



www.isea.gov.in

Information Security Management System Overview for CS&DPL at NALSAR, Hyderabad

Sh. Tapas Bandyopadhyay, Scientist F

Sh. M Vellaipandi , Scientist F

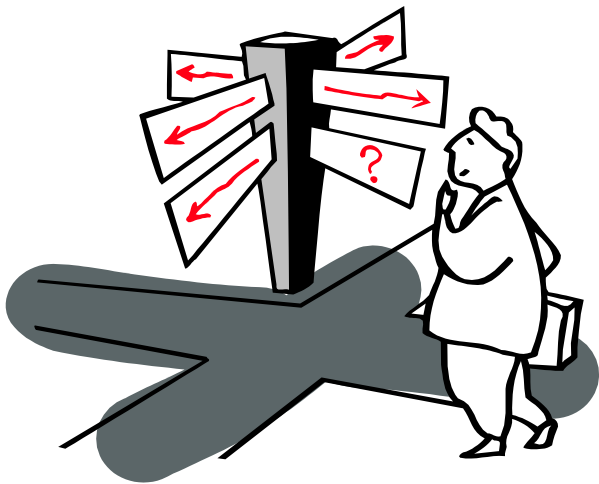
STQC ,MeitY, Govt. of India





www.isea.gov.in

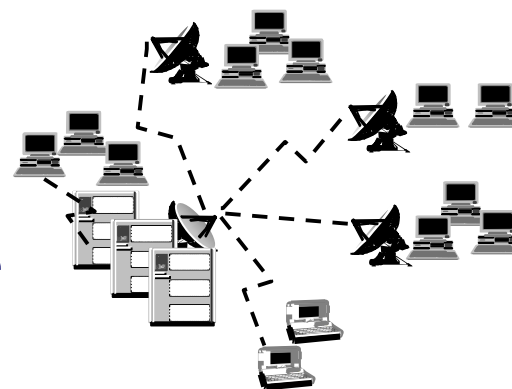
ISMS Overview





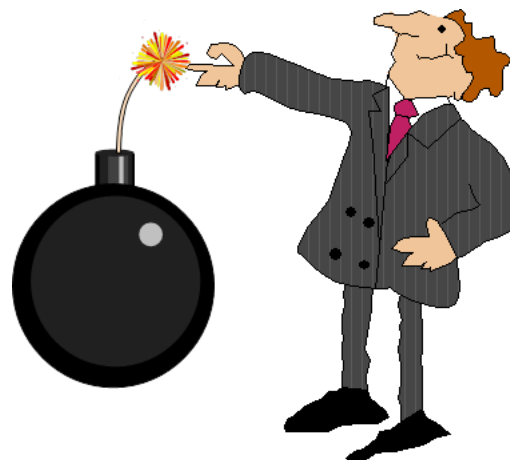
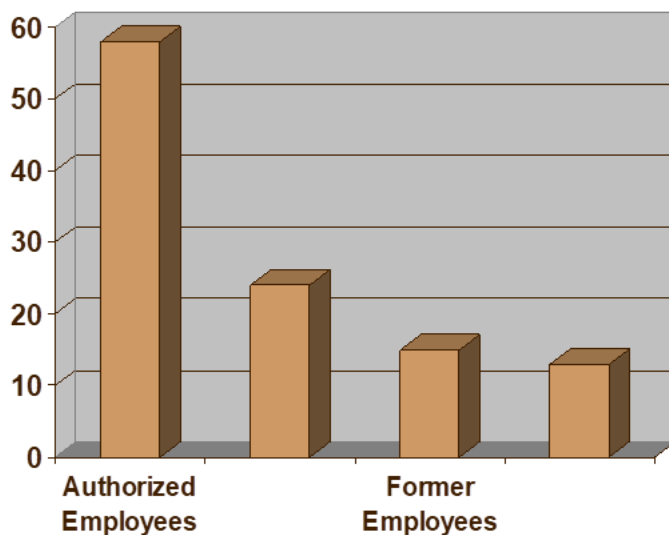
ISMS Overview

- Dependence on IT and other information for development, production and delivery
- Various Internal Applications like
 - Financial databases
 - Employee time booking
 - Providing helpdesk and other services
 - Providing remote access to customers / employees
 - Remote Access of client systems
 - Interaction with the outside world through
 - e-mail, internet
- Usage of information Systems to manage third parties and outsourced suppliers



ISMS Overview

If you think the greatest threat to information security comes from the outside--competitors, hackers or viruses--think again.



Those external threats will only distract from the dangers you face from inside your own organization.



www.isea.gov.in

ISMS Overview

Protection **of Information and Information Systems to meet** Business and Legal Requirement by

- Provision and demonstration of secure environment to clients
- Managing security between projects from competing clients
- Preventing loss of product knowledge to external attacks, internal thefts
- Preventing Leak of confidential information to competition
- Meeting Parent company requirements
- Ease of access to large mobile work force
- Introduction of new technologies and tools
- Managing Cost vs Risk
- Managing Legal Compliance.





www.isea.gov.in

ISMS Overview

What it implies?

Whatever **form** the information takes, or means by which it is **shared** or **stored**, it should always be **appropriately protected** throughout its **life cycle**.





