INFORMATION SECURITY

INFORMATION SECURITY

ISO 27001 security

AGENDA

- What is Information?
- What is Information Security?
- What is RISK?
- An Introduction to ISO for information technology
- User Responsibilities

ISO 27001 security

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

ISO 27001 security

INFORMATION LIFECYCLE

ISO 27001 security

Information can be

- Created
- Stored
- Destroyed
- Processed
- Transmitted
- Used – (For proper & improper purposes)
- Corrupted
- Lost
- Stolen

INFORMATION

TYPES

- Printed or written on paper
- Stored electronically
- Transmitted by post or using electronics means
- Shown on corporate videos
- Displayed / published on web
- Verbal – spoken in conversations

'…Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected'
(BS ISO 27002:2005)

ISO 27001 security

INFORMATION SECURITY

ISO 27001 security

What Is Information Security

- **The quality or state of being secure to be free from danger**
- **Security is achieved using several strategies**
- **Security is achieved using several strategies simultaneously or used in combination with one another**
- **Security is recognized as essential to protect vital processes and the systems that provide those processes**
- **Security is not something you buy, it is something you do**

INFORMATION SECURITY

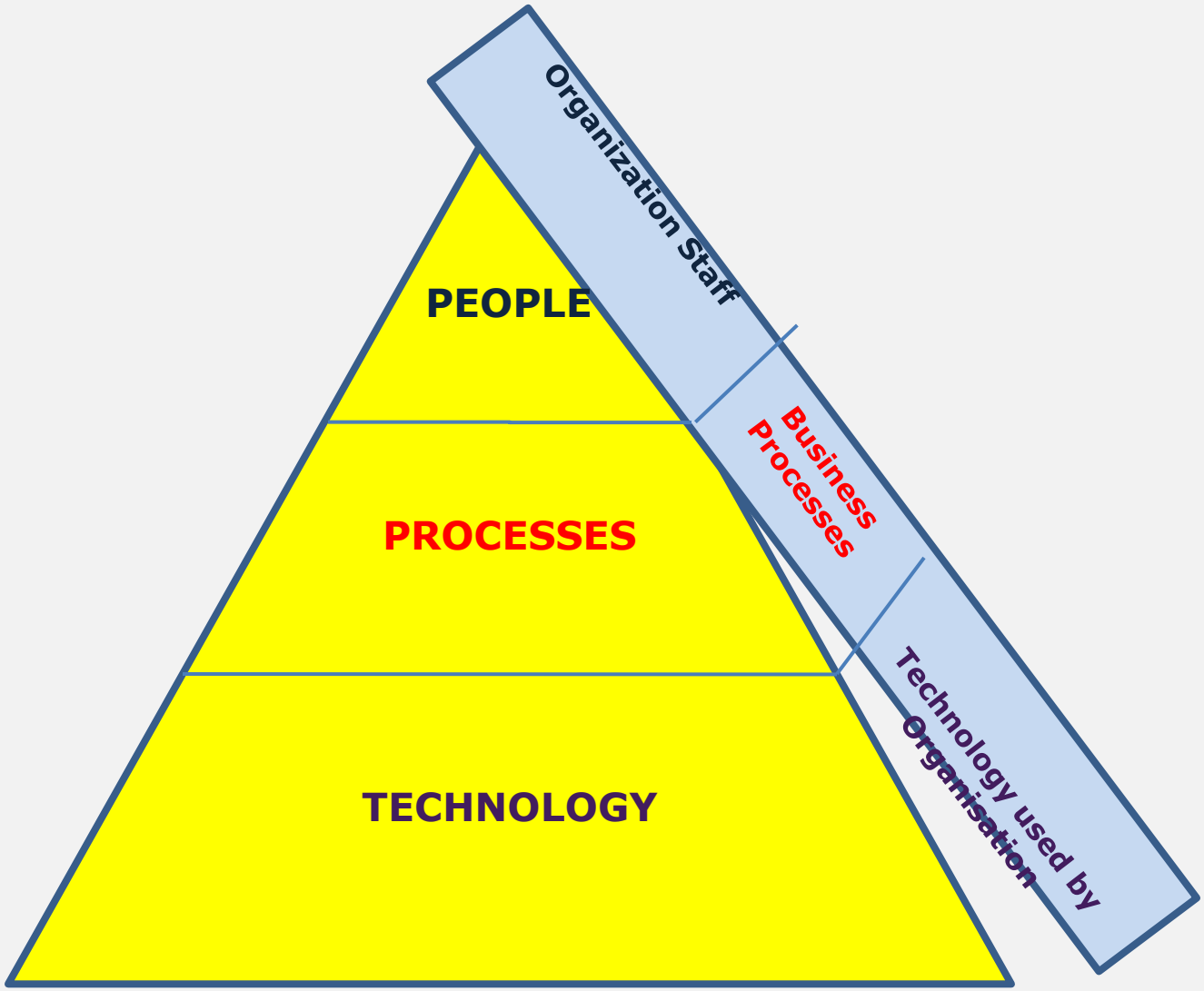
ISO 27001 security

What Is Information Security

- **The architecture where an integrated combination of appliances, systems and solutions, software, alarms, and vulnerability scans working together**
- **Monitored 24x7**
- **Having People, Processes, Technology, policies, procedures,**
- **Security is for PPT and not only for appliances or devices**

INFOSEC

COMPONENTS



ISO 27001 security

PEOPLE

People "Who we are"

- **People who use or interact with the Information include:**
  - **Share Holders / Owners**
  - **Management**
  - **Employees**
  - **Business Partners**
  - **Service providers**
  - **Contractors**
  - **Customers / Clients**
  - **Regulators etc…**

