INFORMATION SECURITY MANAGEMENT

INFORMATION SECURITY RISKS AND RISKS MANAGEMENT

DAY-3, SESSION-5

AGENDA

- What is Information Security Risk?
- Risk Assessment
- Risk Management
- Risk Management Decisions
- ISO 27001
- FISMA, NIST

WHAT IS THE INFORMATION?

- 'Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected’[BS ISO 27002:2005]

- Information can be created, stored, destroyed, processed, transmitted or used; whatever form the information takes or means by which it is shared or stored, it should always be appropriately protected.[BS ISO 27002:2005]

WHAT IS INFORMATION SECURITY?

- Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

- •Information security is concerned with the CIA of data regardless of the form the data may take: electronic, print, or other forms.

- •Preservation of CIA of information; in addition, other properties such as authenticity, accountability, non-repudiation & reliability can also be involved.[ISO/IEC 17799:2005]

WHAT IS THE DIFFERENCE BETWEEN RISK AND SECURITY?

Information Security

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

OBJECTIVES OF INFORMATION SECURITY

PRESERVATION OF

Confidentiality:

Ensuring that information is available to only those authorized to have access.

Integrity:

Safeguarding the accuracy and completeness of information & processing methods.

Availability:

Ensuring that information and vital services are available to authorized users when required.

INFORMATION SECURITY THREATS

Transmission Threats
- Eavesdropping/Sniffers
- DoS/DDoS
- Covert channel
- Spoofing
- Tunnelling
- Masquerading/man-in-the middle attacks

Malicious Code Threats
- Virus
- Worms
- Trojans
- Spyware/adware
- Logic Bombs
- Backdoors
- Bots

Improper usage/Un-authorized access
- Hackers(Grey hats, White hats, Black hats)
- Internal intruders
- Defacement
- Open Proxy
- Spam
- Phishing

Password Threats
- Password crackers

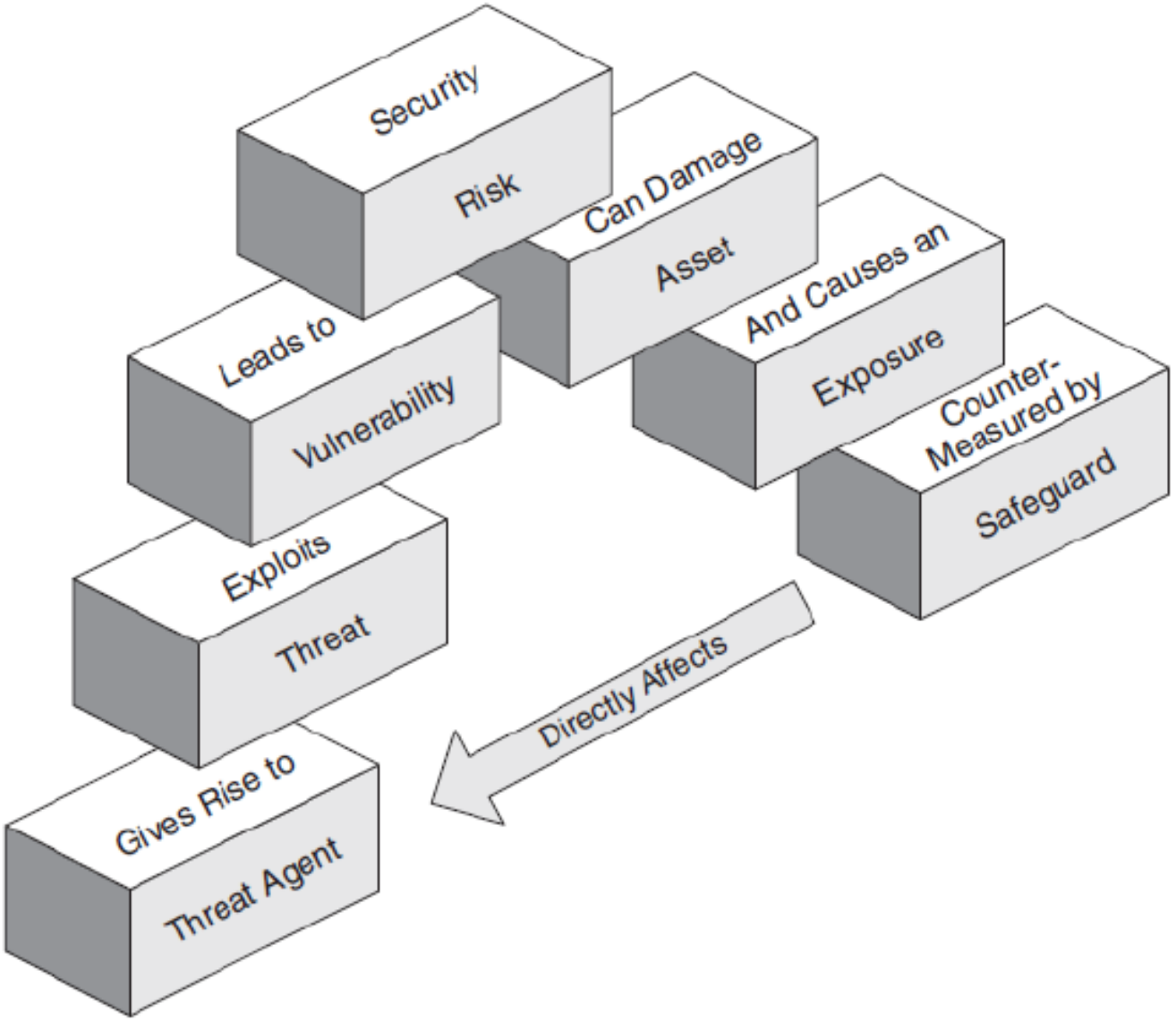
Physical Threats
- Physical access
- Spying