ISMS Overview

Information is an asset, like other important business assets, has value to an organization

Can exist in many forms

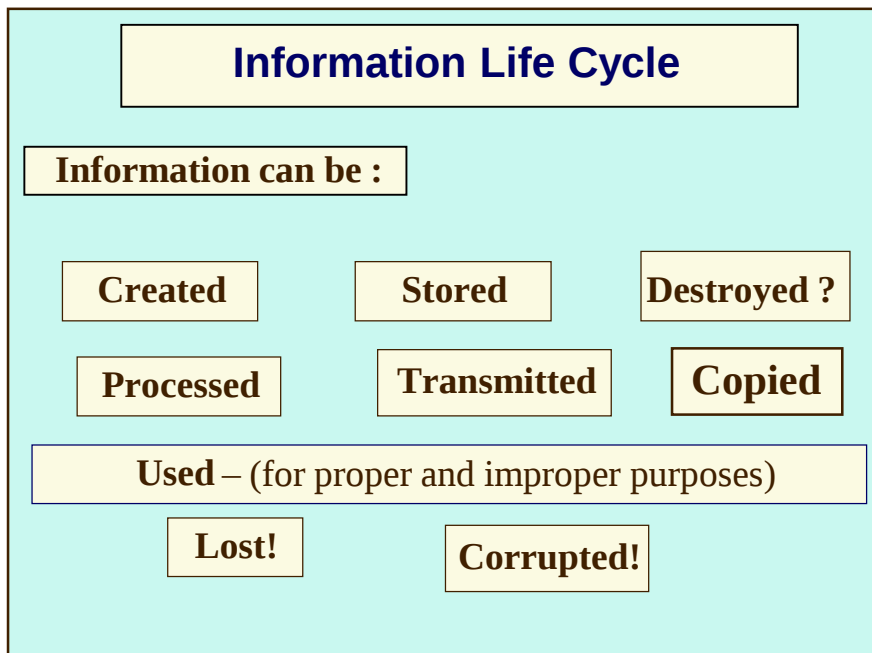
- data stored on computers
- transmitted across networks
- printed out
- written on a paper
- sent by fax
- stored on disks
- held on microfilm
- spoken in conversations over the telephone
- ..





ISMS Overview

Information Life Cycle



Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected throughout its life cycle



ISMS Overview

Challenges faced by implementing organizations

- Lack of written policies (if at all written but not followed)
- Lack of clarity on what needs to be protected and to what extent
- Unstructured approach to security initiatives (without formal Risk Assessment)
- Lack of clarity on threats and organisational vulnerabilities
- Lack of strong password policies
- Inadequately trained manpower on Security issues



ISMS Overview

Challenges faced by implementing organizations

- Lack of planned responses to security events
- No appropriate buy-in at the top level about the importance of security
- Normally absence of a structured disaster recovery and business continuity plan
- Relationship between Security Risk Assessment and Business continuity Plan
- Failure to link the importance of security to business goals of the organization, relegating security to an after-thought
- Over reliance on technical controls
- Keeping security plans and policies as dynamic as the rest of the network, resulting in short-term fixes rather than long term planning



ISMS Overview

Result ?????

- **Uncertainty over issues like**
 - **Accessibility of Information wherever and whenever required**
(Availability)
 - **Completeness and correctness of Information for the purpose at the time of use**
(Integrity)
 - **Availability of information only to those who are authorised to access it**
(Confidentiality)

This is likely to result in lower trust levels



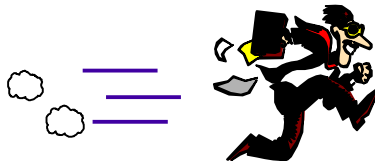
www.isea.gov.in

ISMS Overview

Risk to Information Systems because of



High User knowledge
of IT sys.



