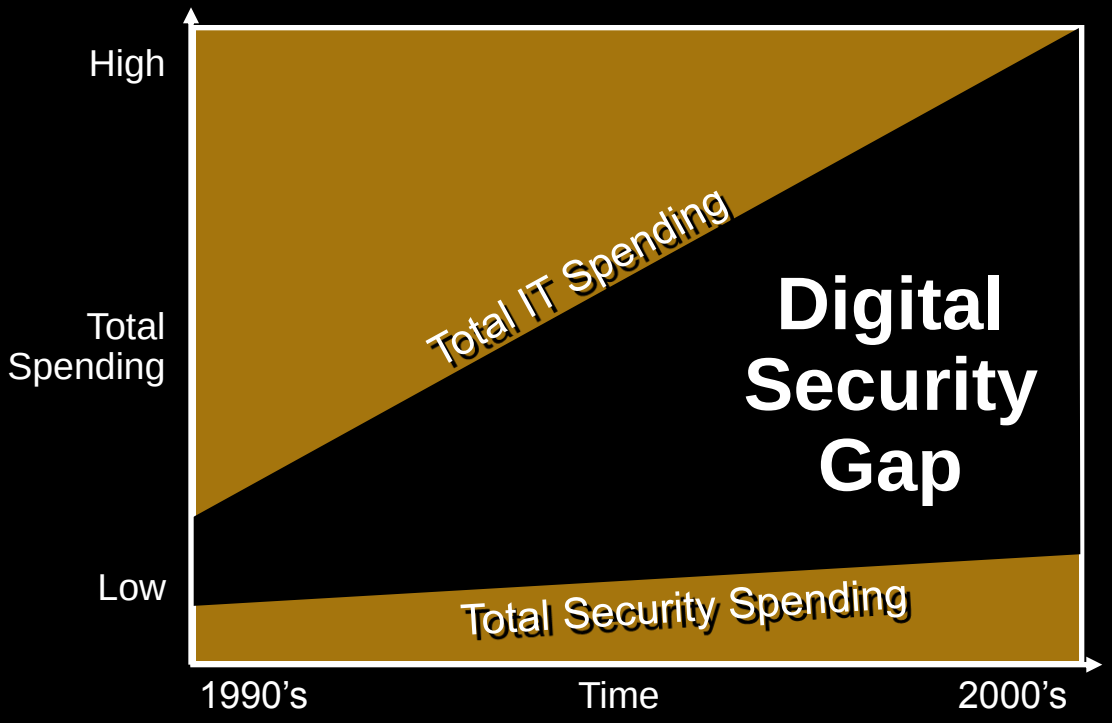
The Security Frontier

The digital frontier and corresponding security risk combine to create a new frontier. We call this the security frontier.



The Digital Security Gap

Caught up in the pursuit of productivity improvements, management apparently overlooked security.



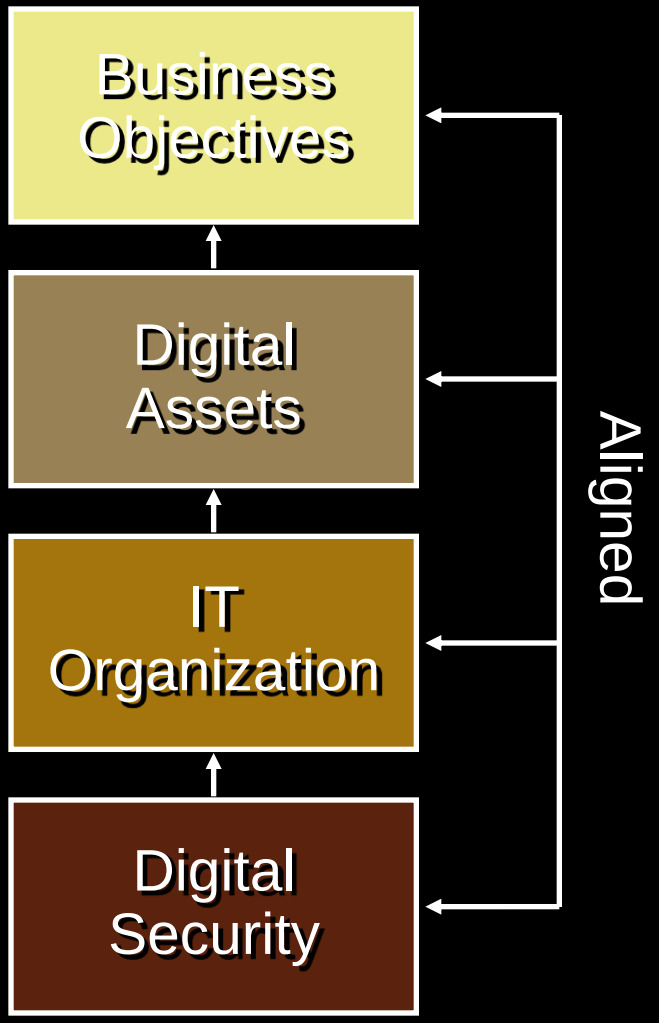
6 Key Security Characteristics

1) Aligned

The attainment and maintenance of appropriate alignment between digital security, the IT organization, digital asset and business objectives.

The distance between the top levels of management and the security team is known as the *Security Management Gap*.

79% of respondents in the 2002 Ernst & Young Digital Security Overview survey indicated that the documentation, implementation, and follow-through cycle for their information security policies was not being carried out completely.



2) Enterprise-Wide

A holistic view of the security needs for the entire organization, as well as its extended enterprise, to ensure consistent, efficient deployment. Critical ***authority*** is given to a centralized body to ensure consistently highly effective security throughout the organization.

86% of companies surveyed have intrusion detection systems in place. However, of those companies, **only 35% actively monitor** 95% to 100% of their *critical* servers for intrusions.

3) Continuous

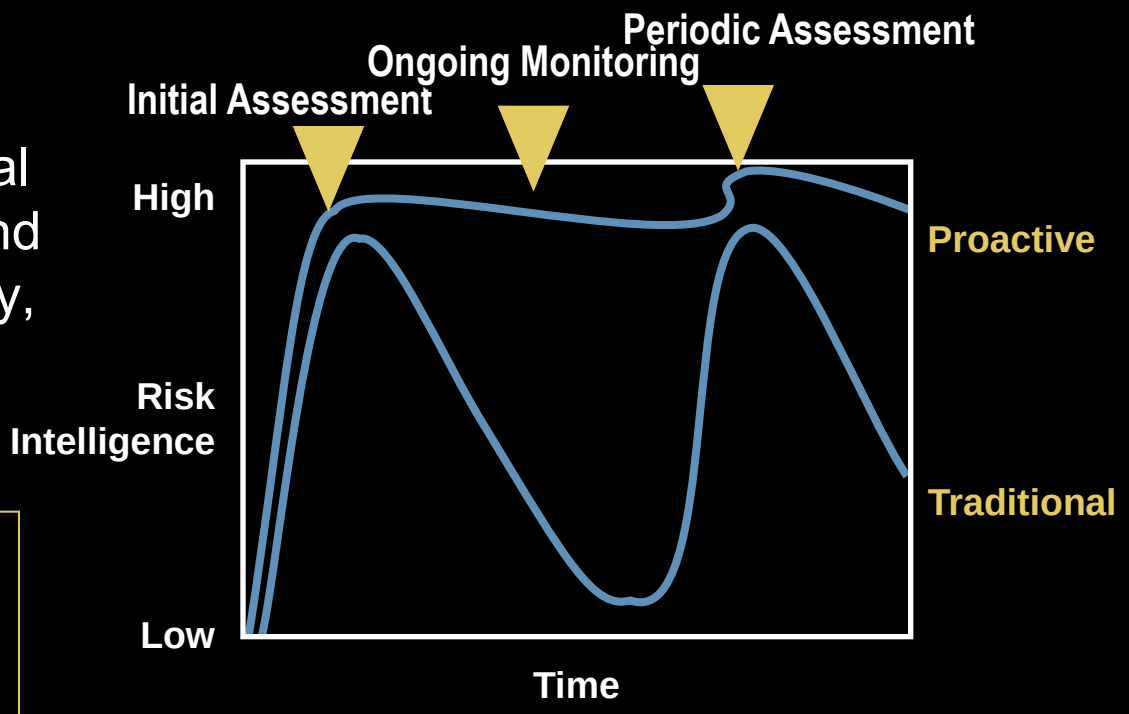
Real-time monitoring and updating of all security policies, procedures, and processes to ensuring a timely response to issues and opportunities.

46% of respondents indicated that they use manual or partially automated methods of tracking physical assets as opposed to fully automated methods.

4) Proactive

The ability of a security program to be able to effectively anticipate potential threats and vulnerabilities and to maintain the confidentiality, integrity, and availability of these digitally.

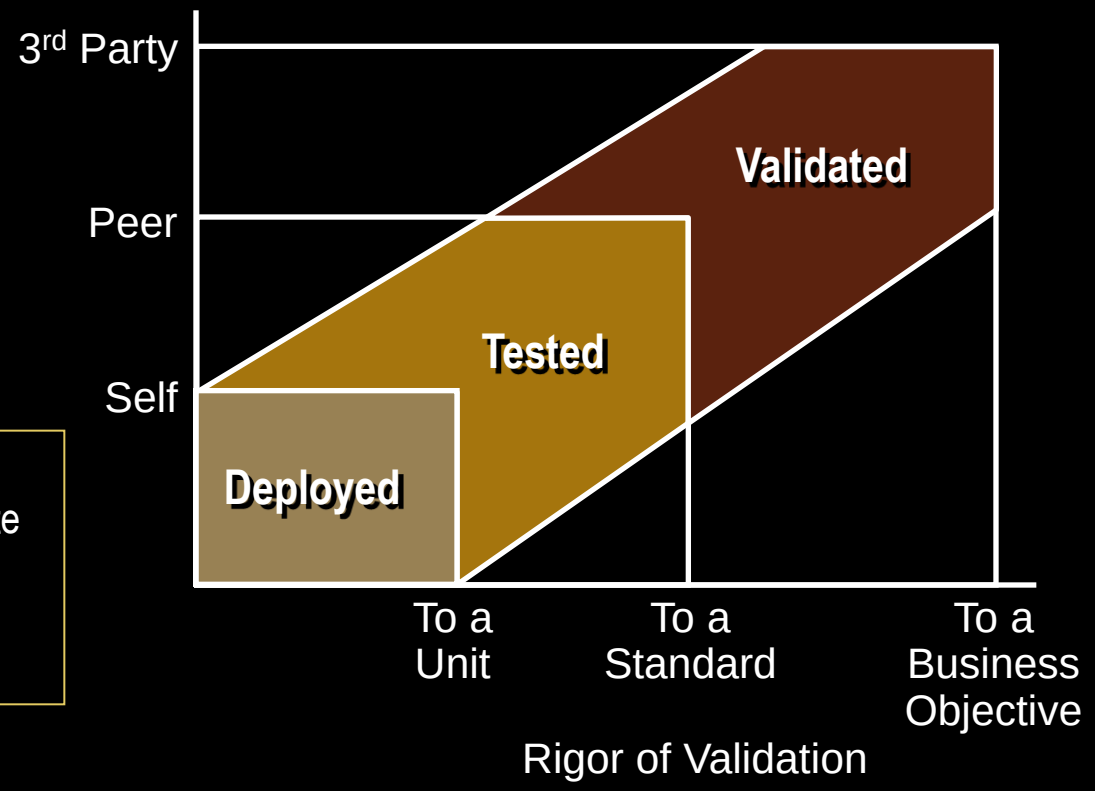
Only 16% percent of respondents have wide-scale deployment of vulnerability tracking mechanism, and knowledge of all critical information vulnerabilities.