Application Threats
- Buffer over flows
- SQL Injection
- Cross-site Scripting

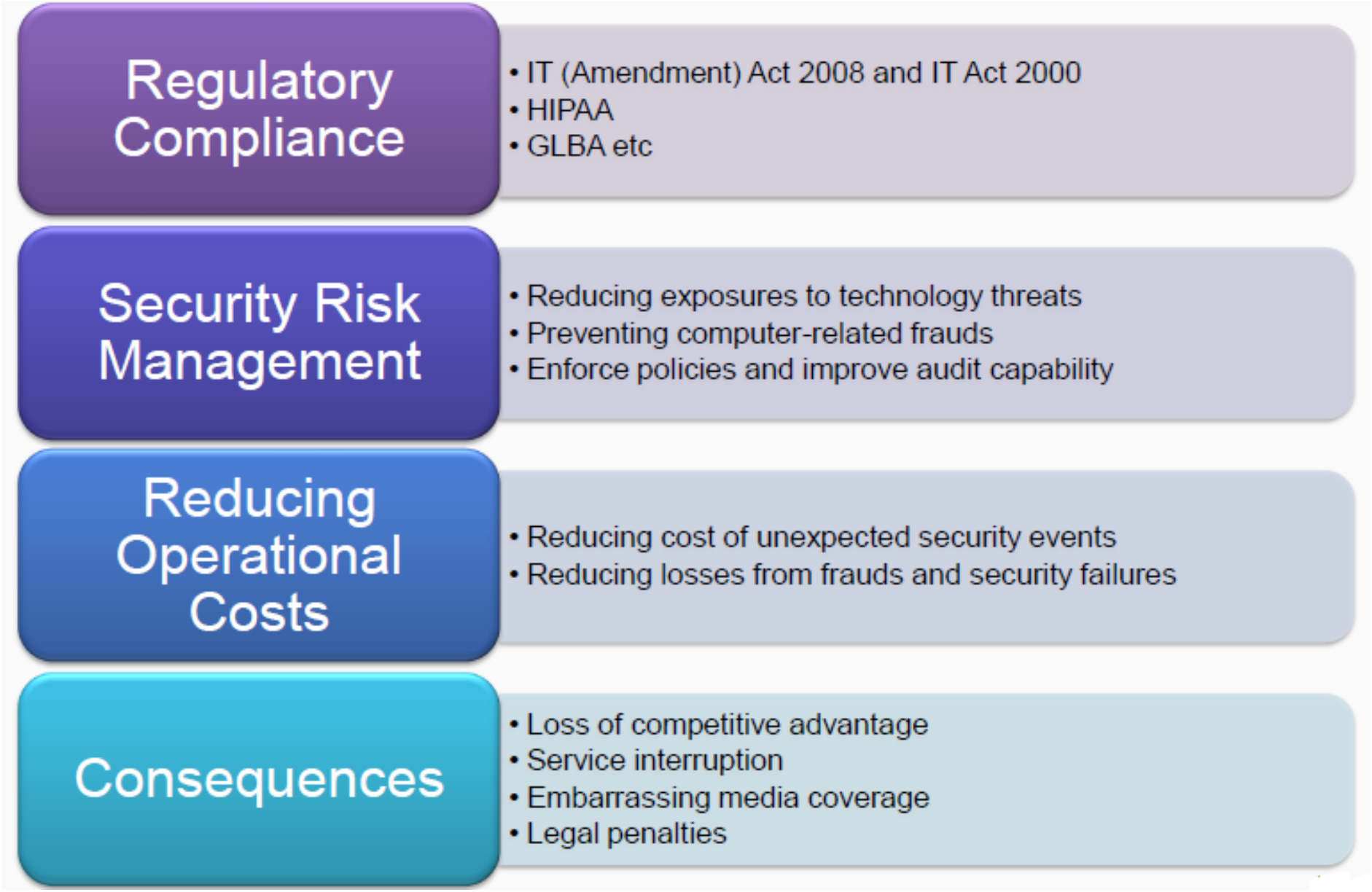
Social engineering
- Dumpster diving
- Impersonation
- Shoulder surfing

Other Threats
- Mobile code

BUILDING BLOCKS OF THE THREAT PROCESS



WHY INFORMATION SECURITY IS IMPORTANT?



UNDERSTANDING RISK - RISK ASSESSMENT

- **Crisis**
- **Dangers**
- –Threats : What are the potential harms
- –Vulnerabilities : Where are the weaknesses that could be exploited
- –Possibility of exposures : Chances of happening
- –Attacks : What are the exploits available today and in the near future
- –Impacts : What losses could the attacks incur
- **Opportunities**
- –Can the desired benefits be retained or sustained if the risk is ignored
- –What other benefits would be removed or added if the risk is managed

ADDRESSING SECURITY THREATS

TECHNOLOGY

- Helps turn IT into a business asset not a cost centre
- Supports day to day security processes
- Is the Enabler for running business successfully