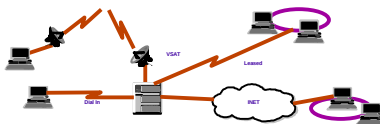
Theft , Sabotage,
Misuse, Hacking



Version Control
Problems



Unrestricted Access



Systems / Network
Failure



Lack of documentation



Virus



Natural calamities

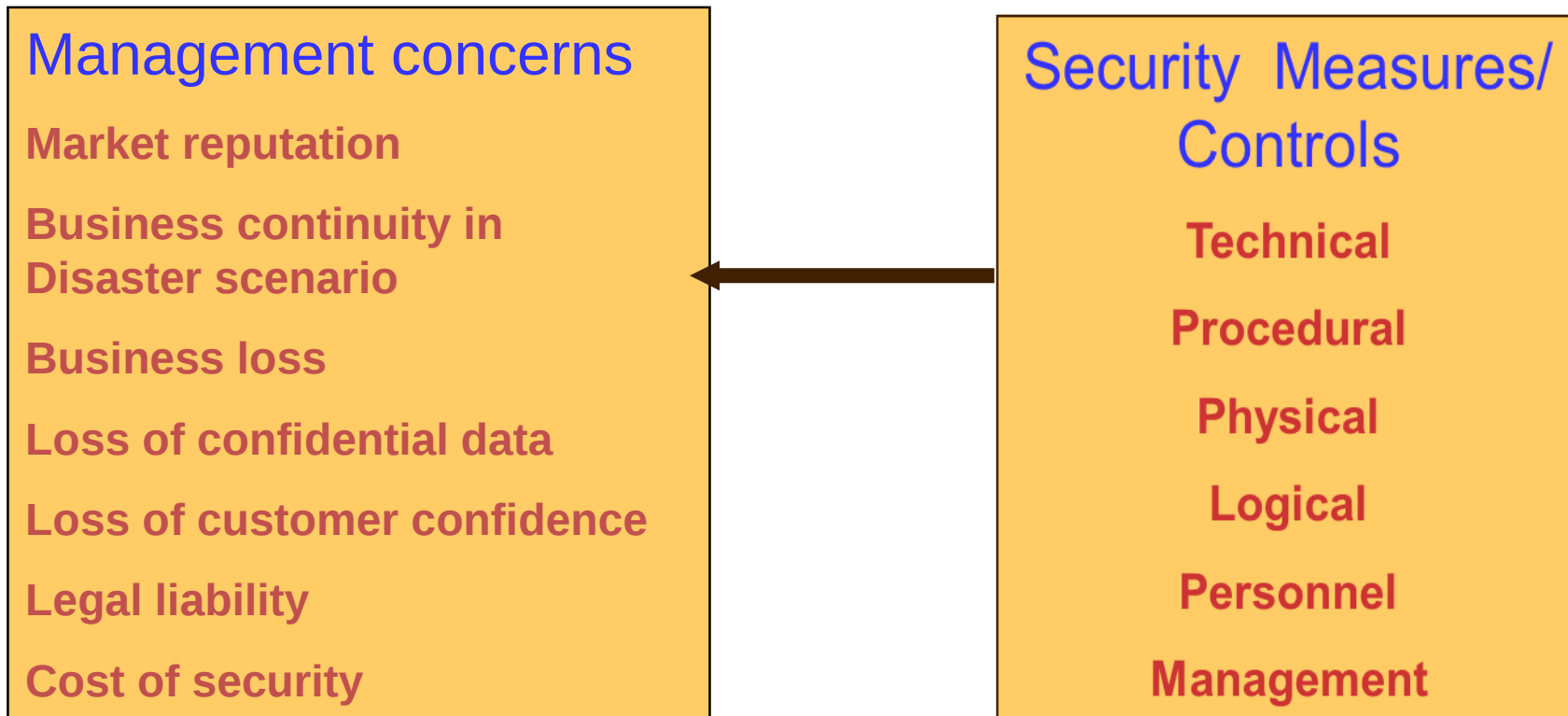


Fire



ISMS Overview

What is needed?





ISMS Overview

Information Security is about protecting Information through selection of appropriate Security Controls

- ✓ protects information from a range of threats
- ✓ ensures business continuity
- ✓ minimizes financial loss
- ✓ maximizes return on investments and business opportunities

IS A BUSINESS ISSUE



ISMS Overview

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.



ISMS Overview

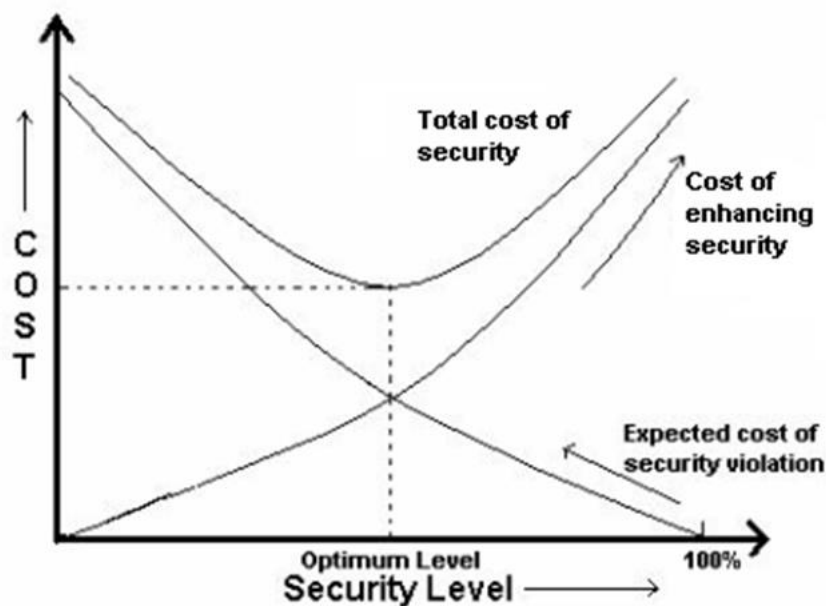
Security Vs Convenience

- To make the decisions concerning the security of computer networks involve a tradeoff between security and convenience
- More security measures may lead to inconvenience and complaints from users



