Xebia

Software Development Done Right

Welcome To
The User Awareness Training Of
ISO/IEC 27001:2013
(Information Security Management Systems)

Xebia

'Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected'

-ISO 27001:2013

Information can be:

- Created
- Stored
- Destroyed
- Processed
- Transmitted
- Used
- Corrupted
- Lost
- Stolen
- Printed or written on paper
- Stored electronically
- Displayed / published on web

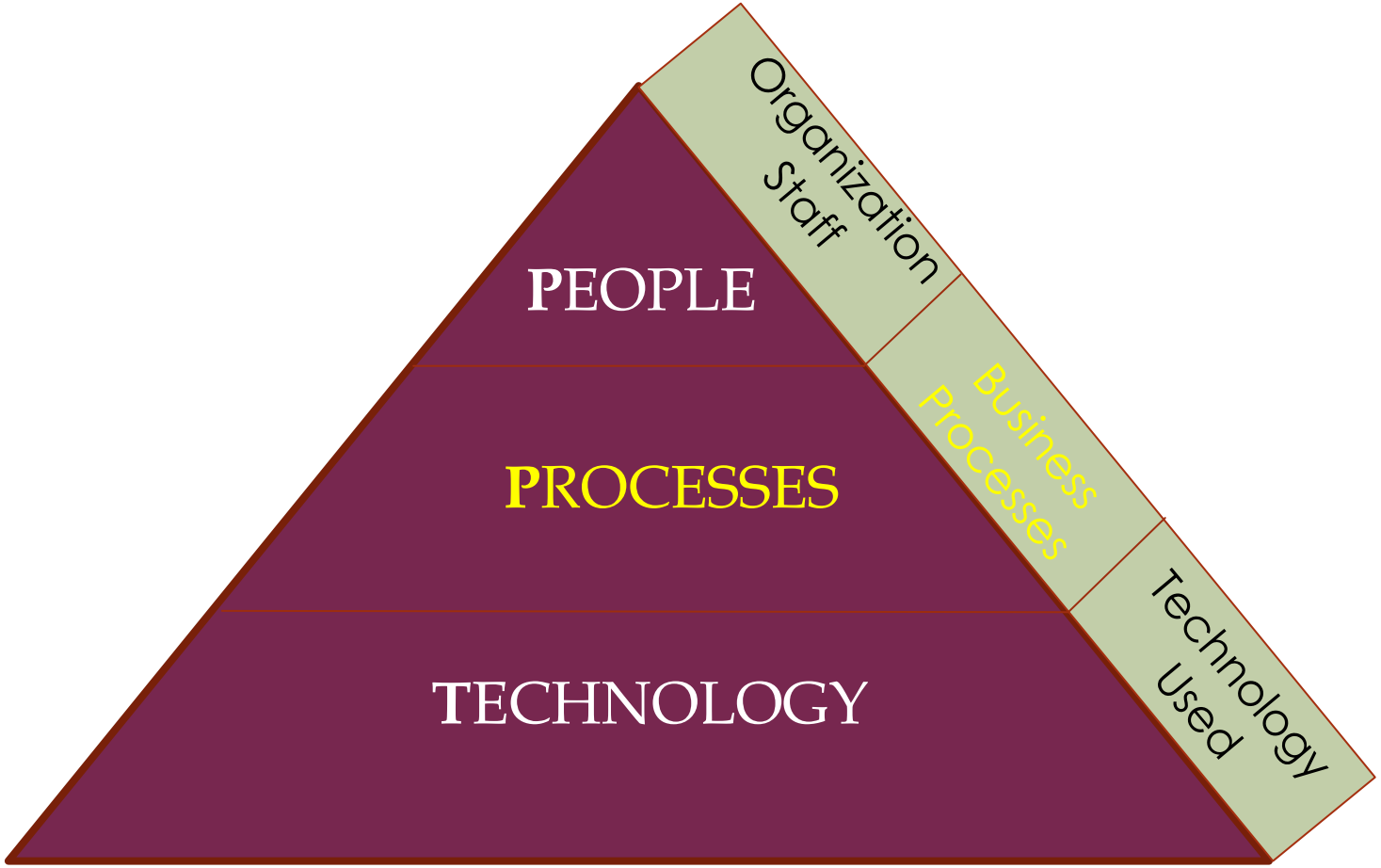
‘…Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected’

-ISO 27001:2013

What is Information Security?