5) Validated

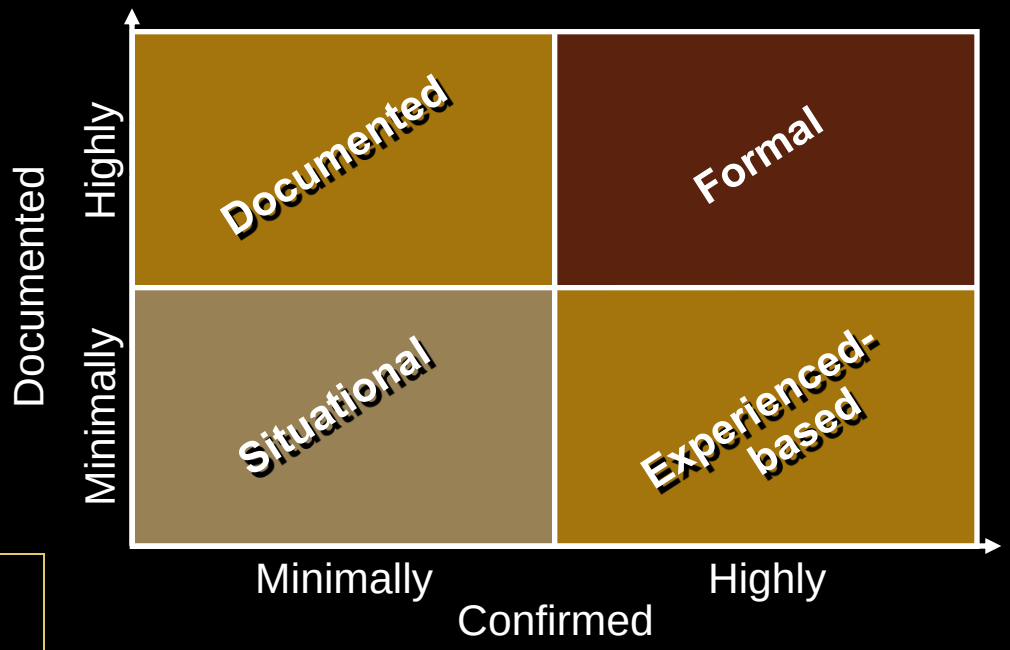
Achieving highly effective digital security requires ***third-party*** validation of critical security components and business objectives.

66% of respondents indicated that their information security policies are not in complete compliance with the domains defined by ISO 17799, CISSP, Common Criteria, or other recognized models.



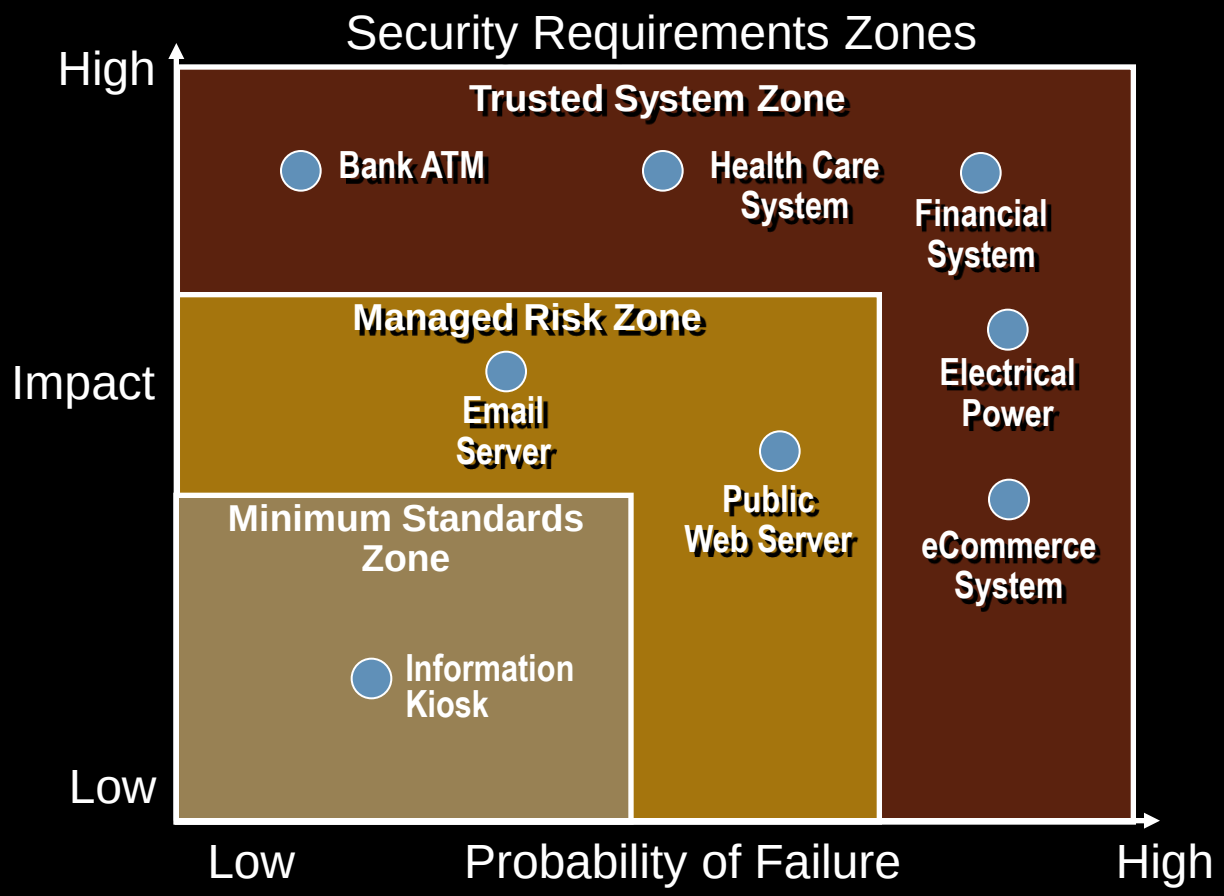
6) Formal

Policies, standards, and guidelines, which provide fundamental direction on digital security issues and are endorsed by senior staff. To be formal, they must be documented and tested, then communicated to every member of the organization.



13% of respondents have integrated business continuity and disaster recovery plans that address recovering the entire enterprise. 7% indicated they have no documented plans in place.