ISMS Overview

Security Vs Convenience

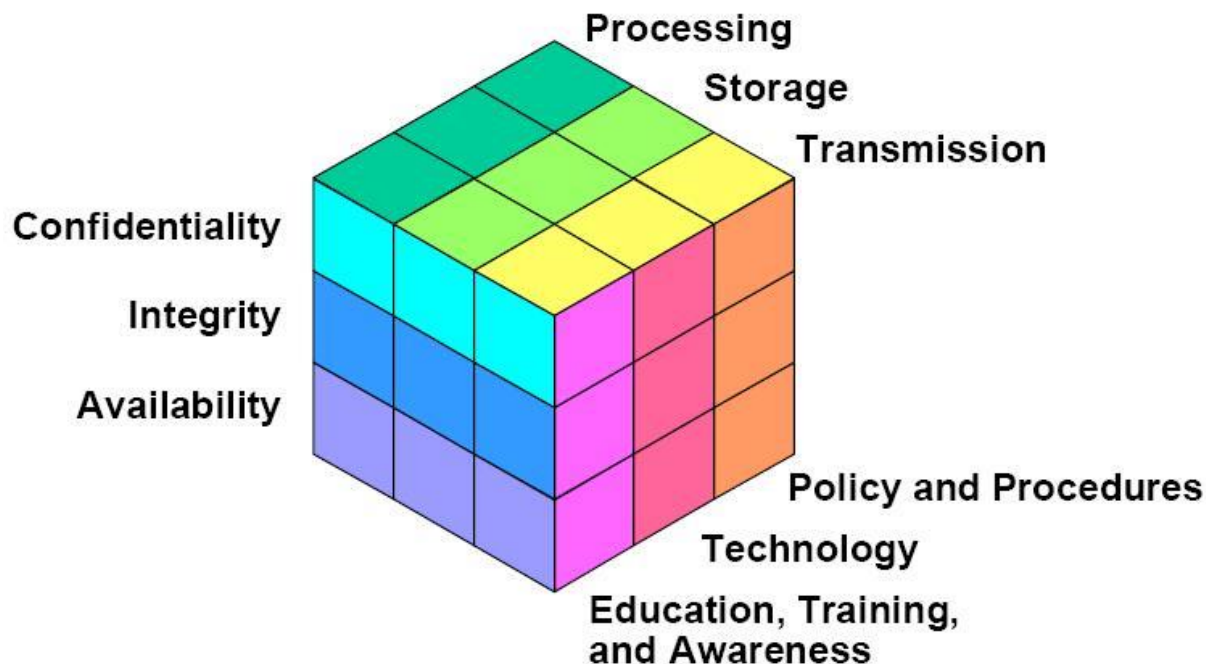




www.isea.gov.in

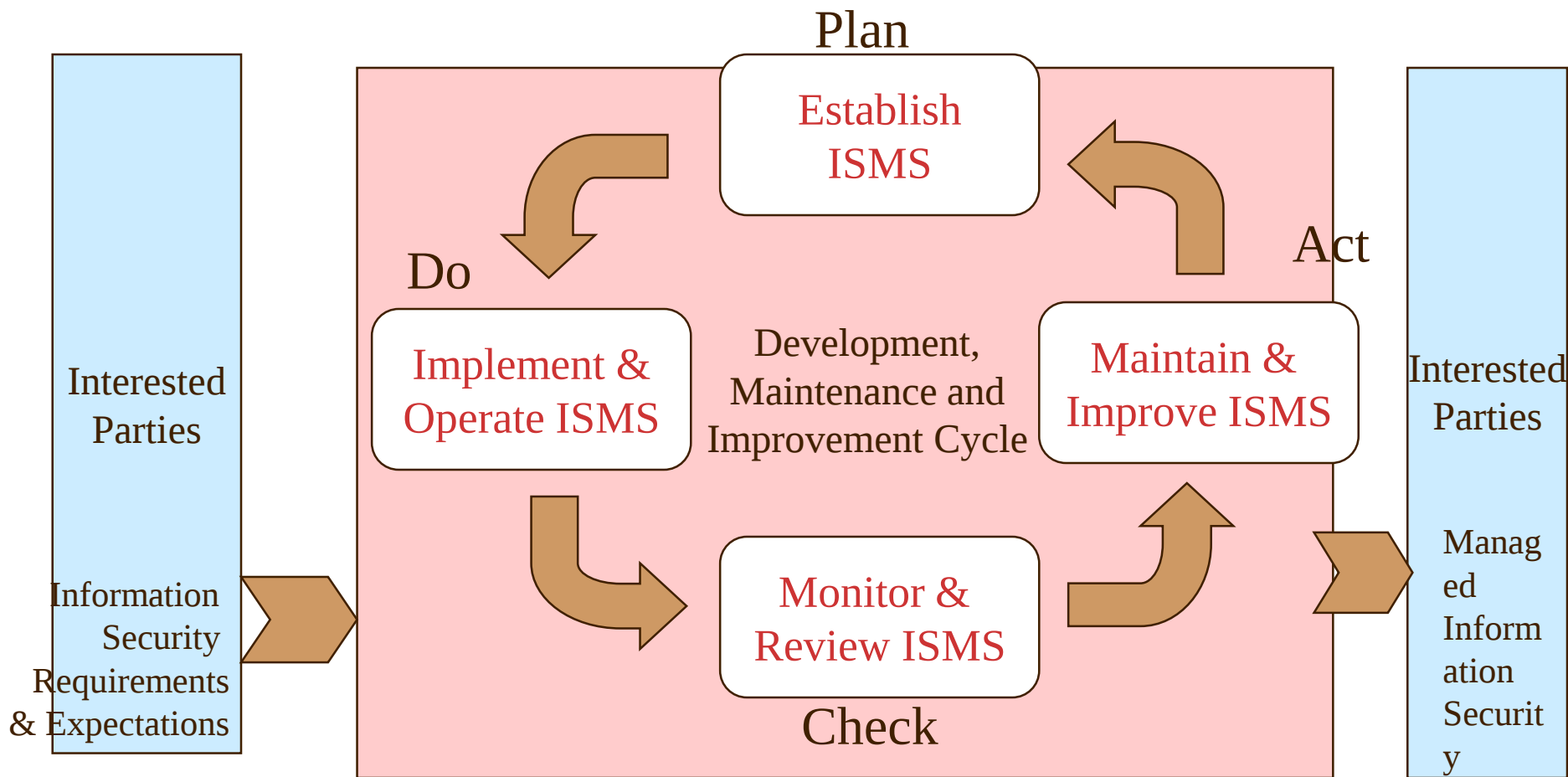
ISMS Overview

Information Security Model



ISMS Overview

PDCA Model applied to ISMS processes





ISMS Overview

Information Security Management System

With an ISMS we are not intending to make the system **‘hacker proof’**, but develop a mechanism which can, to a large extent

- ❖ Anticipate potential problems
- ❖ Prepare through proactive measures
- ❖ Protect against considerable damages
- ❖ Ensure recovery and restoration



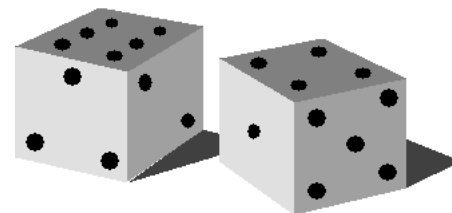
“Failure is not when you fall down, but when you fail to get up”



ISMS Overview

What is security risk

- A security risk is the potential that a given threat will exploit vulnerabilities to cause loss/damage to asset and hence directly/indirectly to the organization
- It is a function of the impact of the undesirable event and the likelihood of the event occurring.