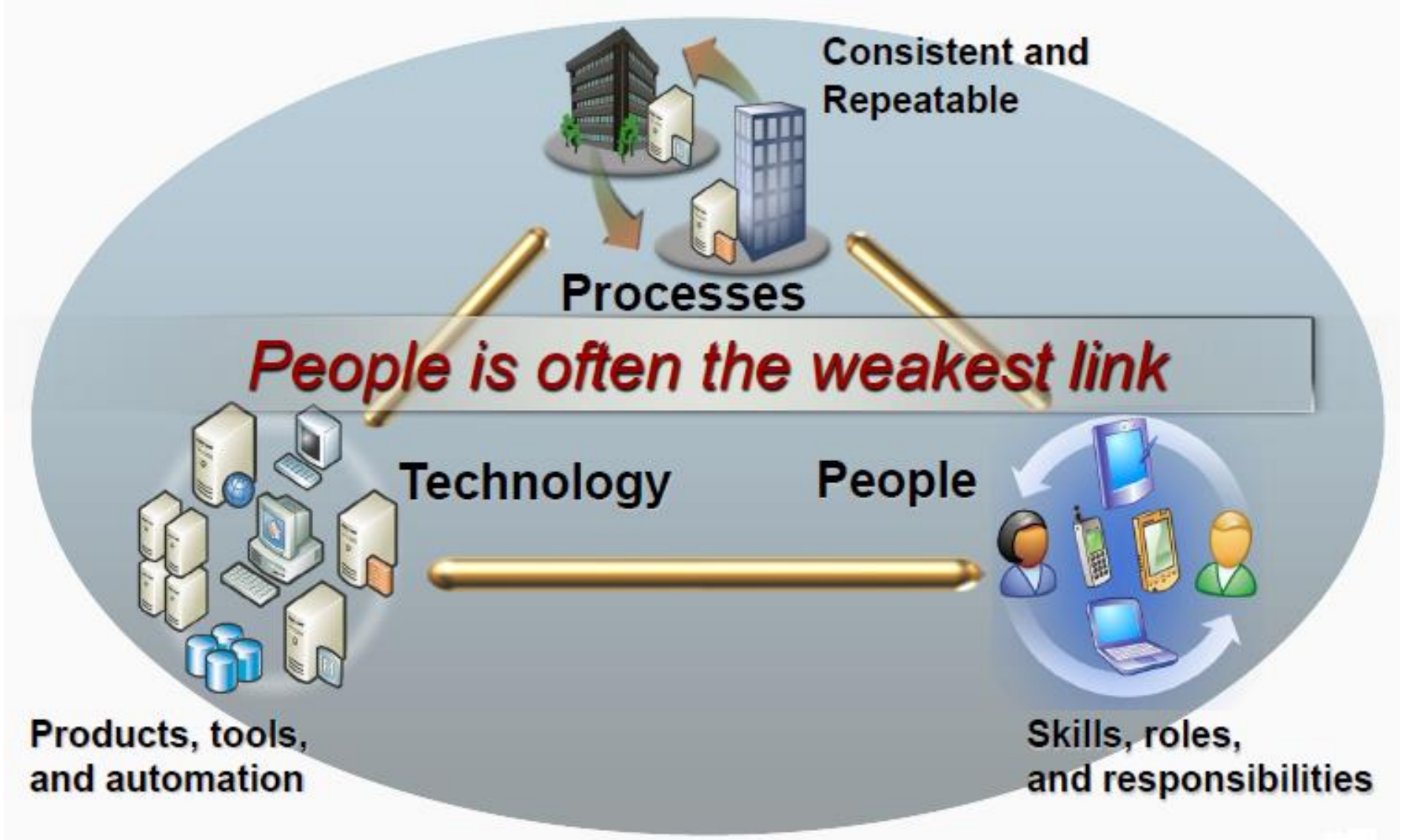
PROCESS

- Data privacy processes to manage data effectively
- IT security processes to implement, manage, and govern security
- Financial reporting processes that include security of the business

PEOPLE

- Company understands the importance of security in the workplace
- Individuals know their role with security governance and compliance
- IT staff has the security skills and knowledge to support your business