ISO 27001 security

PROCESS

ISO 27001 security

Process “what we do”

The processes refer to "work practices" or workflow. Processes are the repeatable steps to accomplish business objectives. Typical process in our IT Infrastructure could include:

- **Helpdesk / Service management**
- **Incident Reporting and Management**
- **Change Requests process**
- **Request fulfillment**
- **Access management**
- **Identity management**
- **Service Level / Third-party Services Management**
- **IT procurement process etc…**

Technology “what we use to improve what we do”

TECHNOLOGY

ISO 27001 security

Network Infrastructure:

- **Cabling, Data/Voice Networks and equipment**
- **Telecommunications services (PABX), including VoIP services , ISDN , Video Conferencing**
- **Server computers and associated storage devices**
- **Operating software for server computers**
- **Communications equipment and related hardware.**
- **Intranet and Internet connections**
- **VPNs and Virtual environments**
- **Remote access services**
- **Wireless connectivity**

Technology "what we use to improve what we do"

TECHNOLOGY

Application software:

- **Finance and assets systems, including Accounting packages, Inventory management, HR systems, Assessment and reporting systems**
- **Software as a service (Sass) - instead of software as a packaged or custom-made product. Etc..**

Physical Security components:

- **CCTV Cameras**
- **Clock in systems / Biometrics**
- **Environmental management Systems: Humidity Control, Ventilation , Air Conditioning, Fire Control systems**
- **Electricity / Power backup**

Access devices:

- **Desktop computers**
- **Laptops, ultra-mobile laptops and PDAs**
- **Thin client computing.**
- **Digital cameras, Printers, Scanners, Photocopier etc.**

ISO 27001 security

INFORMATION SECURITY

INFORMATION SECURITY

1. Protects information from a range of threats
2. Ensures business continuity
3. Minimizes financial loss
4. Optimizes return on investments
5. Increases business opportunities

Business survival depends on information security.

INFORMATION ATTRIBUTES

ISO 27001 security

ISO 27002:2005 defines Information Security as the preservation of:

- **Confidentiality**

Ensuring that information is accessible only to those authorized to have access

- **Integrity**

Safeguarding the accuracy and completeness of information and processing methods

- **Availability**

Ensuring that authorized users have access to information and associated assets when required

Security breaches leads to…

- **Reputation loss**
- **Financial loss**
- **Intellectual property loss**
- **Legislative Breaches leading to legal actions (Cyber Law)**
- **Loss of customer confidence**
- **Business interruption costs**

LOSS OF GOODWILL

ISO 27001 security

INFO SECURITY SURVEY

- Information Security is "Organizational Problem" rather than "IT Problem"
- More than 70% of Threats are Internal
- More than 60% culprits are First Time fraudsters
- Biggest Risk : People
- Biggest Asset : People
- Social Engineering is major threat
- More than 2/3rd express their inability to determine **"Whether my systems are currently compromised?"**

ISO 27001 security

WHAT IS RISK

What is Risk?

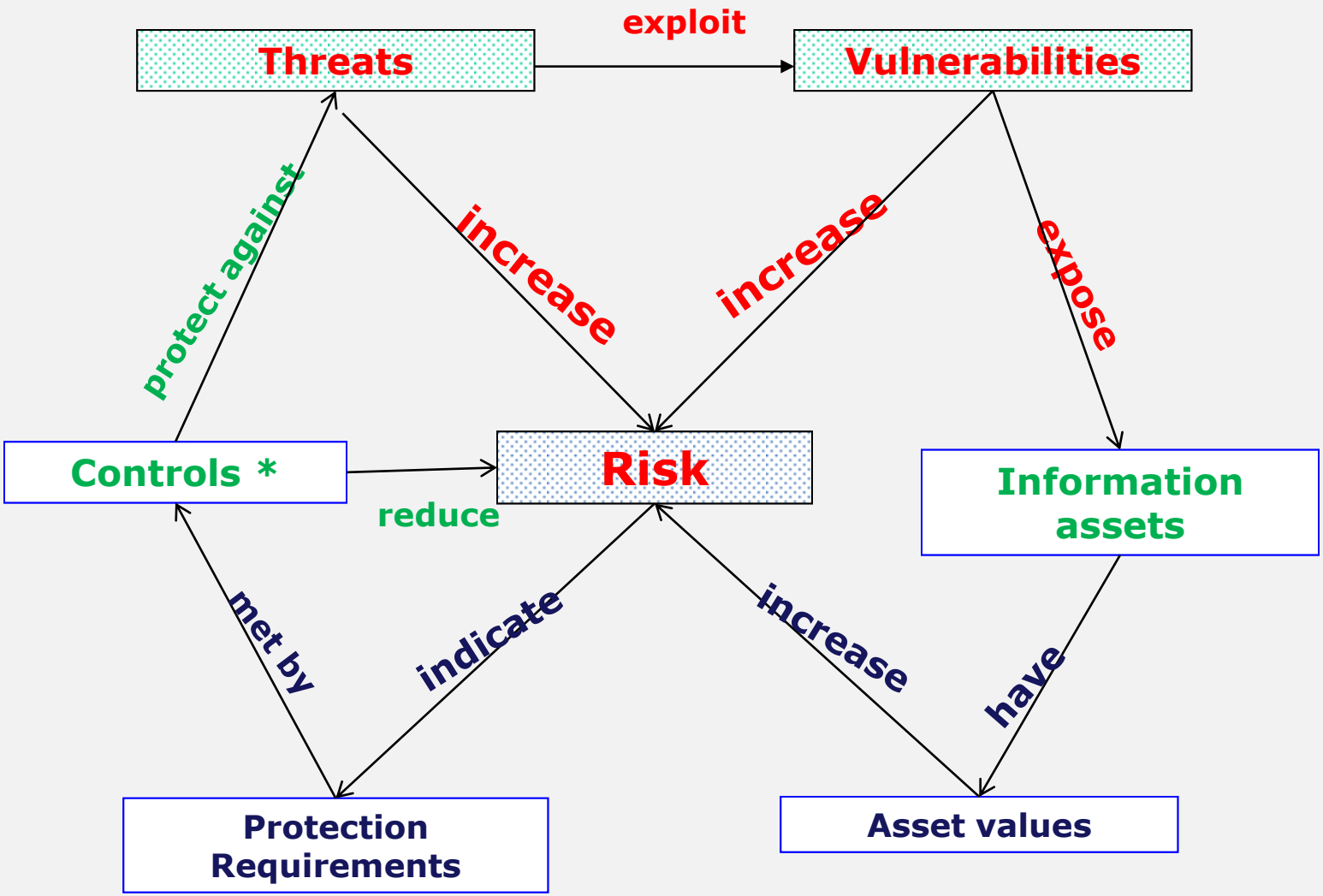
Risk: A possibility that a threat exploits a vulnerability in an asset and causes damage or loss to the asset.