ISMS Overview

What is security risk

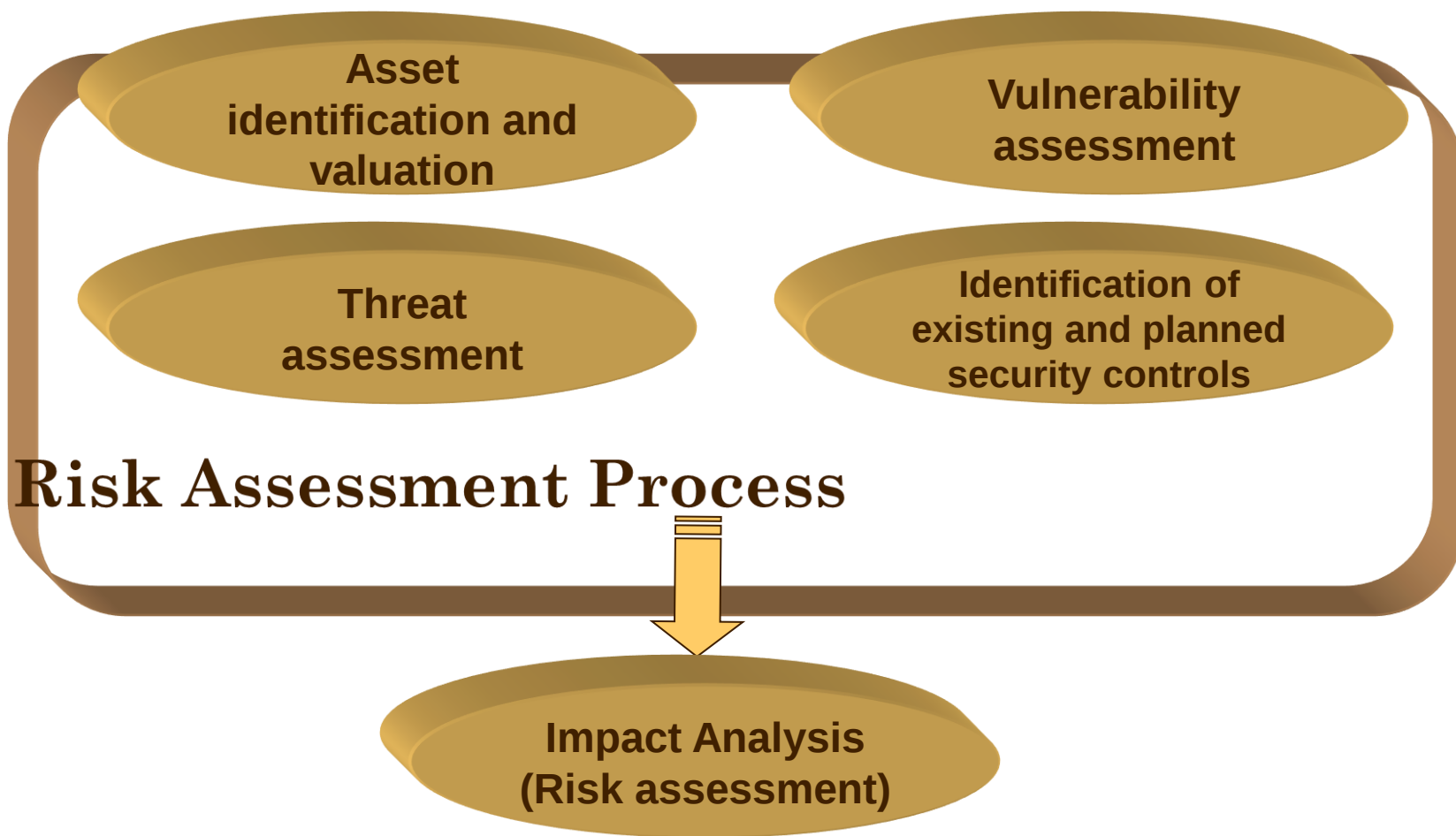
- The process of identifying security risks, and determining their magnitude (this is also sometimes referred to risk analysis)
- It produces an estimate of the risk to an asset at a given point in time. It answers the following questions
 - What can go wrong
 - How bad could it be
 - How likely is it to occur
 - How to manage the risk





ISMS Overview

Risk Assessment Process





ISMS Overview

Information Security Management System

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 Overview

Information Security Management System

ISMS enables an organization to adopt a proactive approach through a mechanism of