Technology and Business Objective Drives Requirements




The Security Agenda

9 Strategic Areas of “The Security Agenda”

Policies, Standards, & Guidelines

Intrusion & Virus Detection

Incident Response

Physical Security

Privacy

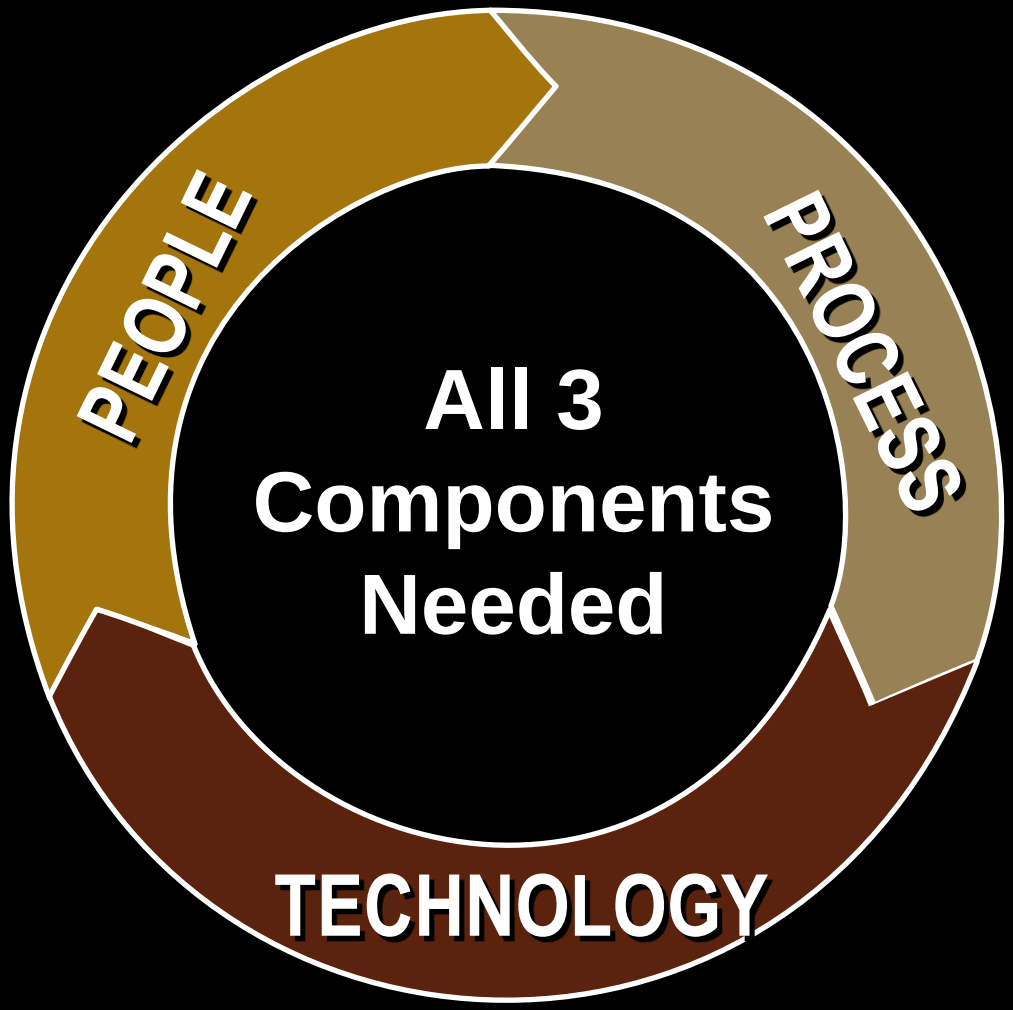
Asset & Service Management

Vulnerability Management

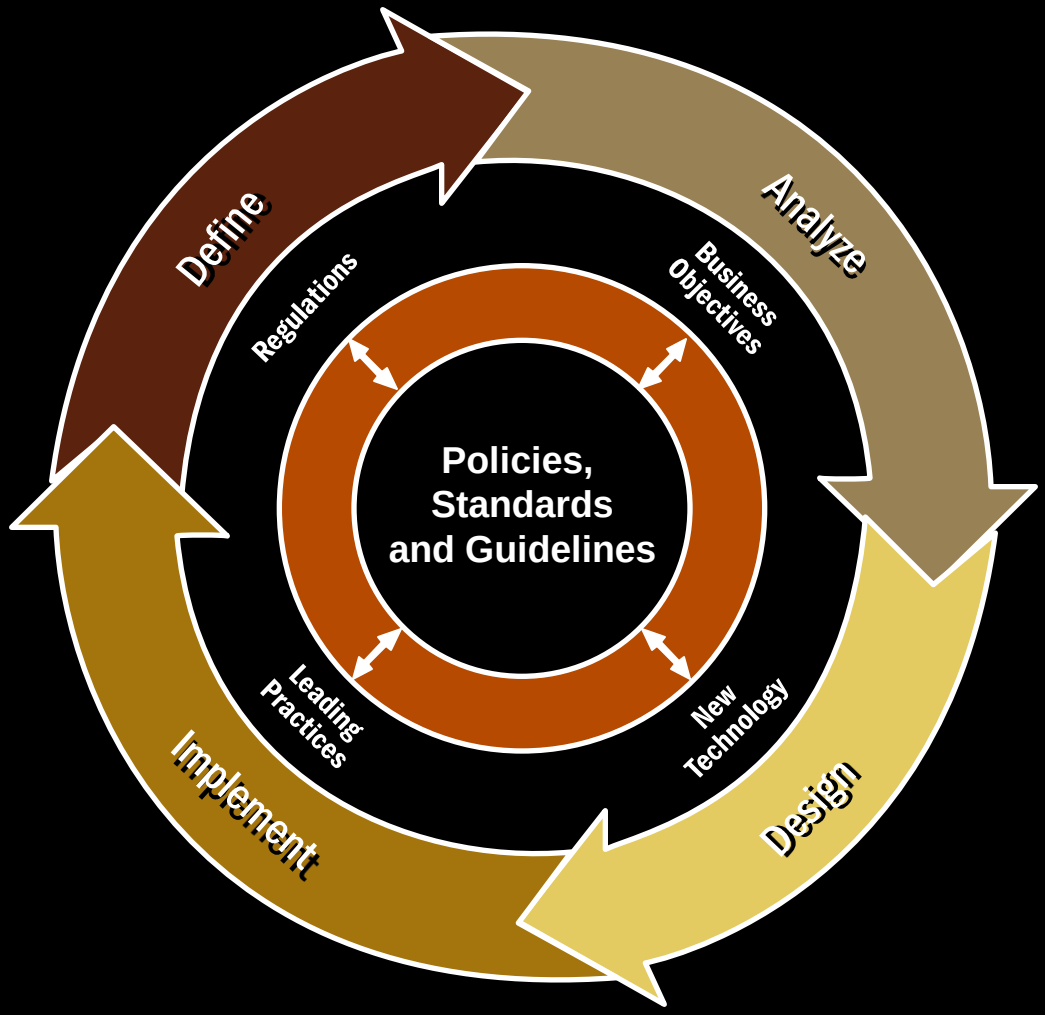
Entitlement Management

Business Continuity

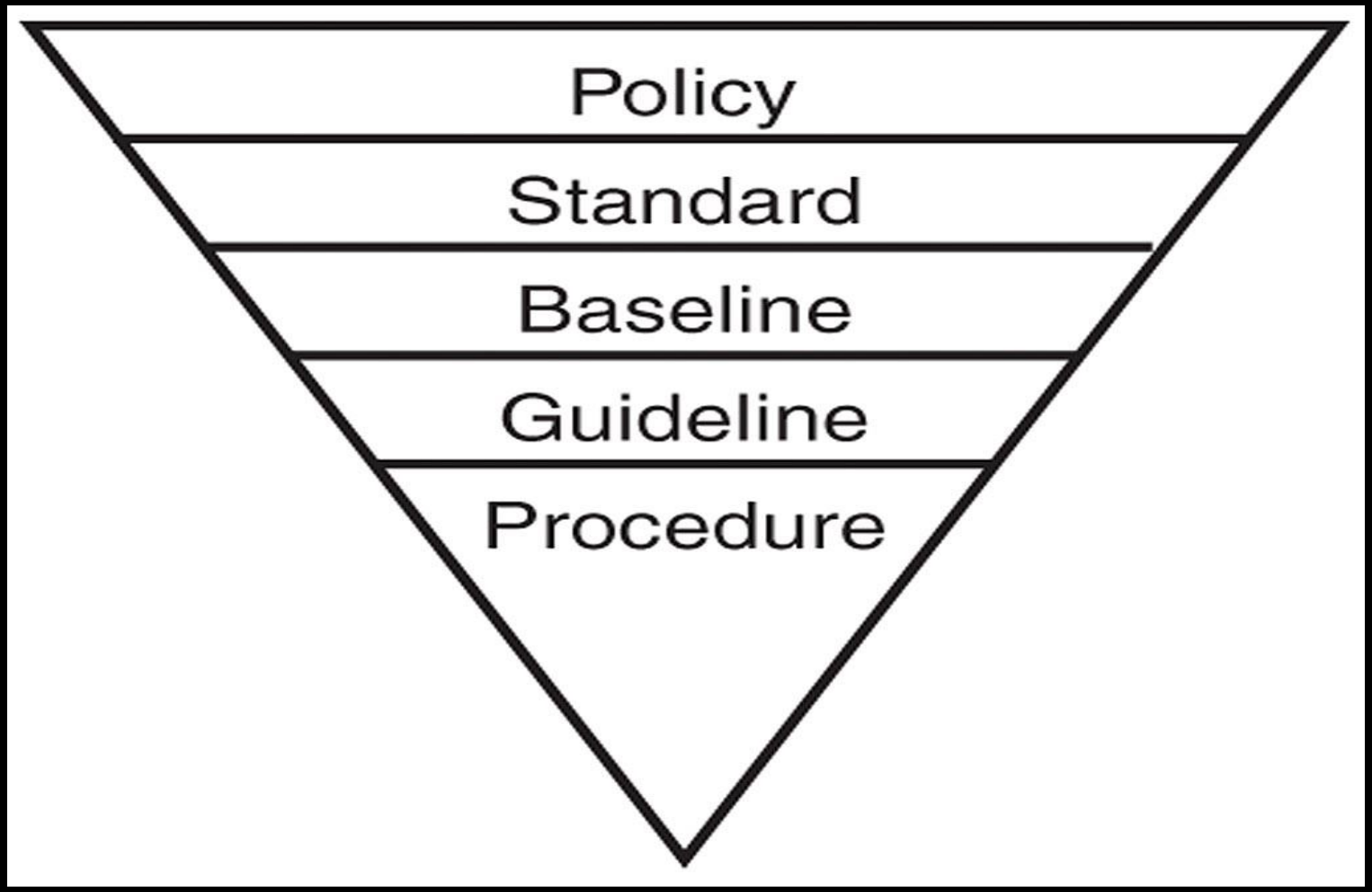
Complex Organizational Transformation



Policies, Standards, and Guidelines



Policy Structure



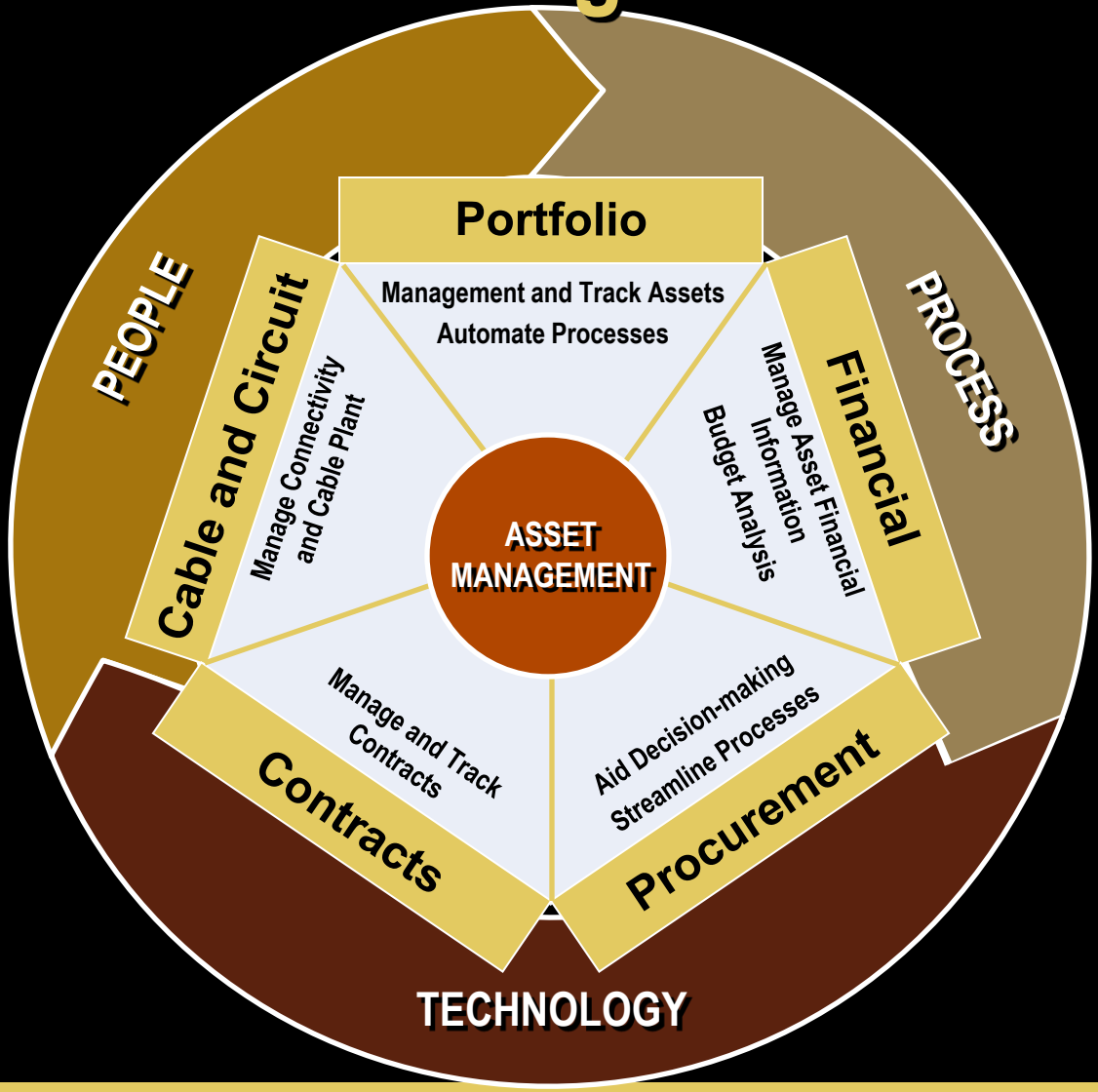
The Difference

Policies	Standards	Baseline	Guidelines	Procedures
▪ Policies are the top tier of formalized security documents. ▪ Policies are high-level plans that describe the goals of the procedures.	▪ Standards are much more specific than policies. ▪ Standards are tactical documents because they lay out specific steps or processes required to meet a certain requirement. ▪ As an example, a standard might set a mandatory requirement that all email communication be encrypted.	▪ A baseline is a minimum level of security that a system or network must adhere to. ▪ Baselines are usually mapped to industry standards.	▪ A guideline refers you to a statement in a policy or procedure by which to determine a course of action. ▪ Guidelines are a recommendation or suggestion of how things should be done.	▪ A procedure is a detailed, in-depth, step-by-step course of action to achieve a specific result. ▪ Procedures are written to support the implementation of a policy.