Threat: Something that can potentially cause damage to the organisation, IT Systems or network.

Vulnerability: A weakness in the organization, IT Systems, or network that can be exploited by a threat.

ISO 27001 security

Relationship between Risk, Threats, and Vulnerabilities



* Controls: A practice, procedure or mechanism that reduces risk

ISO 27001 security

THREAT IDENTIFICATION

ISO 27001 security

Threat Identification

Elements of threats

- Agent : The catalyst that performs the threat.
  - Human
  - Machine
  - Nature

THREAT IDENTIFICATION

ISO 27001 security

Threat Identification

Elements of threats

- Motive : Something that causes the agent to act.
  - Accidental
  - Intentional
  - Only motivating factor that can be both accidental and intentional is human

THREAT IDENTIFICATION

ISO 27001 security

Threat Identification

Elements of threats

Results : The outcome of the applied threat. The results normally lead to the loss of CIA

- Confidentiality
- Integrity
- Availability

THREATS

Threats

- Employees
- External Parties
- Low awareness of security issues
- Growth in networking and distributed computing
- Growth in complexity and effectiveness of hacking tools and viruses
- Natural Disasters eg. fire, flood, earthquake

ISO 27001 security

Threat Sources

Source	Motivation	Threat
External Hackers	Challenge Ego Game Playing	System hacking Social engineering Dumpster diving
Internal Hackers	Deadline Financial problems Disenchantment	Backdoors Fraud Poor documentation
Terrorist	Revenge Political	System attacks Social engineering Letter bombs Viruses Denial of service
Poorly trained employees	Unintentional errors Programming errors Data entry errors	Corruption of data Malicious code introduction System bugs Unauthorized access

No	Categories of Threat	Example
1	Human Errors or failures	Accidents, Employee mistakes
2	Compromise to Intellectual Property	Piracy, Copyright infringements
3	Deliberate Acts or espionage or trespass	Unauthorized Access and/or data collection
4	Deliberate Acts of Information extortion	Blackmail of information exposure / disclosure
5	Deliberate Acts of sabotage / vandalism	Destruction of systems / information
6	Deliberate Acts of theft	Illegal confiscation of equipment or information
7	Deliberate software attacks	Viruses, worms, macros Denial of service
8	Deviations in quality of service from service provider	Power and WAN issues
9	Forces of nature	Fire, flood, earthquake, lightening
10	Technical hardware failures or errors	Equipment failures / errors
11	Technical software failures or errors	Bugs, code problems, unknown loopholes
12	Technological Obsolesce	Antiquated or outdated technologies