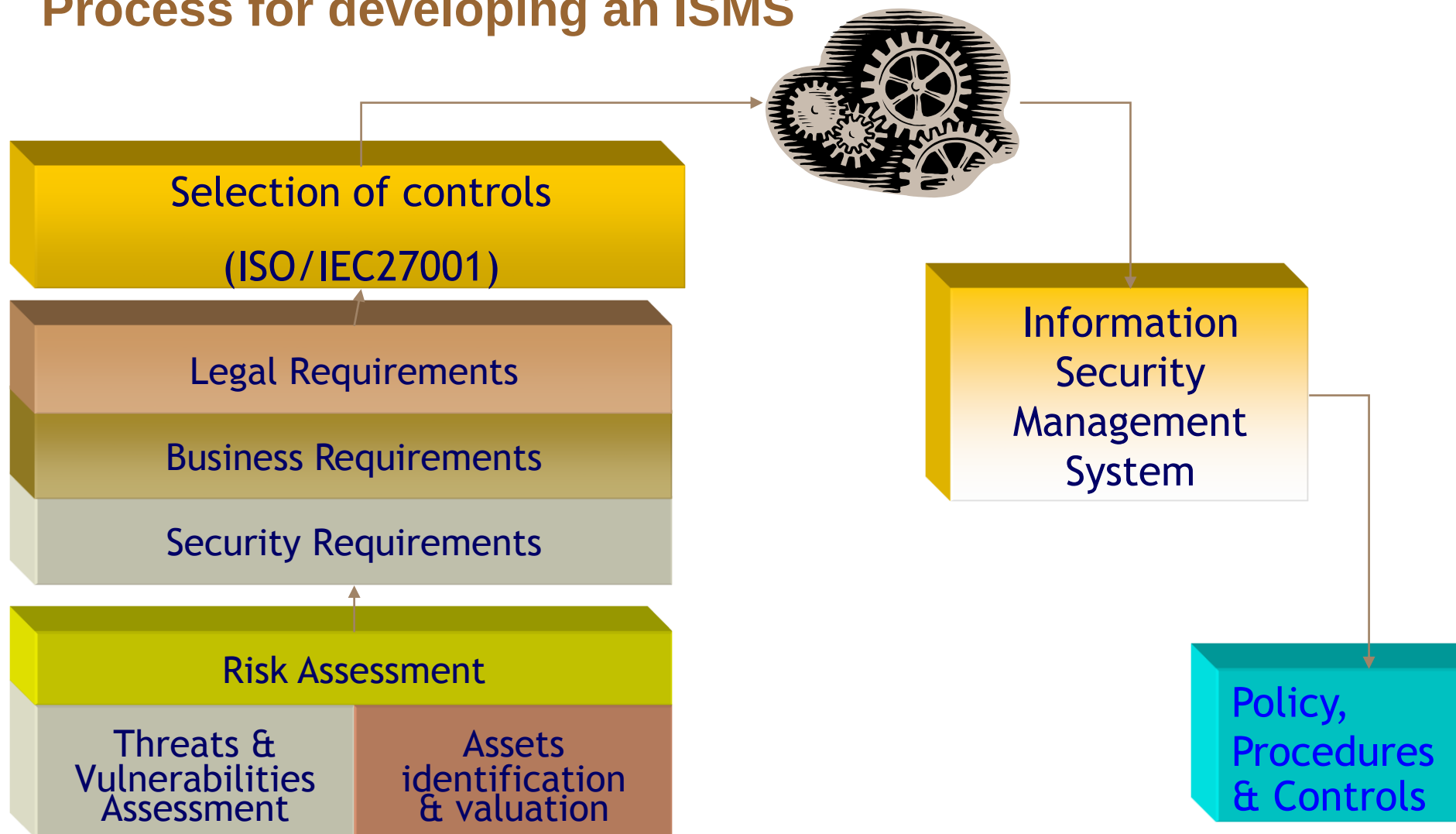
- **awareness**
- **planning**
- **training**
- **action**
- **measurement & reporting and**
- **review on a continuous basis**



www.isea.gov.in

ISMS Overview

Process for developing an ISMS





ISMS Overview

Information Security Management System

ISO/IEC27001: 2013

- A specification (that specifies the requirements for implementing, operating, monitoring, reviewing, maintaining & improving a documented ISMS, within the context of organisation's overall business risks)
- Specifies the requirements of implementing of Security control, customised to the needs of individual organization or a part of it .
- **Used as a basis for certification**



ISMS Overview

Information Security Management System

■ Security Policy Manual

- *Summary of management framework including the information security policy and the control objectives and implemented controls given in the statement of applicability.*