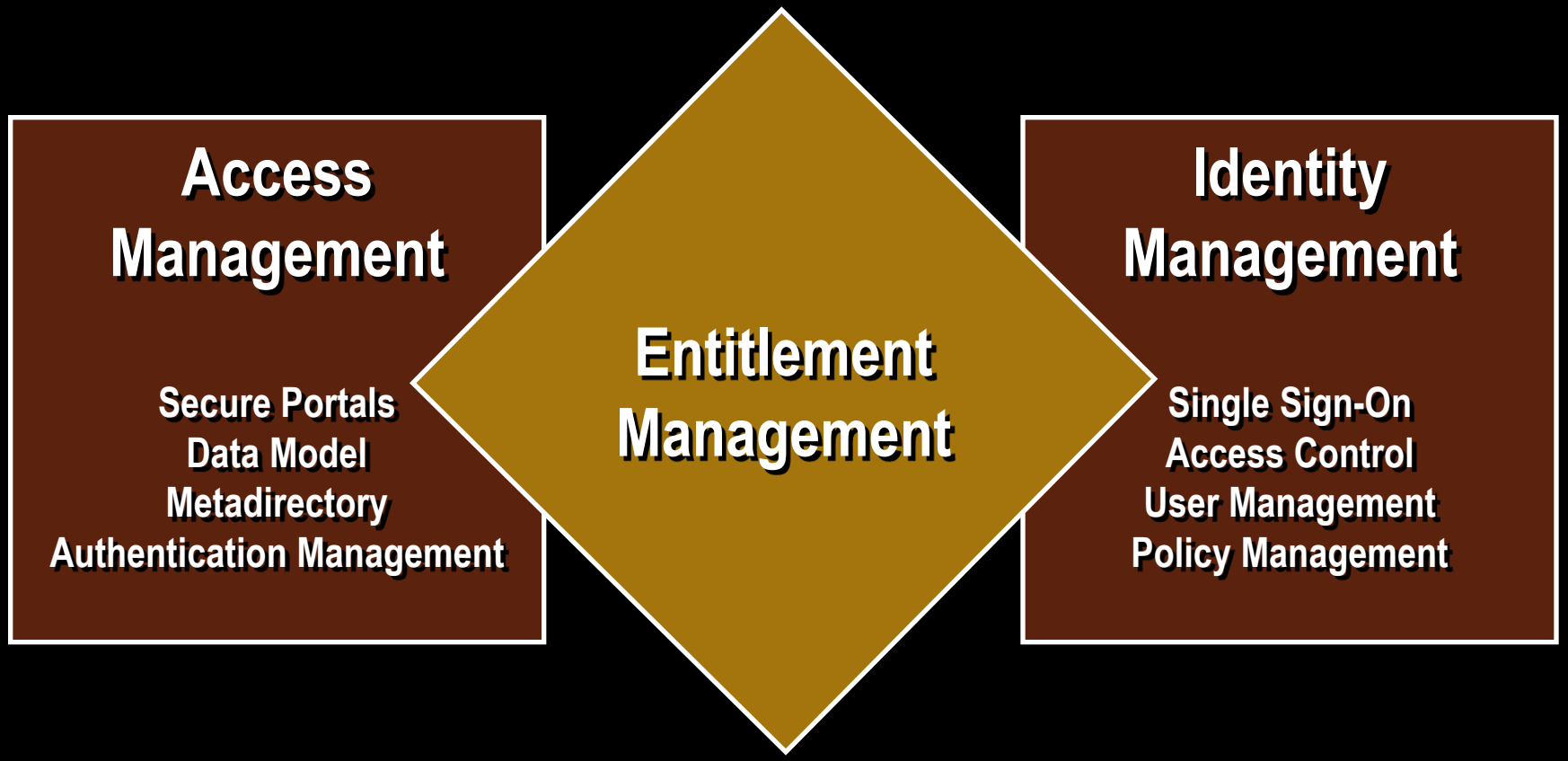
Attributes of a Sound Policy

- Clearly stated policy statement that defines necessity of the policy and relative scope
- Policy/Guidelines are easily understandable by users and should have significance for a substantial number of users
- Guidelines are comprehensive and specifically detail the requirements of the policy
- Additional content includes:
  - term definitions to support clarity;
  - supporting documentation as required;
  - roles and responsibilities with respect to the policy;
  - measurable compliance standards;
  - information on obtaining policy waivers; and
  - details on how the policy will be enforced, with potential sanctions for noncompliance.

Asset & Service Management



Entitlement Management



IAM Overview "Who has access to what and is it appropriate?"

Identity Management – is process for managing the entire lifecycle of digital identities and profiles for people, systems, and services. It typically includes:

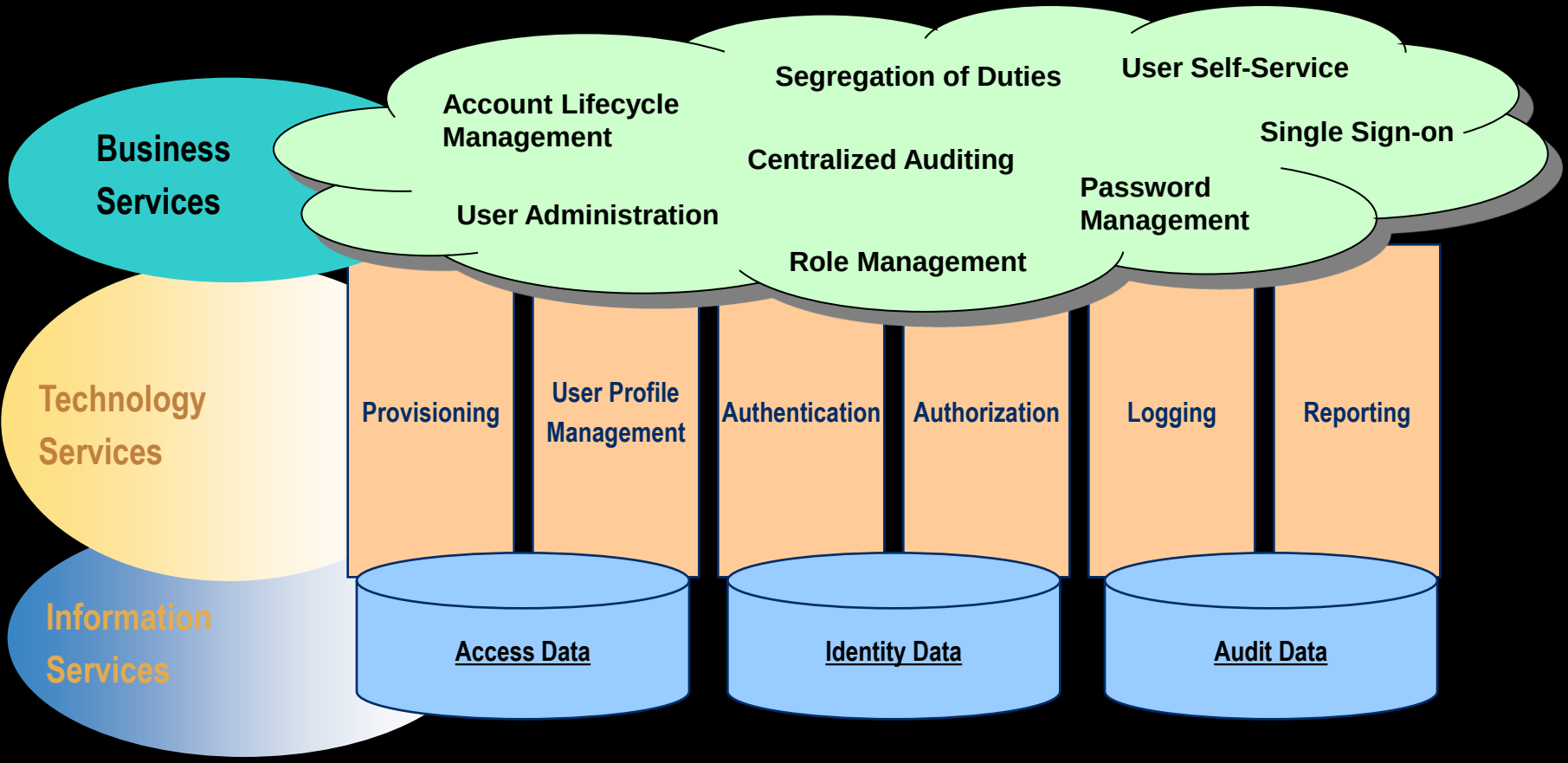
- Establish a unique, global identity and associated user credentials
- Automated provisioning of new users
- User self-service functions (e.g., password reset, password sync)
- Workflow processes for approving account creation, modification, and assignment to specific roles
- Removing users when they no longer require access
- Auditing and reporting of user identity information