RISKS & THREATS

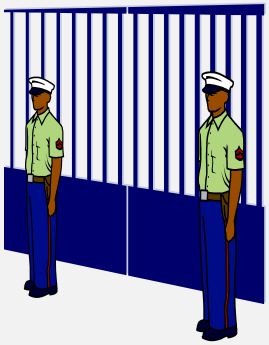
High User Knowledge of IT Systems

Theft, Sabotage, Misuse

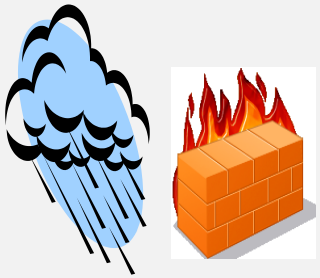
Virus Attacks

Systems & Network Failure

Lack Of Documentation



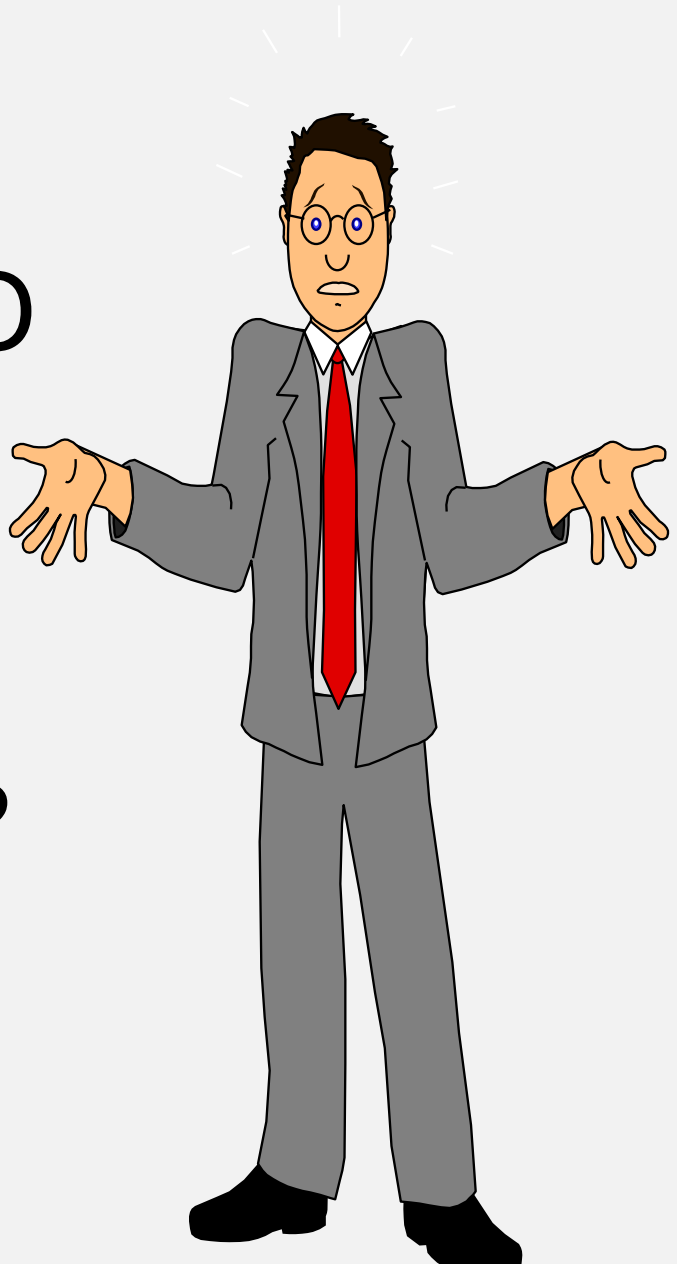
Lapse in Physical Security



Natural Calamities & Fire

ISO 27001 security

SO HOW DO WE OVERCOME THESE PROBLEMS?



ISO 27001 security

History

Early 1990

- DTI (UK) established a working group
- Information Security Management Code of Practice produced as BSI-DISC publication

1995

- BS 7799 published as UK Standard

1999

- BS 7799 - 1:1999 second revision published

2000

- BS 7799 - 1 accepted by ISO as ISO - 17799 published
- BS 7799-2:2002 published

History

- **ISO 27001:2005**

  Information technology — Security techniques — Information security management systems — Requirements

- **ISO 27002:2005**

  Information technology — Security techniques — Code of practice for information security management

ISO 27001

ISO 27001: This International Standard covers all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations). This

International Standard specifies the requirements for establishing; implementing, operating, monitoring, reviewing, maintaining and improving documented ISMS within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.

The ISMS is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties

ISO 27001

Features

FEATURES

Features of ISO 27001

- **Plan, Do, Check, Act (PDCA) Process Model**
- **Process Based Approach**
- **Stress on Continual Process Improvements**
- **Scope covers Information Security not only IT Security**
- **Covers People, Process and Technology**
- **5600 plus organisations worldwide have been certified**
- **11 Domains, 39 Control objectives, 133 controls**