■ Procedures

- *Procedures adopted to implement the controls required.*

■ Operational Documents

- *Explains details of specific tasks or activities.*

■ Records

- *Evidence of activities carried out.*



www.isea.gov.in

ISMS Overview

Information Security Management System

Level 1

Security
Manual

Level 2

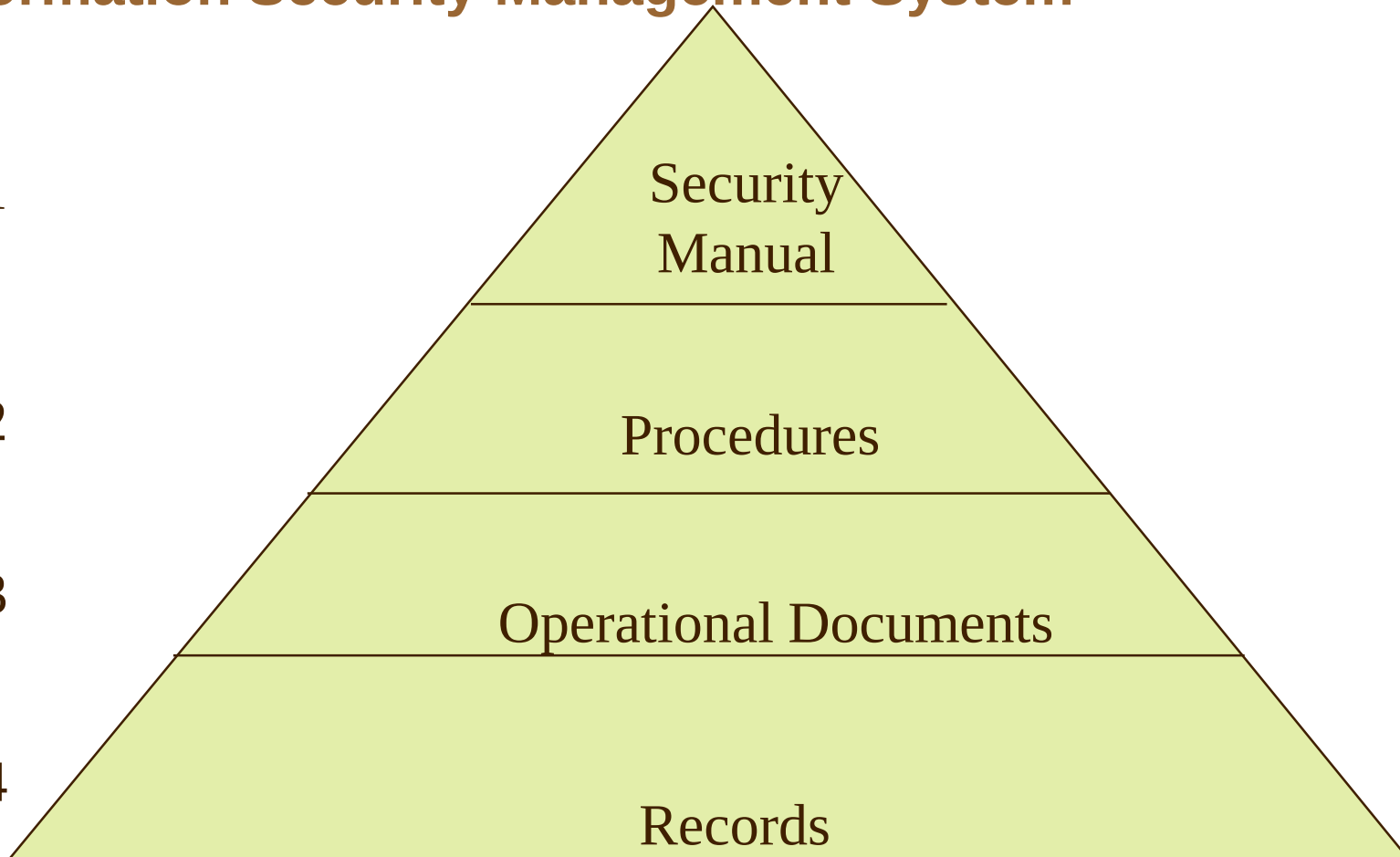