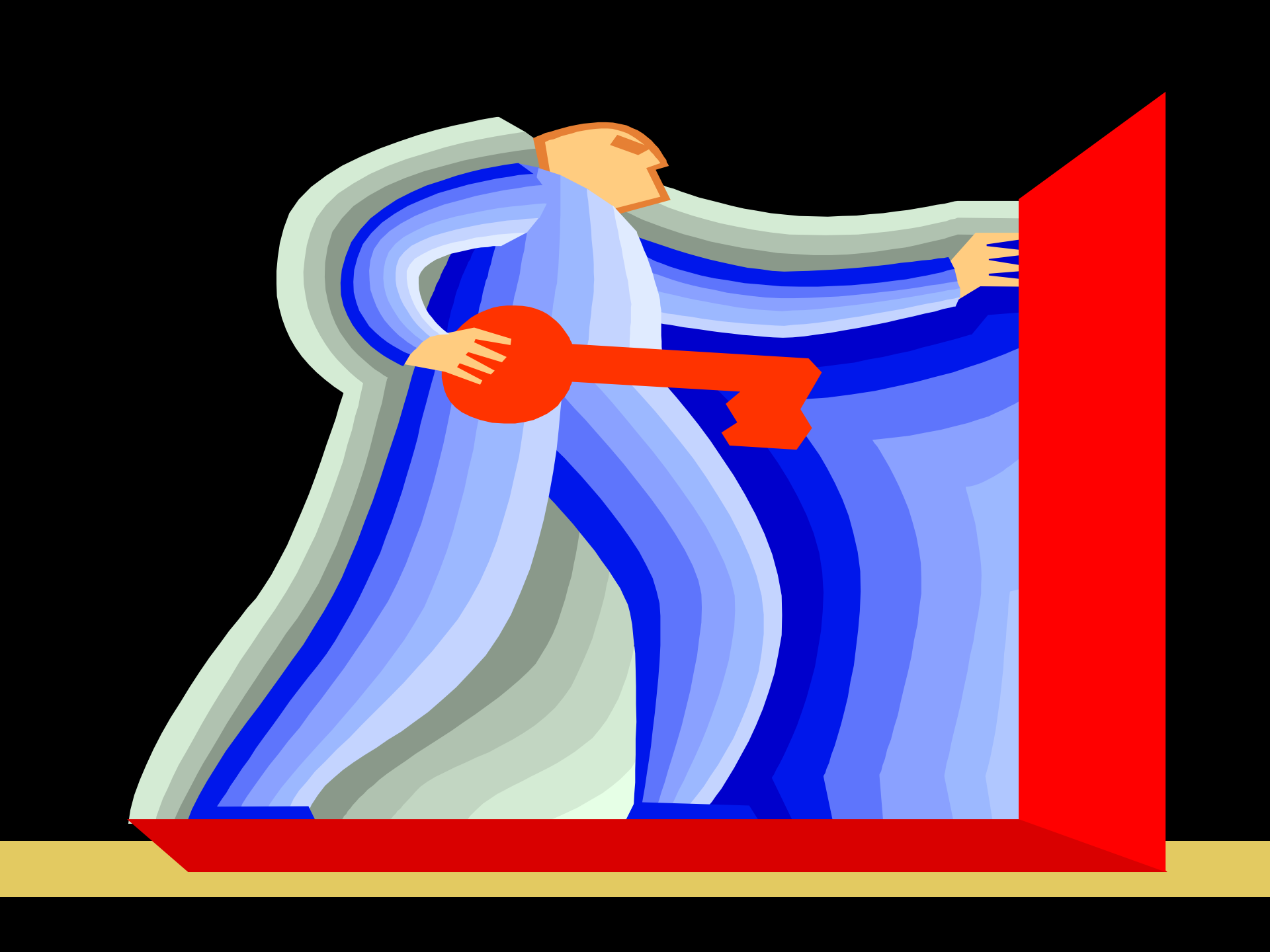
Access Management – process for regulating access to information assets by providing a policy-based control of:

- Who (by role or rule) should access specific applications and systems infrastructure
- What segregation of duties controls must exist within/across systems
- What that role is permitted to do
- What permission or restrictions are on that role
- What permissions or accesses users are granted
- Who approved these permissions
- Sometimes expanded to include both logical and physical assets

IAM Overview

Services Framework





IDENTIFICATION MECHANISM (Who are you ?)

- Initial logon to the system / PC
- User must provide a valid:
  - User Name or
  - Login ID
- User ID is not secret (can be guessed, stolen, duplicated or displayed by system)

AUTHENTICATION MECHANISM (Can you prove it ?)

- User provides:
  - Password (What the user knows)
  - Smart cards / Token cards (What the user has)
  - Biometrics (What the user is)
- Single sign on

Which password is more secure?

- abc12345
- HerculeS
- fzx456TY
- ☺t%1mE☻7

AUTHORIZATION MECHANISM (Access to what ?)

- Only defined users giving correct authentication can gain access to specified network components
- Restrict user access to data & applications
- Discretionary Access Control (DAC)
  - This model allows the owner of the resource to establish privileges to the information they own
- Mandatory Access Control (MAC)
  - This is a static model whereby access to a resource is predefined

ACCESS CONTROL MECHANISMS

- Discretionary Access Control (DAC).
  - Access Control list.
  - Access Control Matrix.
  - Directory List.
- Mandatory Access Control (MAC).
  - Military model.
  - Role based access control.

Access control list

User ID	Access right
Solly	Execute
Thabo	Execute/write
Peter	Execute/read/write

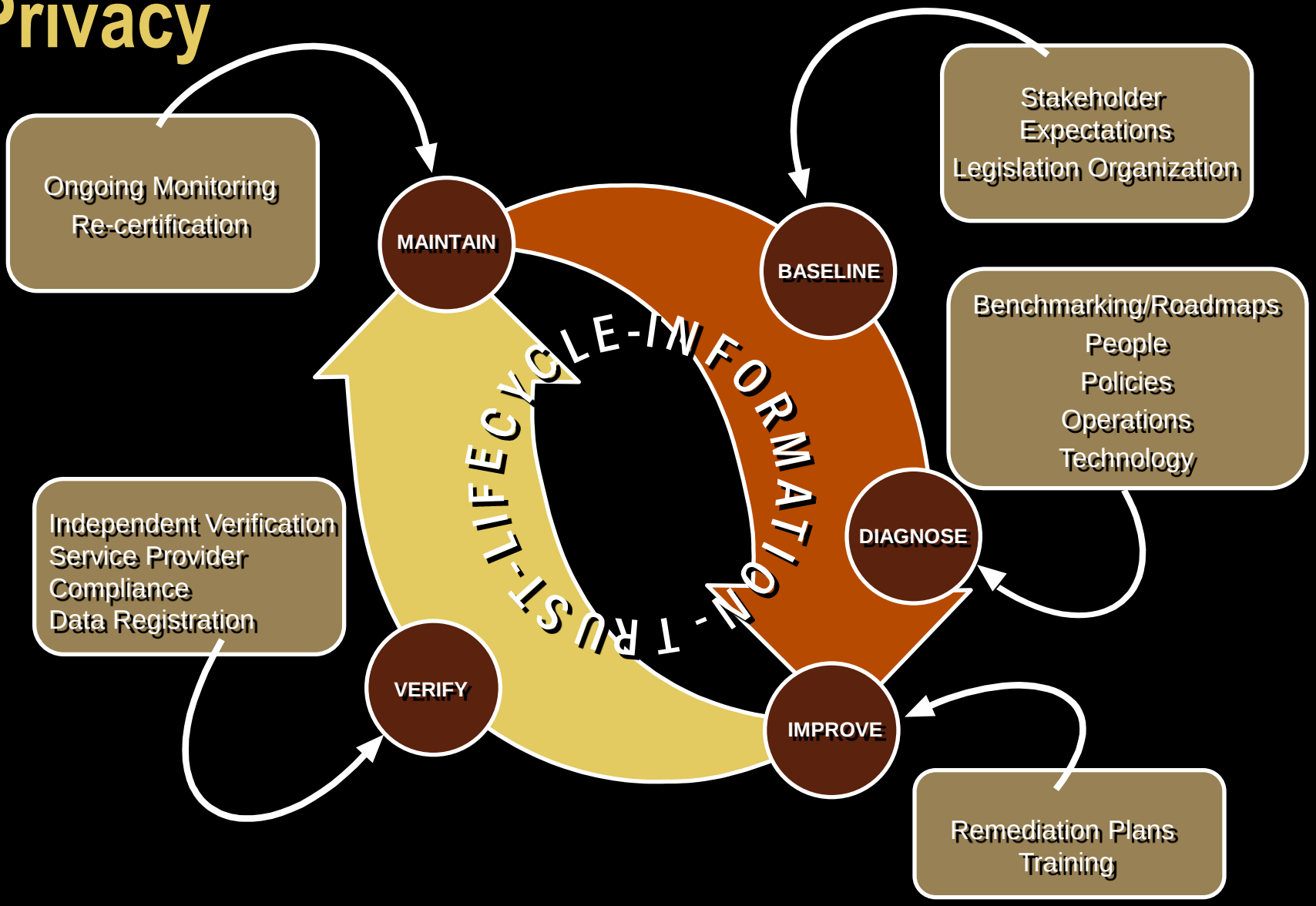
DIRECTORY LIST

Directory list for Solly	
Object	Access right
Purchasing	Execute
Accounting	Read
Production	Read
Sales	Execute/write