MANAGING INFORMATION SECURITY

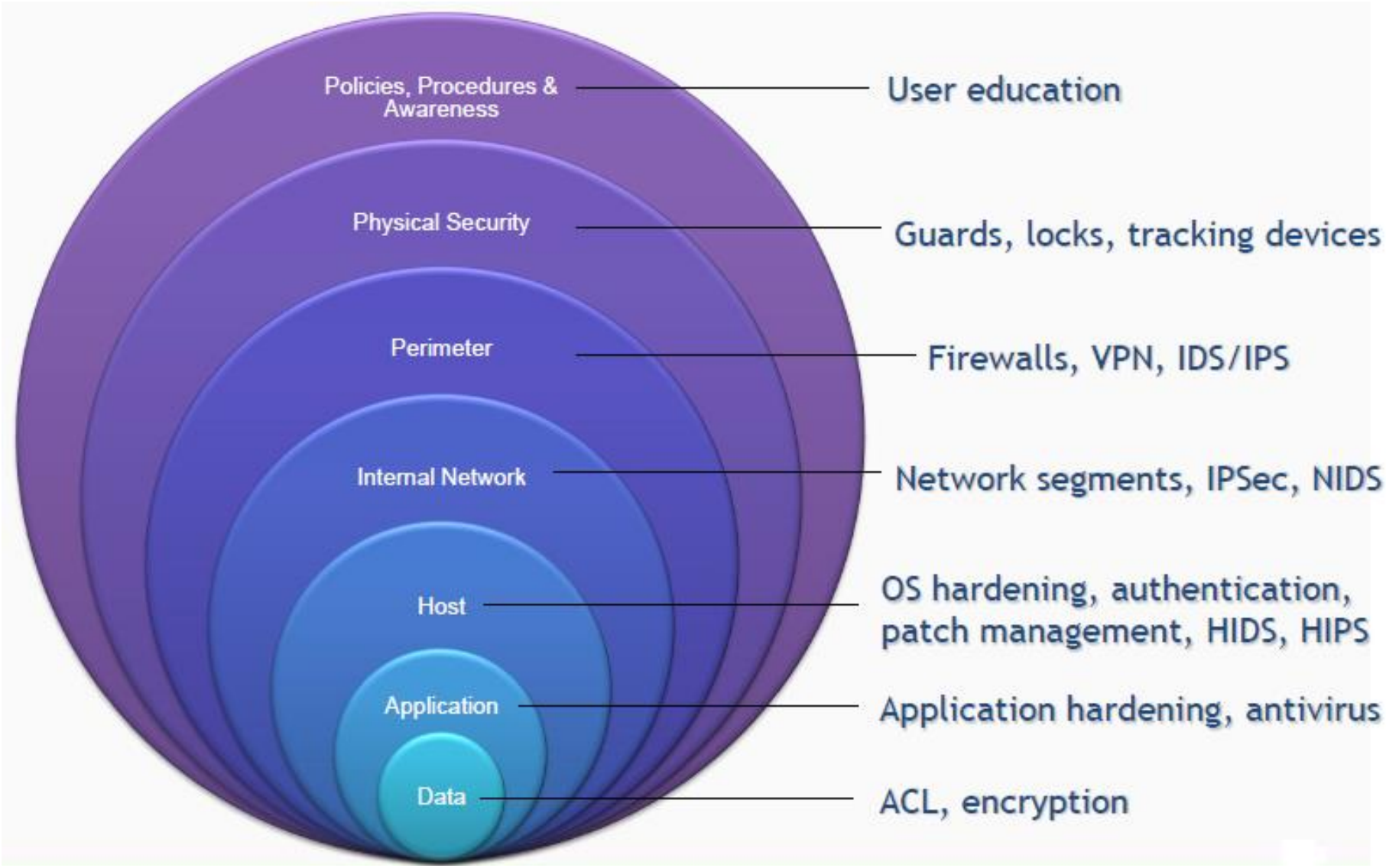


MANAGING INFORMATION SECURITY – PEOPLE & AWARENESS

- No one is going to take precaution if he/she is not aware of the potential negative consequences of his/her actions or inactions
- No one is able to protect himself/herself from attacks if he/she is not aware of how he/she can do it
- Ignorance is no longer a bliss - social engineering attacks remain as one of the most successful attack on the Internet
- Consistently the single most commonly listed program for any security initiatives, in both public and private sector is to:

  - **Communicate security policies, procedures, and processes**
  - **Communicate and clarify roles and responsibilities**
  - **Communicate lessons learned and share experiences for improvements**
  - **Compliance requirement**

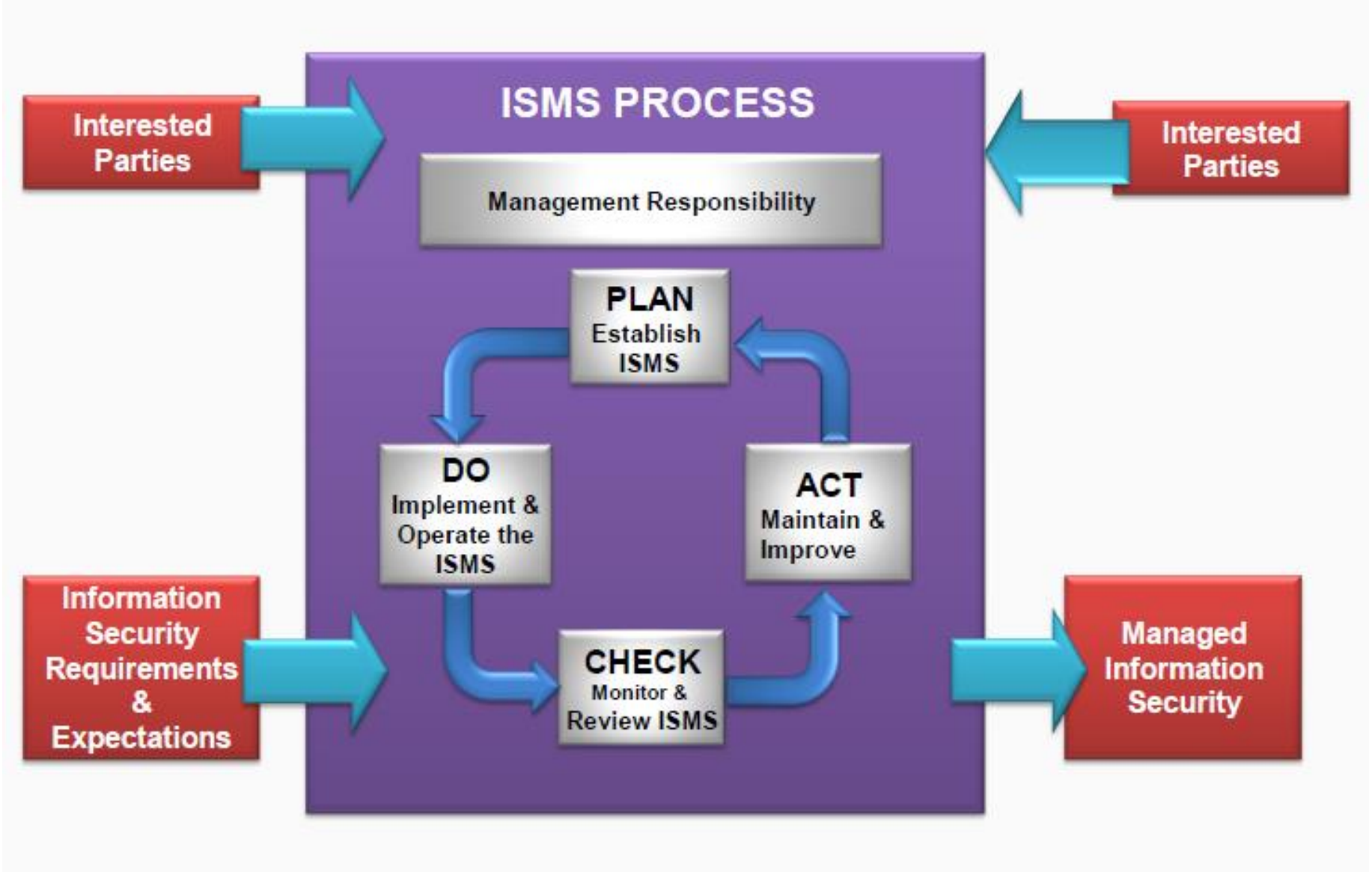
MANAGING INFORMATION SECURITY – TECHNOLOGY