Procedures

Level 3

Operational Documents

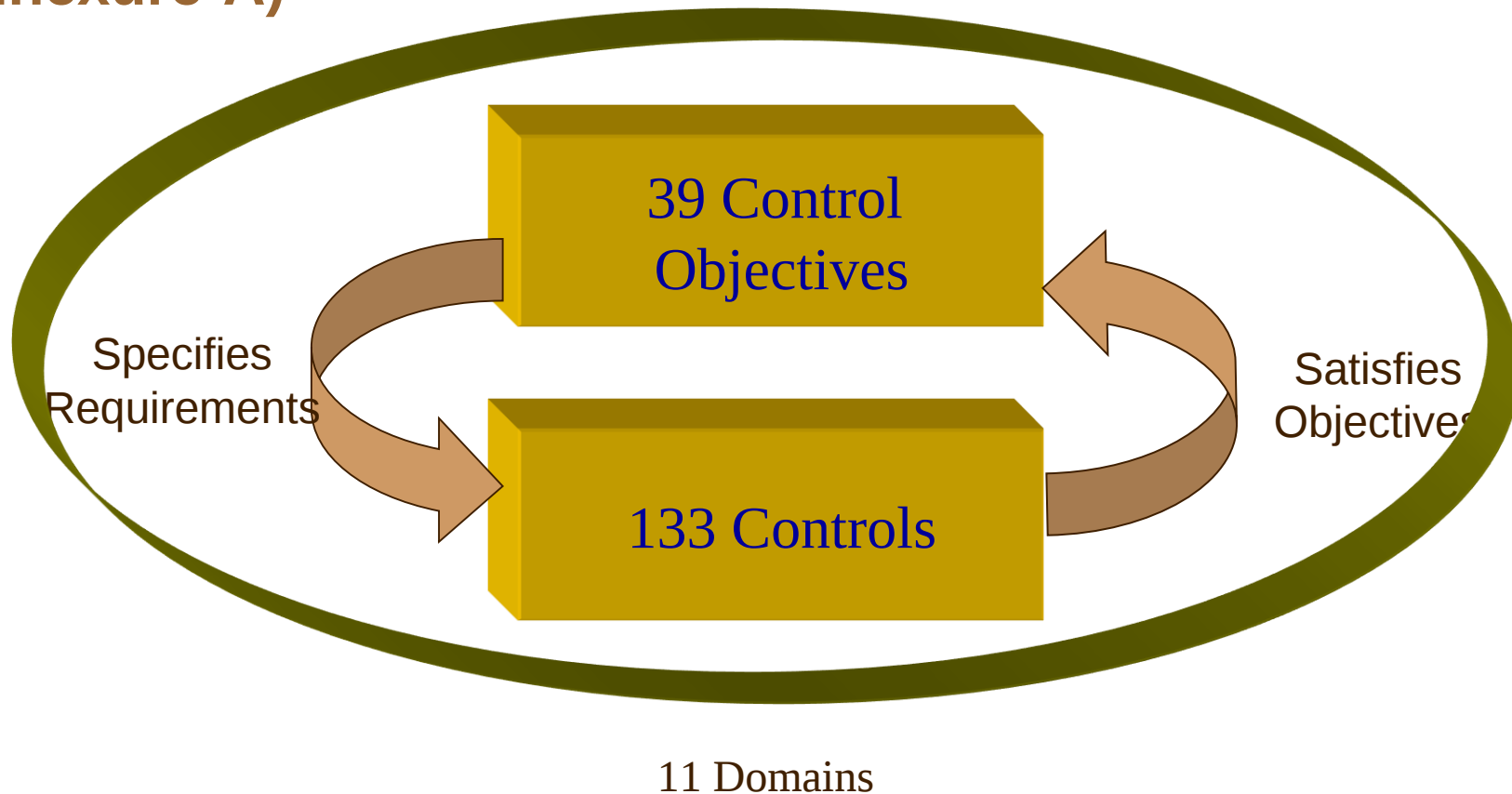
Level 4

Records



ISMS Overview

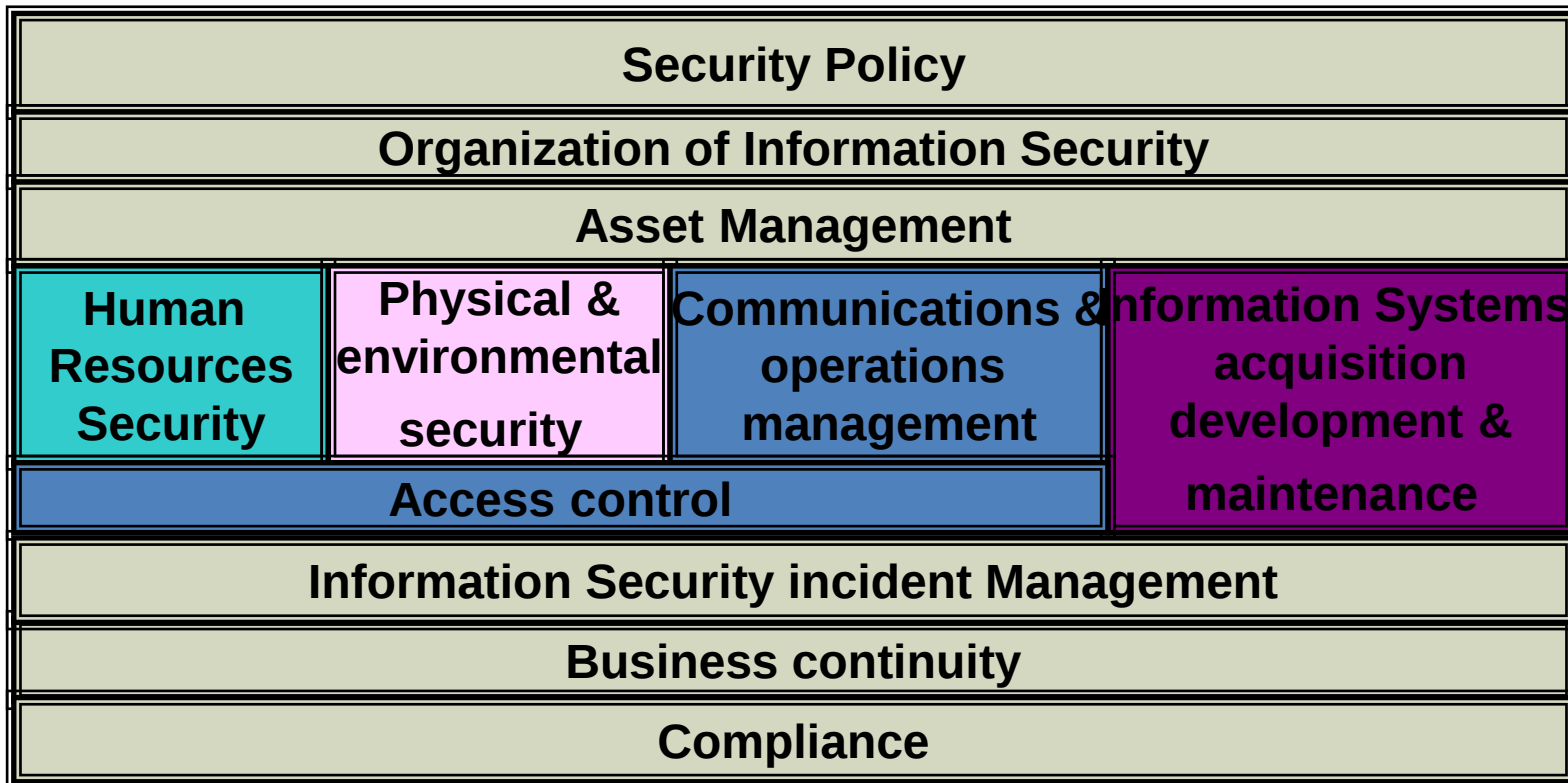
ISO/IEC27001: Control Objectives and Controls (Annexure-A)





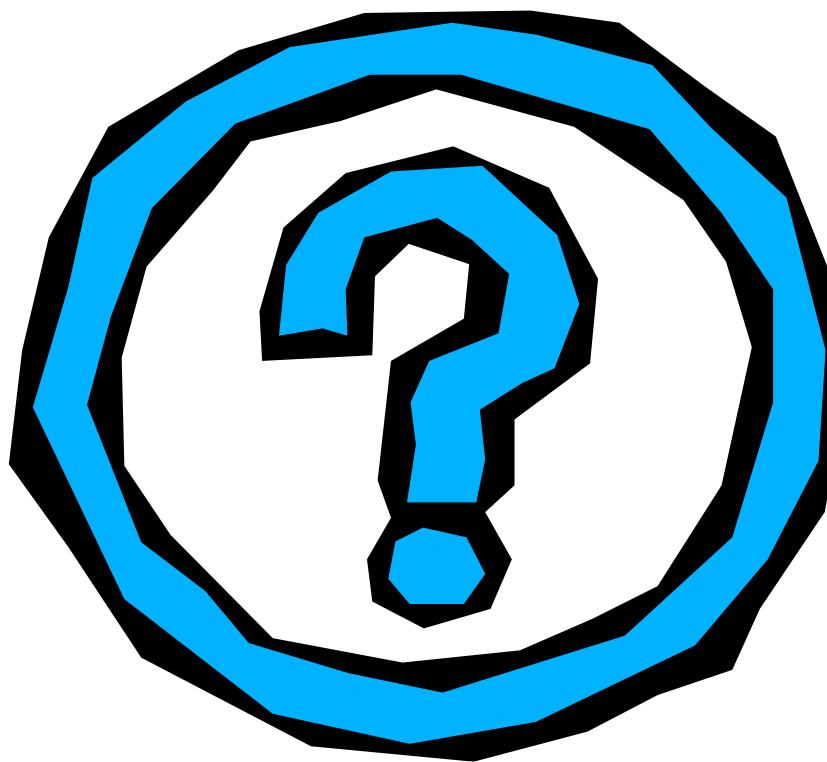
ISMS Overview

ISO27001:2013 Security Domains





www.isea.gov.in





www.isea.gov.in

Thank You