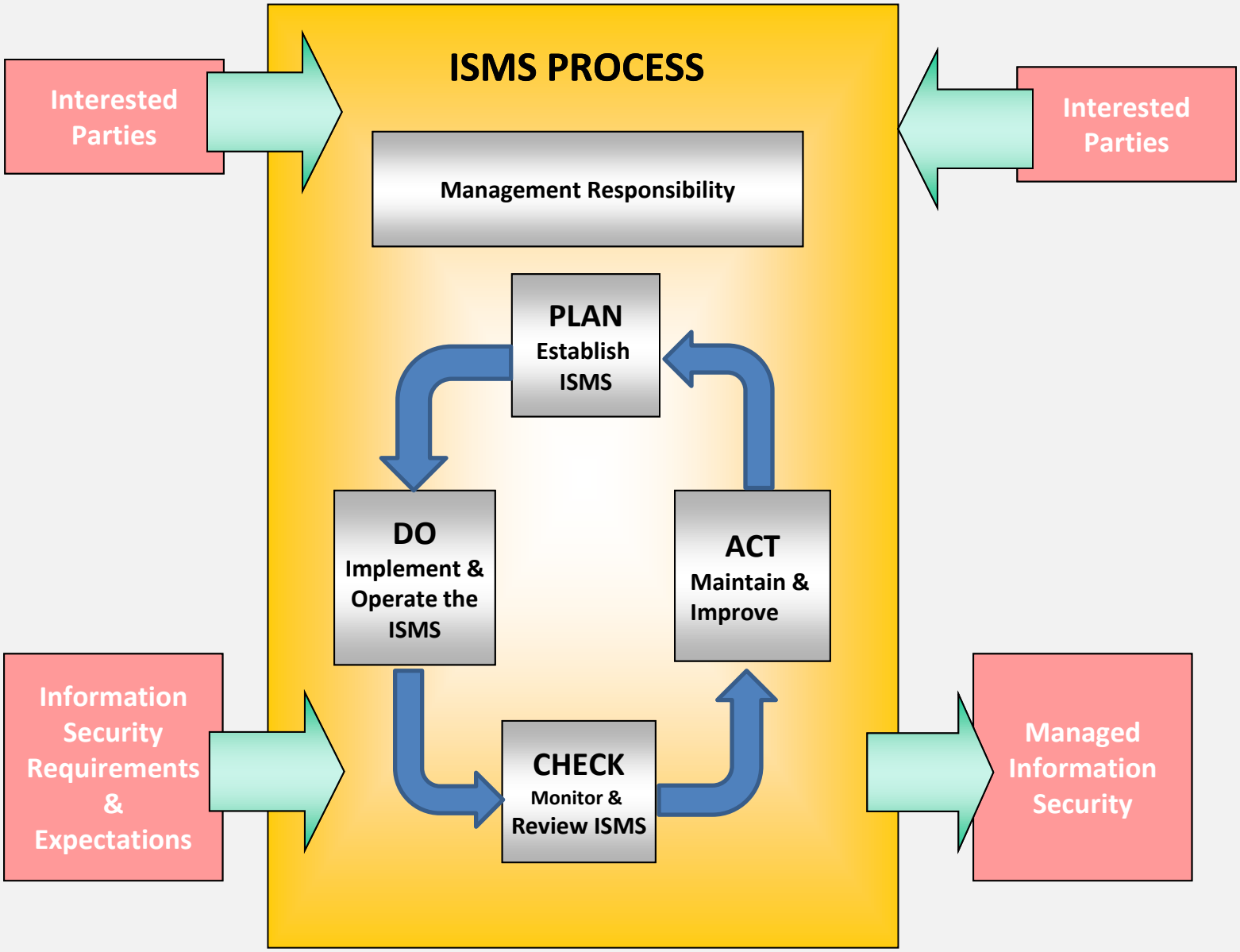
ISO 27001 security

P D C A

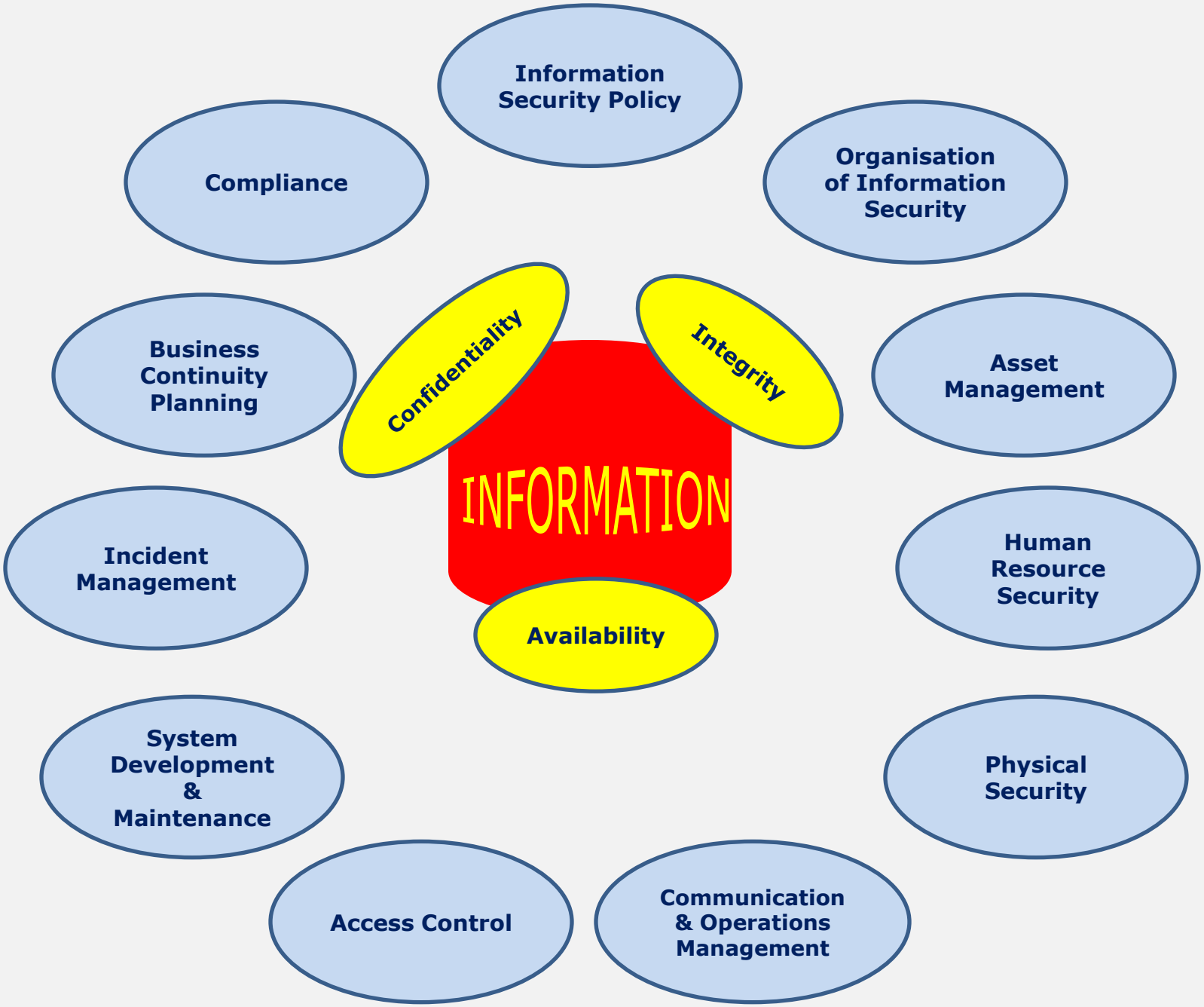
P R O C E S S

ISO 27001 security

PDCA Process



CONTROL CLAUSES



ISO 27001 security

CONTROL CLAUSES

- **Information Security Policy** - To provide management direction and support for Information security.
- **Organisation Of Information Security** - Management framework for implementation
- **Asset Management** - To ensure the security of valuable organisational IT and its related assets
- **Human Resources Security** - To reduce the risks of human error, theft, fraud or misuse of facilities.
- **Physical & Environmental Security** -To prevent unauthorised access, theft, compromise , damage, information and information processing facilities.