ACCESS CONTROL MATRIX

Users	Enquiry program	Alterbal program	Client Database
Tom	Execute	Read	Read/ Write
Peter	Read/ Write/ Execute	Read	No Access

Privacy


Ongoing Monitoring
Re-certification
MAINTAIN
BASELINE
Stakeholder
Expectations
Legislation Organization
Benchmarking/Roadmaps
People
Policies
Operations
Technology
DIAGNOSE
Independent Verification
Service Provider
Compliance
Data Registration
VERIFY
IMPROVE
Remediation Plans
Training
TRUST-LIFECYCLE-INFORMATION

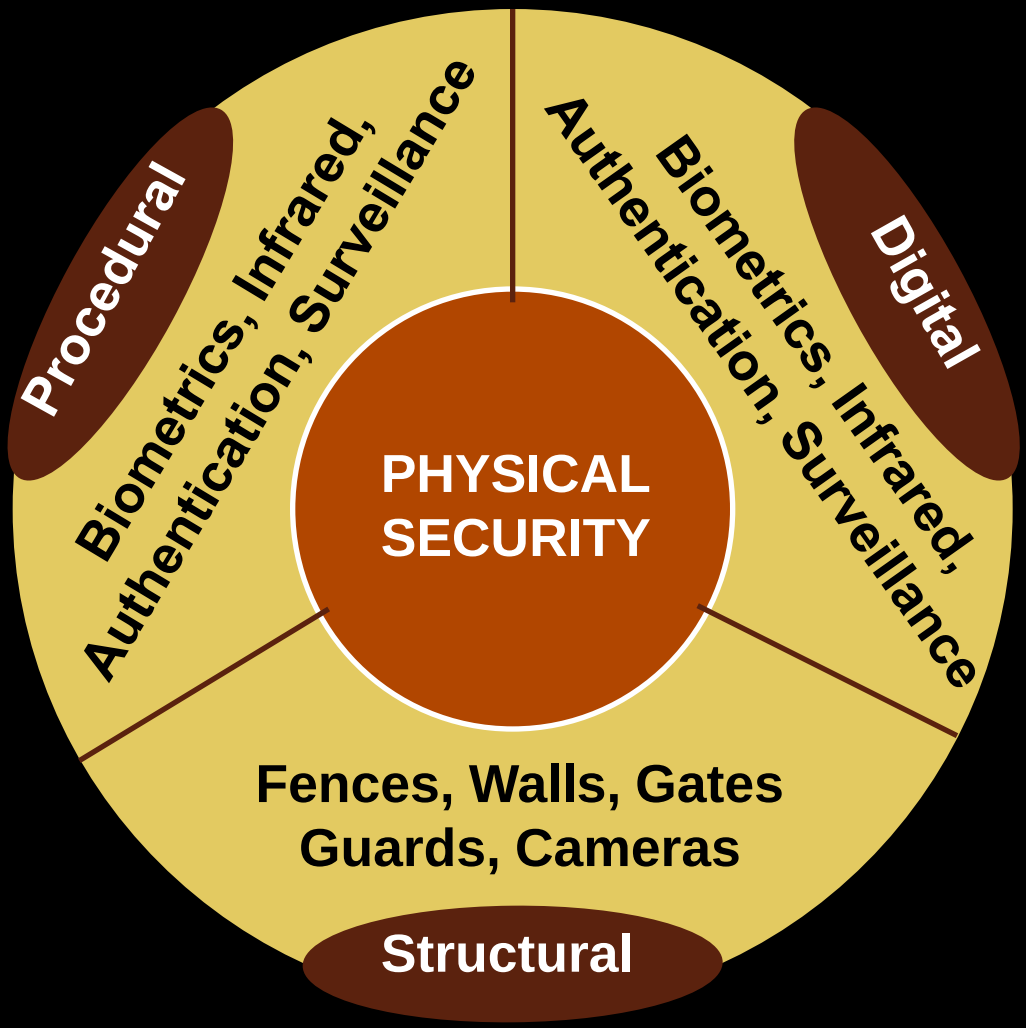
Examples – United States

- Gramm Leach Bliley Act (GLBA)
- E.U. Data Protection Directive: safe harbor and model contracts
- Health Insurance Portability and Accountability Act (HIPAA)
- The Children's Online Privacy and Protection Act (COPPA)
- U.S. Marketing Laws: Telemarketing Sales Rules, Do-not-Fax and CAN-SPAM
- California Data Breach Notification Act (SB1386) and similar laws in nearly every State
- Privacy Act of 1974

Examples - Global

- The E.U. Data Protection Directives (95/46/EC)
- E.U. directives such as the Electronic Communications and e-Privacy Directive
- Specific national laws on data protection, employment, and general civil law
- Guidance from the Article 29 Working Party
- Guidance from national data protection authorities
- Many countries have enacted comprehensive data protection laws, these include: Argentina, Australia, Hong Kong, Japan, New Zealand, Paraguay, Peru, Tunisia (not all of these laws are considered adequate to comply with the E.U. privacy directive)

Physical Security



Business Continuity

Definitions – Business Continuity Program

- Business Continuity Program
  - An ongoing process providing integrated and coordinated business continuity, disaster recovery, high availability, and crisis management to ensure business continuance in the event of a disruption for successful and continuous delivery of critical services and products.
  - The purpose of business continuity is to prepare for the unknown.
  - The objectives are to:
    - Protect human life and company assets
    - Provide for business continuance
    - Minimize loss
    - Protect customer service and company image
    - Ensure sustainability

Definitions

- Disaster Recovery

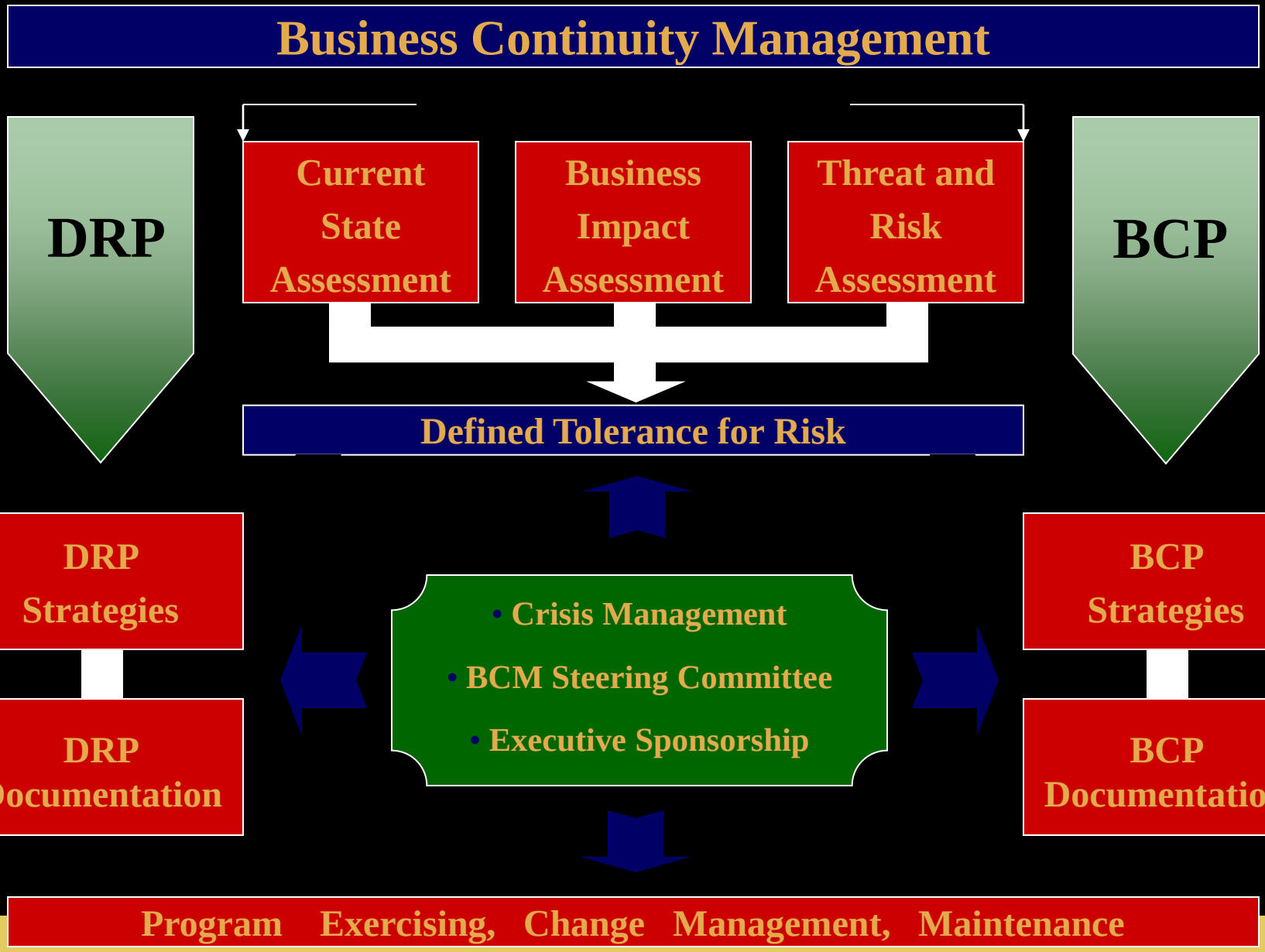
  The advance planning and preparations necessary to minimize loss and help ensure continuity of the computer and communications functions within an organization.