MANAGING INFORMATION SECURITY – PROCESSES

- **POLICIES:** General statement produced by senior management that dictates what role security plays within the organization.
- **STANDARDS:** Mandatory activities, actions or rules
- **BASELINES:** A point in time that is used as a comparison for future changes.
- **GUIDELINES:** Recommended actions and operational guides to users when a specific standard does not apply.
- **PROCEDURES:** Detailed step-by-step tasks that should be performed to achieve a certain goal.

PLAN, DO, CHECK, ACT (PDCA) PROCESS

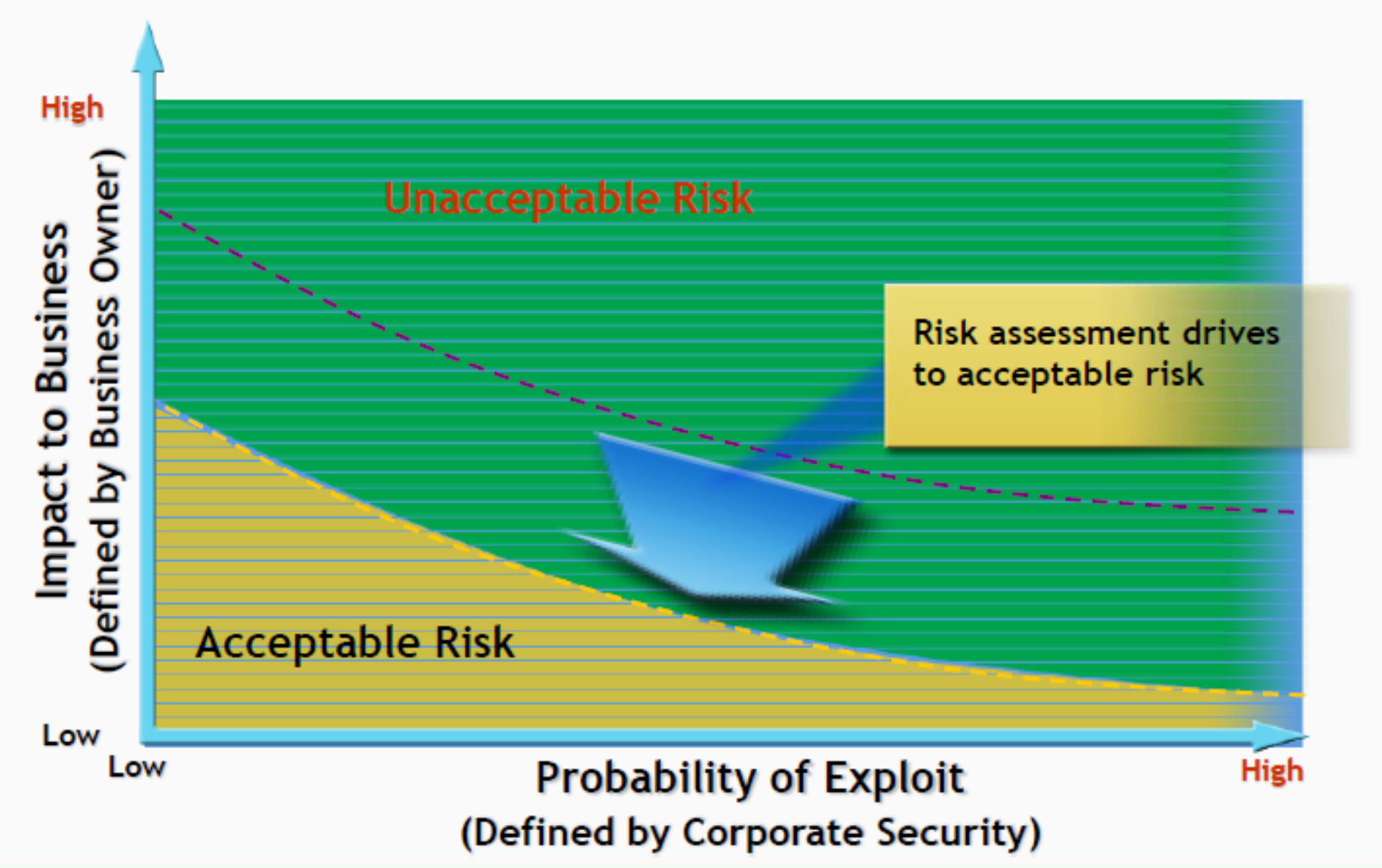


MANAGING RISK

- **RISK**
  - –Dealing with risk is like riding the wind of dangers
  - –Direction and velocity of wind change with monsoon and season
  - –Not always predictable –uncertainty is inherent

- **MANAGING RISK REQUIRES**
  - –Continuous monitoring of the information systems in operation,
  - –Put in place processes and training people to be responsive to new attacks, new weaknesses, and new exploits that could emerge or be discovered from time to time.