ISO 27001 security

CONTROL CLAUSES

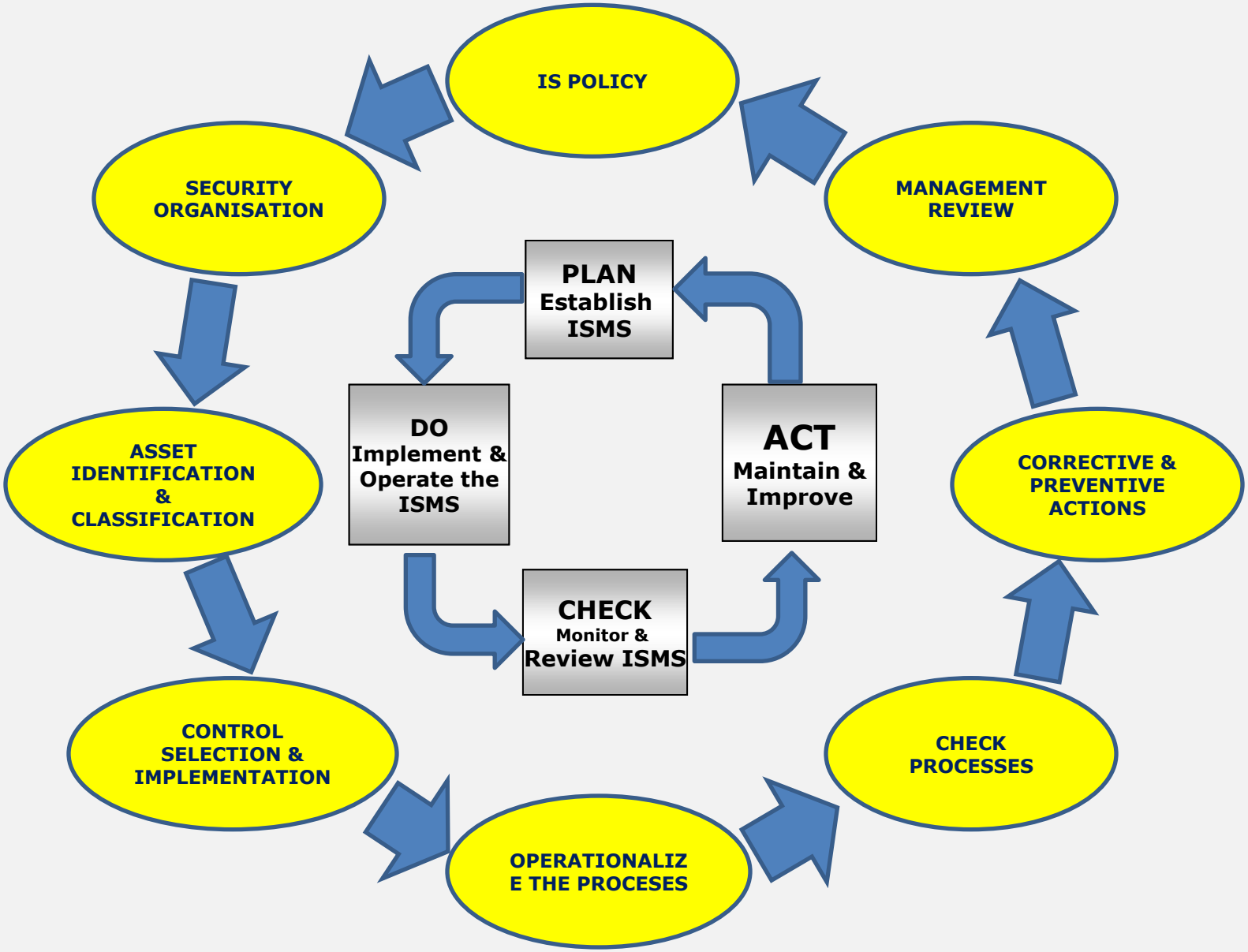
- **Communications & Operations Management** - To ensure the correct and secure operation of information processing facilities.
- **Access Control** - To control access to information and information processing facilities on 'need to know' and 'need to do' basis.
- **Information Systems Acquisition, Development & Maintenance** - To ensure security built into information systems
- **Information Security Incident Management -** To ensure information security events and weaknesses associated with information systems are communicated.

ISO 27001 security

- **Business Continuity Management** - To reduce disruption caused by disasters and security failures to an acceptable level.

- **Compliance** - To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.

IMPLEMENTATION PROCESS CYCLE



ISO 27001 security

BENEFITS

- **At the organizational level –** Commitment
- **At the legal level –** Compliance
- **At the operating level -** Risk management
- **At the commercial level -** Credibility and confidence
- **At the financial level -** Reduced costs
- **At the human level -** Improved employee awareness

ISO 27001 security

USER RESPONSIBILITIES

WHO IS AT THE CENTRE OF

SECU  RITY

U-R

ISO 27001 security

USER RESPONSIBILITIES

ISO 27001 security

Information Security Policy

IS Policy is approved by Top Management

Policy is released on Intranet at http://xx.xx.xx.xx/ISMS/index.htm

INFO ASSET CLASSIFICATION

ISO 27001 security

Information Asset Classification

CONFIDENTIAL:
If this information is leaked outside Organisation, it will result in major financial and/or image loss. Compromise of this information will result in statutory, legal non- compliance.
Access to this information must be restricted based on the concept of need-to-know. Disclosure requires the information owner's approval. In case information needs to be disclosed to third parties a signed confidentiality agreement is also required. Examples include Customer contracts, rate tables, process documents and new product development plans.