- Business Continuity

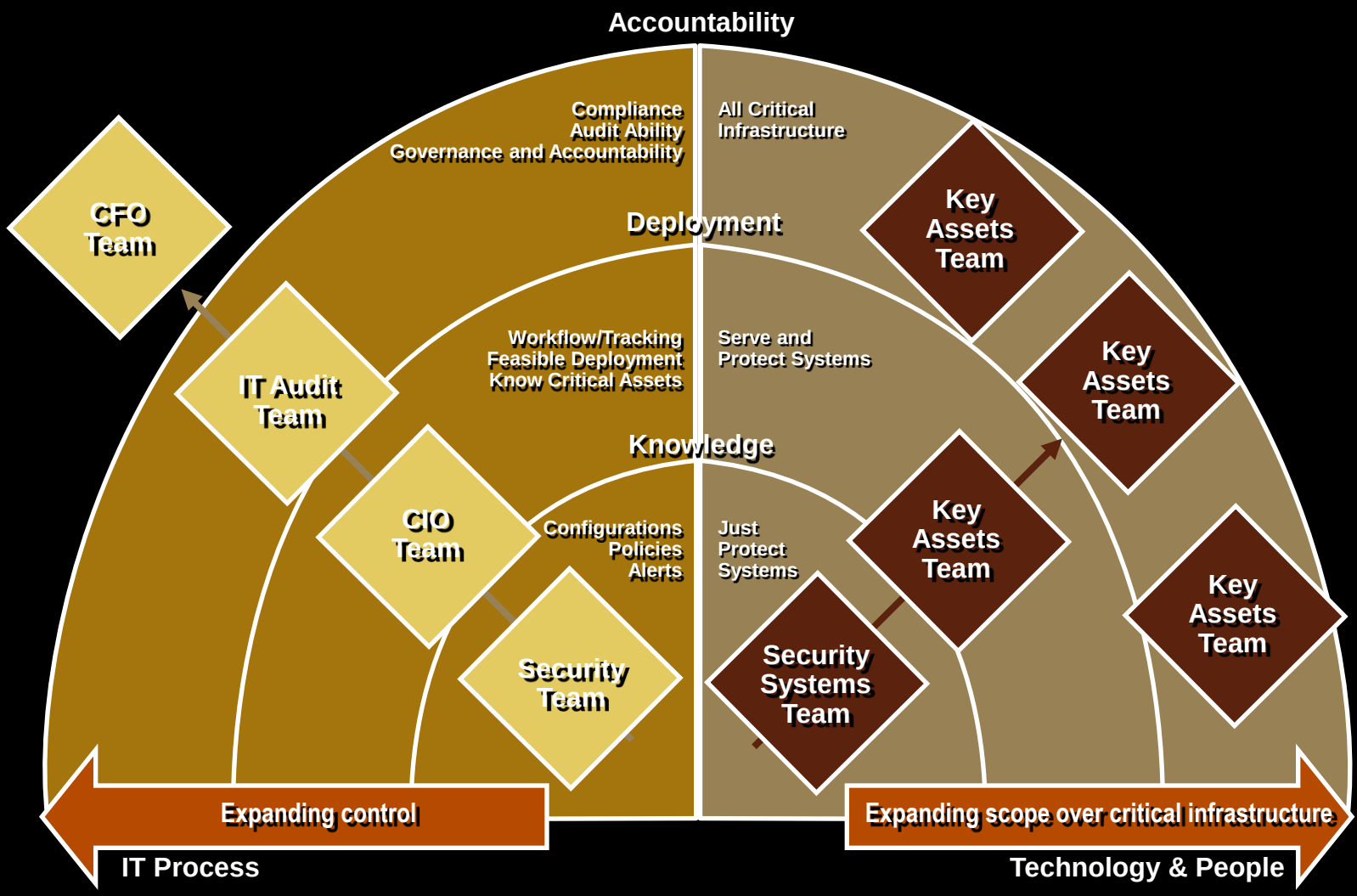
  The advanced planning and preparations that are necessary to identify the impact of potential losses, to formulate and implement viable recovery strategies, to develop plans that help ensure continuity of organizational services in the event of an emergency or disaster.

- Crisis Management

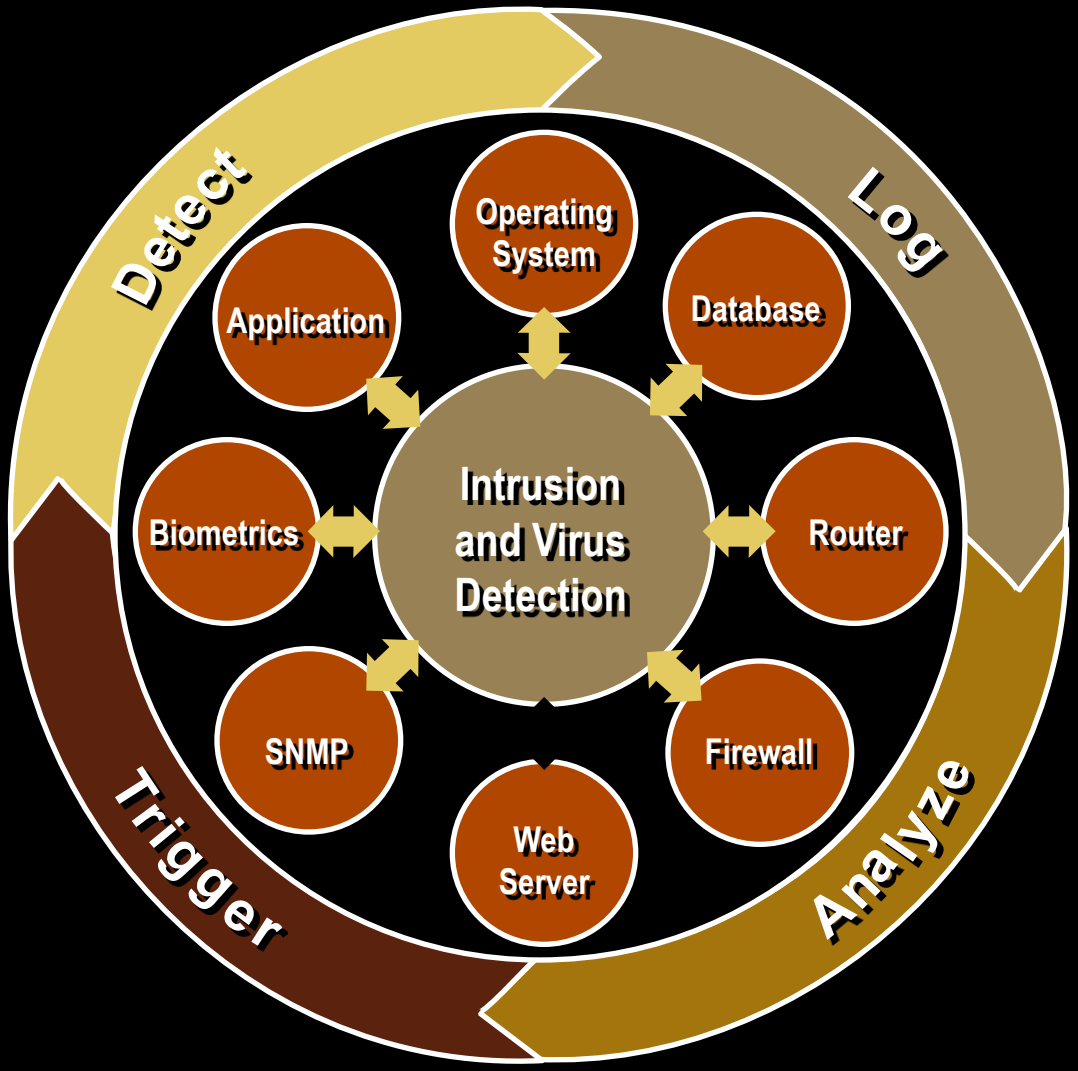
  The team structure, membership, roles, responsibilities, procedures, and training necessary to provide the framework to manage any crisis. The crisis management team manages the crisis to its completion.


Business Continuity Management
DRP
Current State Assessment
Business Impact Assessment
Threat and Risk Assessment
BCP
Defined Tolerance for Risk
DRP Strategies
DRP Documentation
• Crisis Management
• BCM Steering Committee
• Executive Sponsorship
BCP Strategies
BCP Documentation
Program Exercising, Change Management, Maintenance