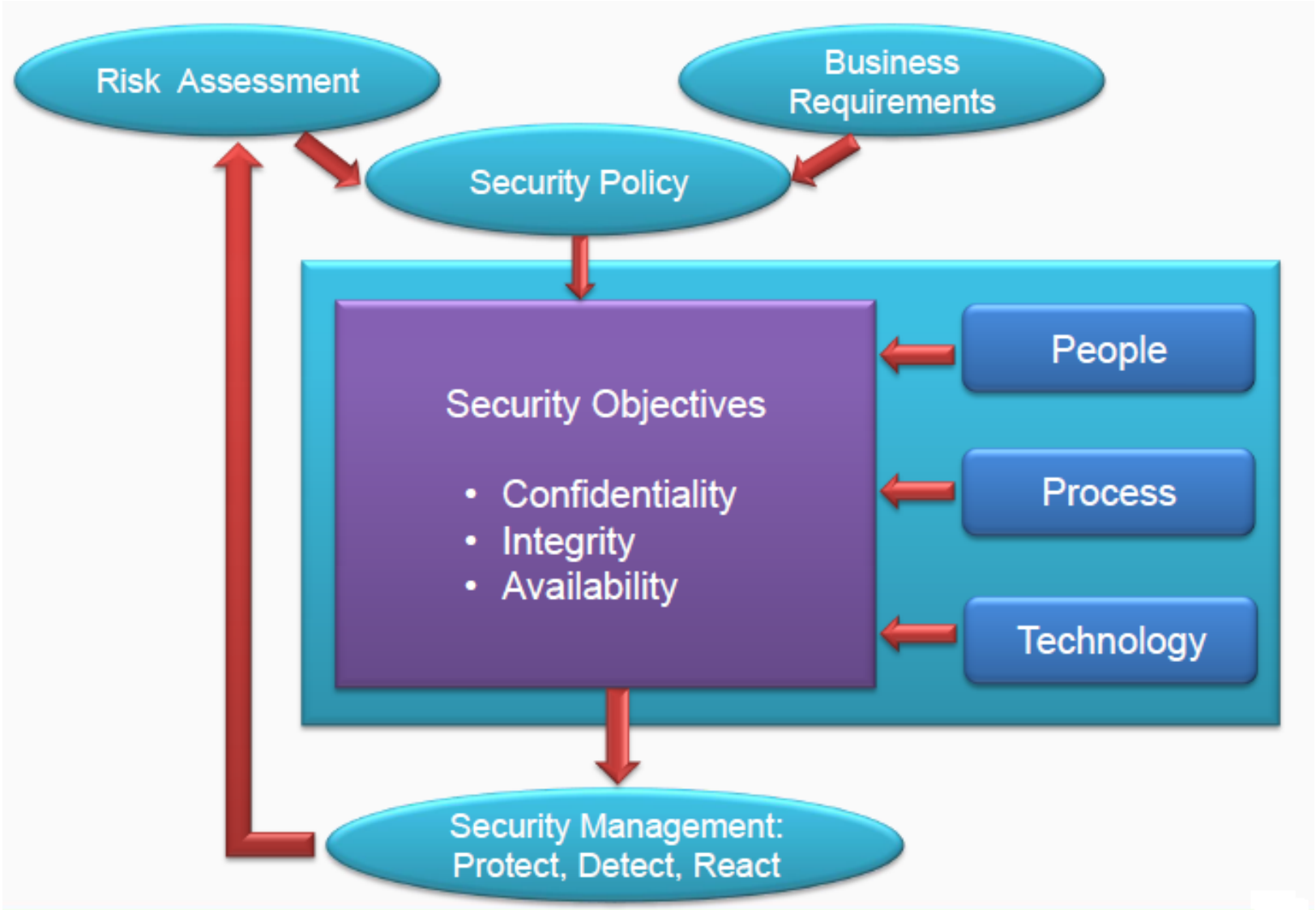
ENTERPRISE RISK MODEL



SECURITY POLICY

- Business objectives should drive the policy's creation, implementation, and enforcement. The policy should not dictate business objectives.
- It should be an easily understood document that is used as a reference point for all employees and management.
- It should be developed and used to integrate security into all business functions and processes.
- It should be derived from and support all legislation and regulations applicable to the company.
- It should be reviewed and modified as a company changes, such as through adoption of a new business model, a merger with another company, or change of ownership.
- Each iteration of the policy should be dated and under version control

FRAMEWORK FOR INFORMATION SECURITY



INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

- **ISMS is that part of overall management system based on a business risk approach to**
  - Establish
  - Implement
  - Operate
  - Monitor
  - Review
  - Maintain &
  - Improve