INTERNAL USE ONLY:
If this information is leaked outside Organisation, it will result in Negligible financial loss and/or embarrassment.
Disclosure of this information shall not cause serious harm to Organisation, and access is provided freely to all internal users. Examples include circulars, policies, training materials etc.

PUBLIC:
Non availability will have no effect. If this information is leaked outside Organisation, it will result in no loss.
This information must be explicitly approved by the Corporate Communications Department or Marketing Department in case of marketing related information, as suitable for public dissemination. Examples include marketing brochures, press releases.

INFO ASSET CLASSIFICATION

ISO 27001 security

Confidentiality - Information Asset

Confidentiality of information refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from jeopardizing organization security to the disclosure of private data of employees. Following table provides guideline to determine Confidentiality requirements:

Confidentiality Requirement	Explanation
Low	Non-sensitive information available for public disclosure. The impact of unauthorized disclosure of such information shall not harm Organisation anyway. E.g. Press releases, Company's News letters e.g. Information published on company's website
Medium	Information belonging to the company and not for disclosure to public or external parties. The unauthorized disclosure of information here can cause a limited harm to the organization. e.g. Organization Charts, Internal Telephone Directory.
High	Information which is very sensitive or private, of highest value to the organization and intended to use by named individuals only. The unauthorized disclosure of such information can cause severe harm (e.g. Legal or financial liability, adverse competitive impact, loss of brand name). E.g. Client's pricing information, Merger and Acquisition related information, Marketing strategy

INFO ASSET CLASSIFICATION

ISO 27001 security

Integrity - Information Asset

Integrity refers to the completeness and accuracy of Information. Integrity is lost if unauthorized changes are made to data or IT system by either intentional or accidental acts. If integrity of data is not restored back, continued use of the contaminated data could result in inaccuracy, fraud, or erroneous decisions. Integrity criteria of information can be determined with guideline established in the following Table.

Integrity Requirement	Explanation
Low	There is minimal impact on business if the accuracy and completeness of data is degraded.
Medium	There is significant impact on business if the asset if the accuracy and completeness of data is degraded.
High	The Integrity degradation is unacceptable.

INFO ASSET CLASSIFICATION

ISO 27001 security

Availability - Information Asset

Availability indicates how soon the information is required, in case the same is lost. If critical information is unavailable to its end users, the organization's mission may be affected. Following Table provides guideline to determine availability criteria of information assets.

Availability Requirement	Explanation
Low	There is minimal impact on business if the asset / information is not Available for up to 7 days
Medium	There is significant impact on business if the asset / information is not Available for up to 48 hours
High	The Asset / information is required on 24x7 basis

NON INFO ASSET CLASSIFICATION

ISO 27001 security

Non-information Assets [Physical]

Information is processed with the help of technology. The assets, which are helpful in creating, processing, output generation and storage. Such assets need to be identified and valued for the purpose of their criticality in business process.

Asset valuation of non information / physical Assets like software, Hardware, Services is carried out based on different criteria applicable to the specific group of physical assets involved in organization's business processes.

NON INFO ASSET CLASSIFICATION

ISO 27001 security

Confidentiality - Non-information Asset

Confidentiality factor is to be determined by the services rendered by the particular asset in specific business process and the confidentiality requirement of the information / data processed or stored by the asset. This table provides a guideline to identify the Confidentiality requirements and its link to Classification label.

Confidentiality Requirement	Explanation
Low	Information processed / stored / carried or services rendered by the asset in the business process have confidentiality requirements as LOW.
Medium	Information processed / stored / carried or services rendered by the asset in the business process have confidentiality requirements as Medium.
High	Information processed / stored / carried or services rendered by the asset in the business process have confidentiality requirements as HIGH.

NON INFO ASSET CLASSIFICATION

ISO 27001 security

Integrity - Non Information Asset

Integrity factor is to be determined by the reliability and dependability of the particular asset in specific business process and the Integrity requirement of the information / data processed or stored by the asset. This table provides a guideline to identify the Integrity requirements and its link to Classification label.

Integrity Requirement	Explanation
Low	Dependency and reliability of the services rendered by the particular asset in a business process is LOW. Information processed / stored / carried or services rendered by the asset in the business process have Integrity requirements as LOW.
Medium	Dependency and reliability of the services rendered by the particular asset in a business process is Medium. Information processed / stored / carried or services rendered by the asset in the business process have Integrity requirements as Medium.
High	Dependency and reliability of the services rendered by the particular asset in a business process is HIGH. Information processed / stored / carried or services rendered by the asset in the business process have Integrity requirements as High.

NON INFO ASSET CLASSIFICATION

Availability - Non-information Asset

Availability factor is to be determined on the basis of impact of non availability of the asset on the business process. This table provides a guideline to identify the Availability requirements and its link to Classification label.

Integrity Requirement	Explanation
Low	Impact of non availability of an asset in a business process is LOW. Information processed / stored / carried or services rendered by the asset in the business process have Availability requirements as LOW.
Medium	Impact of non availability of an asset in a business process is Medium. Information processed / stored / carried or services rendered by the asset in the business process have Availability requirements as MEDIUM.
High	Impact of non availability of an asset in a business process is HIGH. Information processed / stored / carried or services rendered by the asset in the business process have Availability requirements as HIGH.

ISO 27001 security

PEOPLE ASSET CLASSIFICATION

ISO 27001 security

People Assets

Information is accessed or handled by the people from within the organisation as well as the people related to organisation for business requirements.