Vulnerability Management

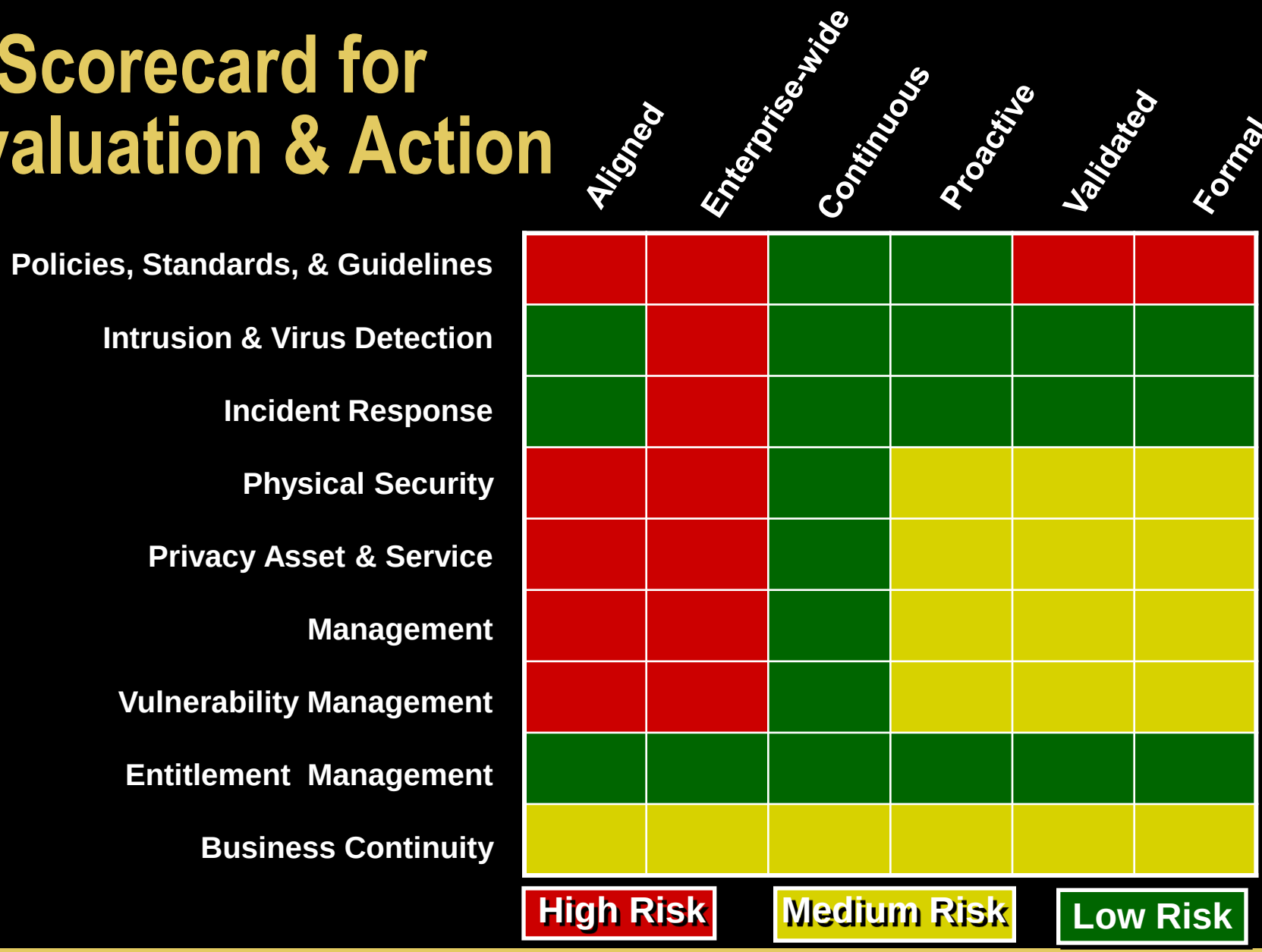


Intrusion and Virus Detection

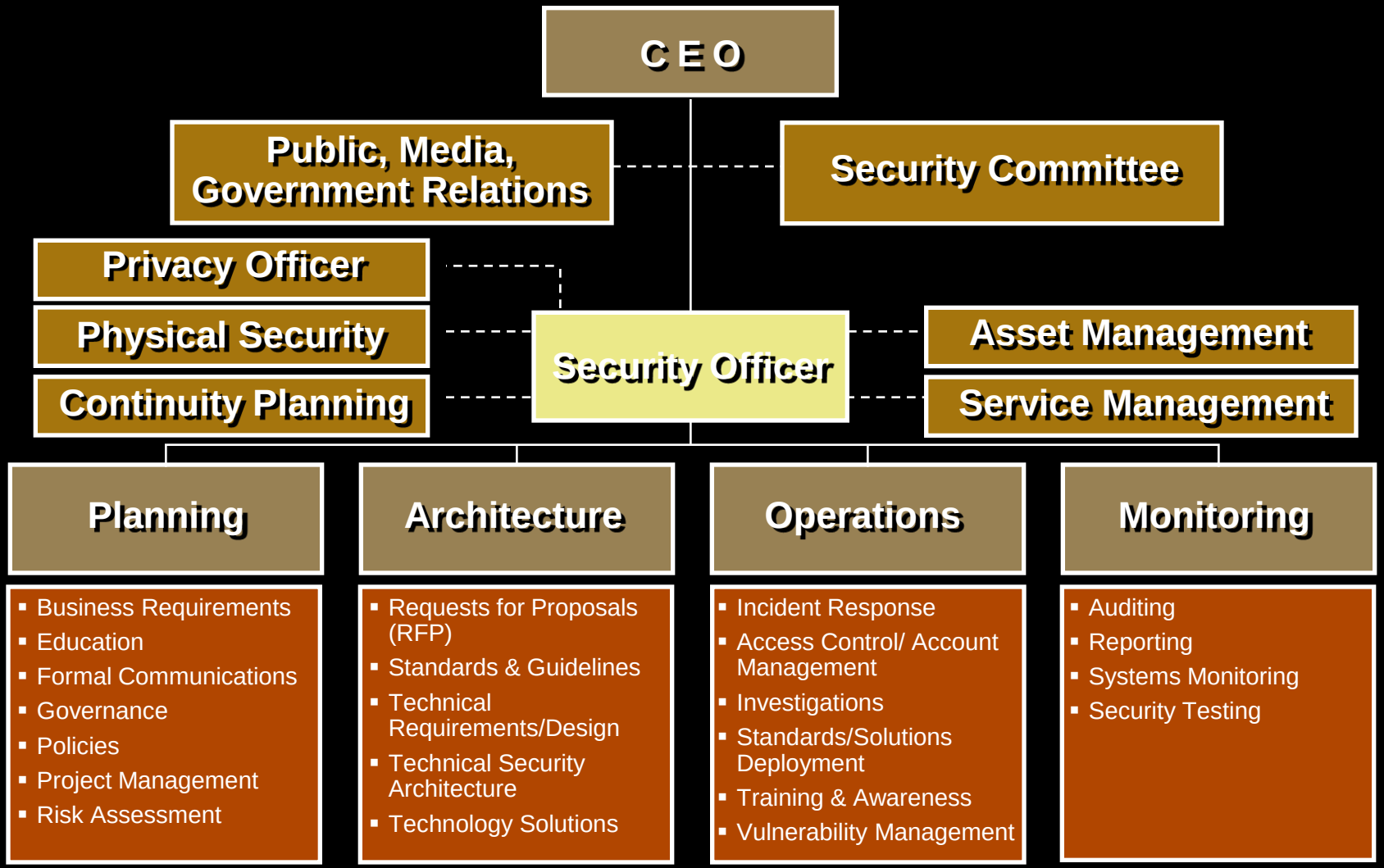


Incident Response

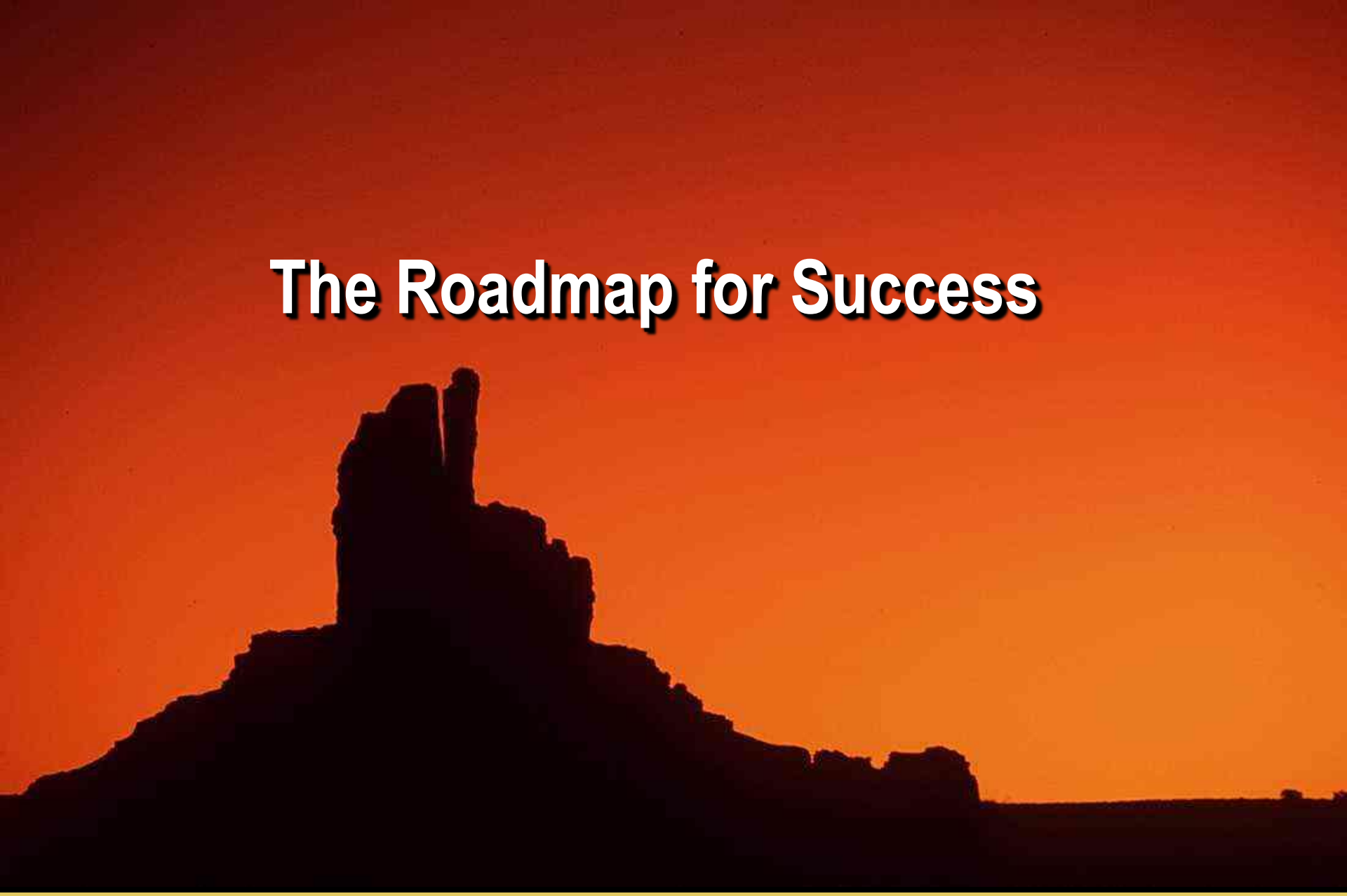
A Scorecard for Evaluation & Action



Security Organizational Framework



The Roadmap for Success



Executive management must understand

- Scenario-based simulations – Table-Top Exercises
- The organizations response
- Critical roles and responsibilities
- Actions plans to minimize the effect of an incident
- Monitor and test responses

Highly Effective Security Cultures:

- are chief executive-driven
- maintain a heightened sense of awareness
- utilize a digital security guidance council
- establish timetables for success and monitor progress
- drive an enterprise-wide approach

The level commitment of organization's personnel to the principles of security will determine the success or failure of the digital security program.

7 WORST SECURITY MISTAKES EXECUTIVES MAKE

- Assigning untrained people to maintain security
- Not understanding relationship of Information Security to Business problems
- Not dealing with Operational aspects of security
- Relying primarily on firewalls
- Not realizing how much their information and organizational reputation is worth
- Authorizing reactive, short time fixes (problems re-emerge rapidly)
- Pretending the problem will go away

10 WORST SECURITY MISTAKES IT PROFESSIONALS MAKE

- Connecting systems to Internet/Intranet before hardening them
- Connecting test systems to Internet/ Intranet with default accounts/ passwords
- Not updating/ patching systems when holes are found
- Using TELNET & other unencrypted protocols to manage systems, routers, firewalls & PKI
- Giving password over phone or changing user password without authenticating user first

10 WORST SECURITY MISTAKES (CONTINUED)

- Fail to maintain & test backups
- Running unnecessary services e.g. Ftpd, Telnetd, Finger, RPC, Mail, Rservices etc
- Implementing firewalls with rules that don’t stop malicious/ dangerous traffic (in & out)
- Outdated virus software & definitions
- Failing to educate users in identifying security problems

For More Information…

Sajay Rai CPA, CISSP, CISM
CEO
Securely Yours LLC
248-723-5224
Sajayrai@securelyyoursllc.com