- The quality or state of being secure to be free from danger.
- 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.

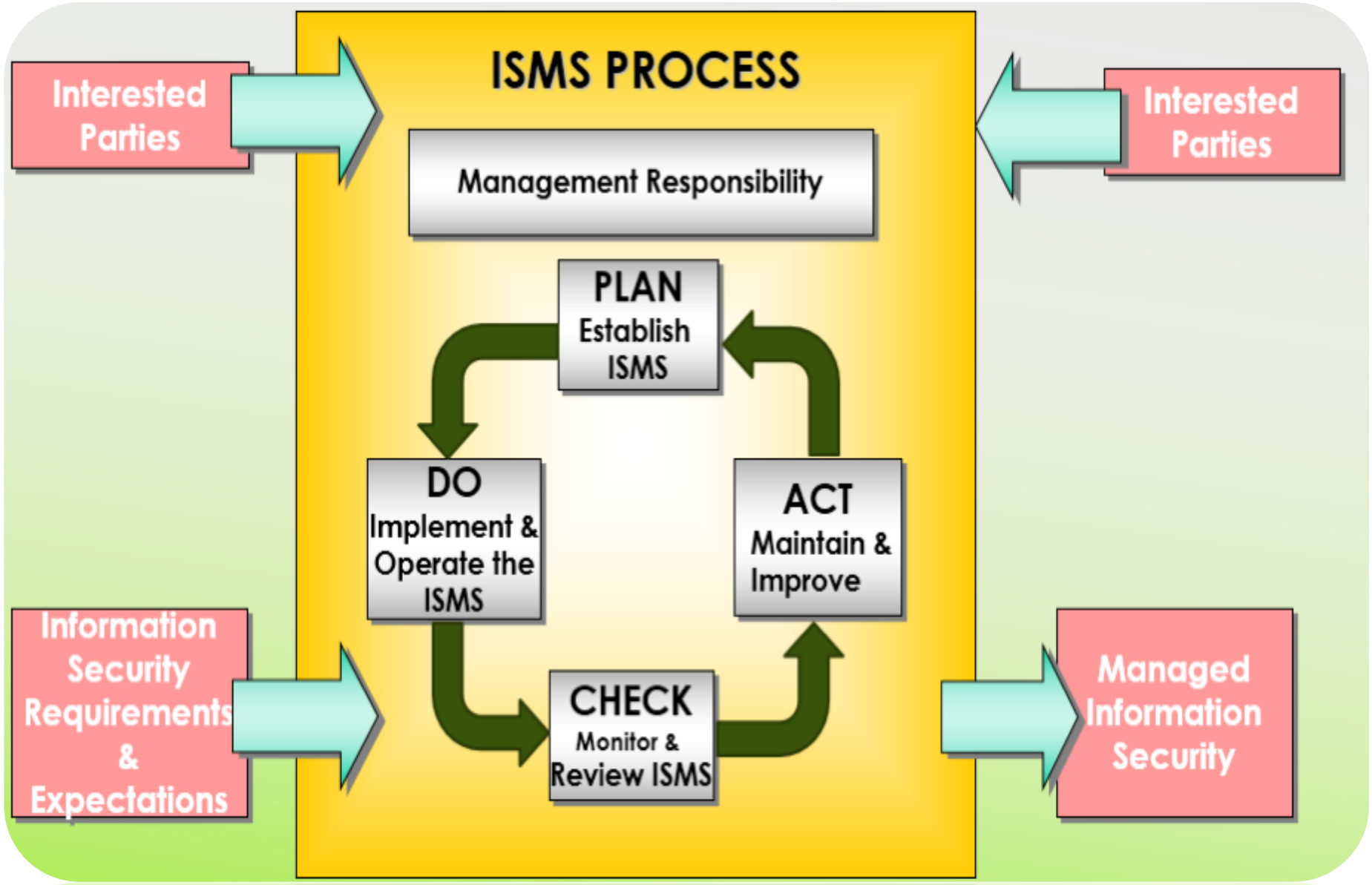
- The architecture where an integrated combination of appliances, systems and solutions, software, alarms, and vulnerability scans working together.
- Monitored 24x7
- Having People, Processes, Technology, policies, procedures.
- Security is for PPT and not only for appliances or devices.