It becomes necessary to identify such people from within the organisation as well as outside the organisation who handle the organization's information assets.

The analysis such people, who has access rights to the assets of the organisation, is to be done by Business Process Owner i.e. process / function head.

The people assets shall include roles handled by

a. Employees
b. Contract Employees
c. Contractors & his employees

PEOPLE ASSET CLASSIFICATION

ISO 27001 security

Confidentiality - People Assets

Confidentiality Requirement	Explanation
Low	The role or third party identified has access limited to information assets classified as 'Public'. Security breach by individual/s whom the role is assigned would insignificantly affect the business operations.
Medium	The role or third party identified has access limited to information assets classified as 'Internal' and 'Public'. Security breach by individual/s whom the role is assigned would moderately affect the business operations.
High	The role employee or third party identified has access to all types of information assets including information assets classified as 'Confidential' Or IT Assets classified as 'Critical'. Security breach by individual/s to whom the role is assigned would severely affect the business operations.

PEOPLE ASSET CLASSIFICATION

ISO 27001 security

Integrity – People Assets

Integrity Requirement	Explanation
Low	The role or third party identified has limited privilege to change information assets classified as 'Internal' or 'Public' and the his work is supervised. Security breach by individual/s to whom the role is assigned would insignificantly affect the business operations.
Medium	The role or third party identified has privilege to change information assets classified as 'Internal', and 'Public' Security breach by individual/s whom the role is assigned would moderately affect the business operations.
High	The role or third party identified has privilege to change information assets classified as 'Confidential' Or Change the configuration of IT assets classified as 'Critical' Security breach by individual/s to whom the role is assigned would severely affect the business operations.

PEOPLE ASSET CLASSIFICATION

Availability – People Assets

Availability Requirement	Explanation
Low	Unavailability of the individual/s whom the role is assigned would have insignificant affect the business operations.
Medium	Unavailability of the individual/s whom the role is assigned would moderately affect the business operations.
High	Unavailability of the individual/s whom the role is assigned would severely affect the business operations.

ISO 27001 security

USER RESPONSIBILITIES

Access Control - Physical

- Follow Security Procedures
- Wear Identity Cards and Badges
- Ask unauthorized visitor his credentials
- Attend visitors in Reception and Conference Room only

- **Bring visitors in operations area without prior permission**
- **Bring hazardous and combustible material in secure area**
- **Practice "Piggybacking"**
- **Bring and use pen drives, zip drives, ipods, other storage devices unless and otherwise authorized to do so**

ISO 27001 security

USER RESPONSIBILITIES

ISO 27001 security

Password Guidelines

- Always use at least 8 character password with combination of alphabets, numbers and special characters (*, %, @, #, $, ^)
- Use passwords that can be easily remembered by you
- Change password regularly as per policy
- Use password that is significantly different from earlier passwords

- **Use passwords which reveals your personal information or words found in dictionary**
- **Write down or Store passwords**
- **Share passwords over phone or Email**
- **Use passwords which do not match above complexity criteria**

USER RESPONSIBILITIES

Internet Usage

- Use internet services for business purposes only

- Do not access internet through dial-up connectivity
- Do not use internet for viewing, storing or transmitting obscene or pornographic material
- Do not use internet for accessing auction sites
- Do not use internet for hacking other computer systems
- Do not use internet to download / upload commercial software / copyrighted material

Technology Department is continuously monitoring Internet Usage. Any illegal use of internet and other assets shall call for Disciplinary Action.

ISO 27001 security

USER RESPONSIBILITIES

E-mail Usage

✓Use official mail for business purposes only
✓Follow the mail storage guidelines to avoid blocking of E-mails
✓ If you come across any junk / spam mail, do the following
  a) Remove the mail.
  b) Inform the security help desk
  c) Inform the same to server administrator
  d) Inform the sender that such mails are undesired

- Do not use official ID for any personal subscription purpose
- Do not send unsolicited mails of any type like chain letters or E-mail Hoax
- Do not send mails to client unless you are authorized to do so
- Do not post non-business related information to large number of users
- Do not open the mail or attachment which is suspected to be virus or received from an unidentified sender

ISO 27001 security

USER RESPONSIBILITIES

Security Incidents

Report Security Incidents (IT and Non-IT) to Helpdesk through

- E-mail to info.sec@organisation.com
- Telephone : xxxx-xxxx-xxxx
- Anonymous Reporting through Drop boxes

e.g.:

IT Incidents: Mail Spamming, Virus attack, Hacking, etc.

Non-IT Incidents: Unsupervised visitor movement, Information leakage, Bringing unauthorized Media

- Do not discuss security incidents with any one outside organisation
- Do not attempt to interfere with, obstruct or prevent anyone from reporting incidents

ISO 27001 security

USER RESPONSIBILITIES

- ✓ Ensure your Desktops are having latest antivirus updates
- ✓ Ensure your system is locked when you are away
- ✓ Always store laptops/ media in a lockable place
- ✓ Be alert while working on laptops during travel
- ✓ Ensure sensitive business information is under lock and key when unattended
- ✓ Ensure back-up of sensitive and critical information assets
- ✓ Understand Compliance Issues such as
  - Cyber Law
  - IPR, Copyrights, NDA
  - Contractual Obligations with customer
- ✓ Verify credentials, if the message is received from unknown sender
- ✓ Always switch off your computer before leaving for the day
- ✓ **Keep your self updated on information security aspects**

ISO 27001 security

Human Wall Is Always Better Than A Firewall

. . . LET US BUILD A HUMAN WALL ALONG WITH FIREWALL

ISO 27001 security