Information security

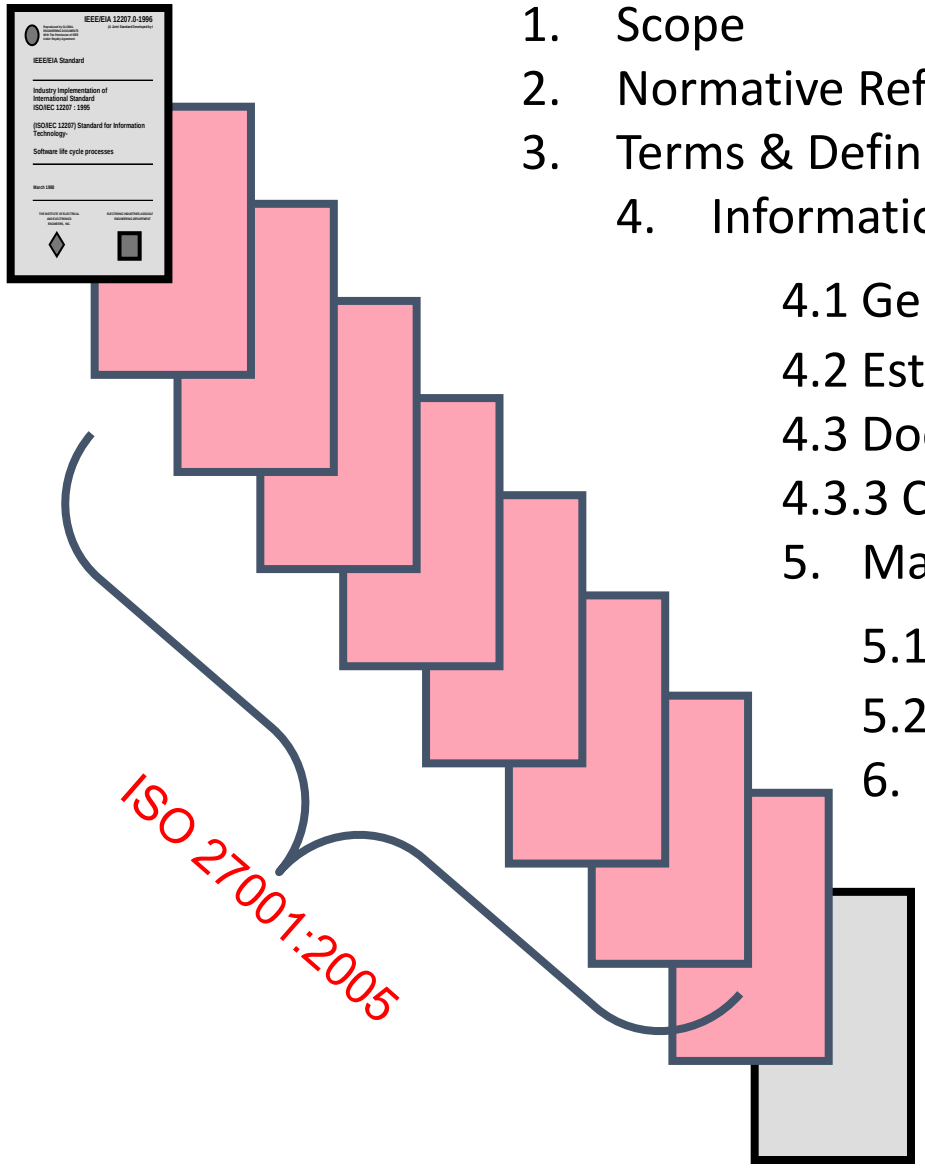
- **ISMS is a management assurance mechanism for security of information asset concerning its**
  - Availability
  - Integrity and
  - Confidentiality

ISMS STANDARDS

- ISO/ IEC 27001 : 2005
  - A specification (specifies requirements for implementing, operating, monitoring, reviewing, maintaining & improving a documented ISMS)
  - Specifies the requirements of implementing of Security control, customised to the needs of individual organisation or part thereof.
  - Used as a basis for certification
- ISO/IEC 27002 : 2005 (Originally ISO/IEC 17799:2005)
  - A code of practice for Information Security management
  - Provides best practice guidance
  - Use as required within your business
  - Not for certification

Both ISO 27001 and ISO 27002 security control clauses are fully harmonized

ISO 27001 STRUCTURE



1. Scope
2. Normative References
3. Terms & Definitions
4. Information Security Management System

4.1 General

4.2 Establish and manage ISMS

4.3 Documentation

4.3.3 Control of Records

5. Management Responsibility

5.1 Management Commitment

5.2 Resource Management

6. Internal ISMS Audits
7. Management Review of the ISMS

8. ISMS Improvement

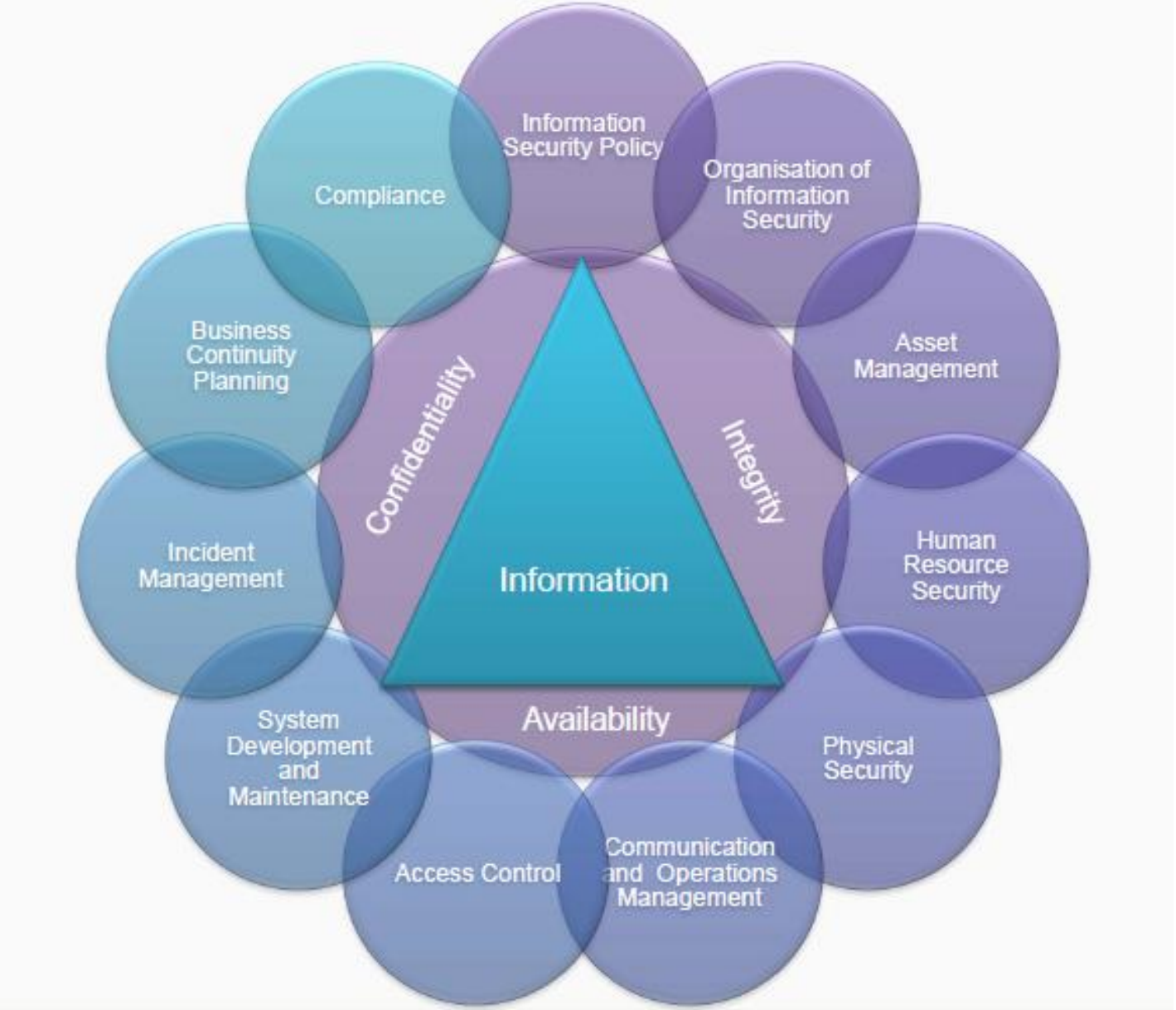
8.1 Continual Improvement

8.2 Corrective Actions

8.3 Preventive Actions

Annexure A, B & C

ISO 27001 CONTROL CLAUSES



SECURITY CONTROL CLAUSES OF ISO 27001

A.5 Security Policy

A.6 Organization of Information Security

A.7 Asset Management

A.8 Human Resource Security

A.9 Physical & environmental security

A.10 Communications & operations management

A.12 Info. Systems Acquisition development & maintenance

A.11 Access control

A.13 Information Security Incident Management

A.14 Business Continuity Management

A.15 Compliance

NIST

- NIST : National Institute of Standards and Technology
- Mission:

  To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

FISMA

- The Federal Information Security Management Act (FISMA) is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats.
- FISMA was signed into law part of the Electronic Government Act of 2002.

PURPOSE OF FISMA

- Provide a consistent framework for protecting information at the federal level.
- Provide effective management of risks to information security.
- Provide for the development of adequate controls to protect information and systems.
- Provides a mechanism for effective oversight of federal security programs.

FISMA AND NIST

VISION INCLUDES:

- **Standards for categorizing information and information systems by mission impact.**
- **Standards for minimum security requirements for information and information systems.**
- **Guidance for selecting appropriate security controls for information systems.**
- **Guidance for assessing security controls in information systems and determining security control effectiveness.**
- **Guidance for certifying and accrediting information systems.**

GOALS INCLUDE:

- **The implementation of cost-effective, risk-based information security programs.**
- **The establishment of a level of security due diligence for federal agencies and contractors supporting the federal government.**
- **More consistent and cost-effective application of security controls across the federal information technology infrastructure.**
- **More consistent, comparable, and repeatable security control assessments.**
- **A better understanding of enterprise-wide mission risks resulting from the operation of information systems.**
- **More complete, reliable, and trustworthy information for authorizing officials--facilitating more informed security accreditation decisions.**
- **More secure information systems within the federal government including the critical infrastructure of the United States.**

NIST OUTLINES NINE STEPS TOWARD COMPLIANCE WITH FISMA:

- Categorize the information to be protected.
- Select minimum baseline controls.
- Refine controls using a risk assessment procedure.
- Document the controls in the system security plan.
- Implement security controls in appropriate information systems.
- Assess the effectiveness of the security controls once they have been implemented.
- Determine agency-level risk to the mission or business case.
- Authorize the information system for processing.
- Monitor the security controls on a continuous basis.

BEST PRACTISES FOR INFORMATION SECURITY RISK MANAGEMENT

- Establish an Information Security Policy
- Dedicate resource/s for Information Security System
- Do Risk Assessments regularly
- Create Awareness across the Organisation
- Involve App Development Teams in implementation
- Conduct Vulnerability Assessments at periodic intervals
- Enable Monitoring of your Digital Assets –Security Operations & Management
- Integrate Vulnerability reports into Security Operations
- Regular reviews to measure control effectiveness

THANKS