PEOPLE
PROCESSES
TECHNOLOGY
Organization
Staff
Business
Processes
Technology
Used

IMPORTANCE OF INFORMATION SECURITY

- Protects information from a range of threats
- Ensures business continuity
- Minimizes financial loss
- Optimizes return on investments
- Increases business opportunities

Business survival depends on information security.


ISMS PROCESS
Interested Parties
Interested Parties
Management Responsibility
PLAN
Establish ISMS
DO
Implement & Operate the ISMS
ACT
Maintain & Improve
CHECK
Monitor & Review ISMS
Information Security Requirements & Expectations
Managed Information Security

ISO 27001:2013 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

Xebia

Confidentiality

- 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:

RATING	DEFINITION	EXAMPLES
4	These information / assets are restricted to Xebia Leadership team and are intended for business use. Impact of unauthorized disclosure can result in: • Severe disruptions in business operations • Adverse publicity • Significant business loss/ financial loss	1. Financial and other company related information 2. Employee remuneration /compensation related. 3. Customer provided information requiring confidentiality as per request or classification, etc.
3	These information / assets are permitted to be shared / used within a group of users / team for the project / function. Impact of unauthorized disclosure can result in: • Affecting the functioning of the individual projects /functions. • Adverse impact on relations with customer's business associates. • Adverse effect on employee's Minimal business / financial loss	Memos, Work programs, Schedules, Test results, Status reports, Software code, Project plans and another project related artifacts, TEAMS application and content, Software Requirement Specifications, User mailbox access
2	These information / assets are permitted to be shared / used by all the employees (authorized users) of the company. Unauthorized disclosure outside the company is against policy. Disclosure however, is not expected to seriously impact the company, employees, business partners, customers and /or other stakeholders.	Training material, Policy manuals, ISMS documents and templates, Other policies and resources available on the website and intranet, company policies and schemes, SOP
1	These information / assets have been explicitly approved by management for release in the public domain and may be shared freely with all including outsiders (unauthorized users) without any potential harm.	Sales brochures and pamphlets, press releases

Integrity

- 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:

RATING	DEFINITION
4	Loss of integrity of the information / asset (either partially or completely) could lead to: • Significant Business, Financial and / or Legal Impact • Embarrassment and / or negative publicity to the company • The integrity of the information in this case either cannot be recovered or may be totally or partially recoverable at a significant and material financial cost.
3	Loss of integrity of the information / asset (either partially or completely) would lead to a business impact for a project. The information can be recovered (either partially or completely) with some level of effort and minimal financial cost.
2	Loss of integrity of the information / asset would moderately affect the completeness of the information and low business impact. The information can be recovered with minimal effort.
1	No impact due to loss of integrity of the information / asset.

Availability

- 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 business operations may be affected.
- Following table provides guideline to determine availability criteria of information assets:

RATING	DEFINITION
4	The information / asset is such that: • Accessibility or Unavailability would constitute disruption in work leading to high impact to the business operations and / or financial loss to the company. • a very high cost, effort and will require a lot of time to restore • Required for legal and regulatory compliance E.g.: Mail Server, Contingency Assets, Link Failure, Internet connection etc.
3	The information / asset is such that: • Accessibility or Unavailability would constitute a disruption in work leading to business impact to a part of the company restore
2	The information / asset is such that: • Non-Accessibility or unavailability would constitute a disruption of work leading to impact on the functioning of individual projects / functions • Loss due to unavailability is moderate, provided functions are restored within a certain timeframe • Non-availability of asset may have some impact on Xebia, if prolonged for a long period.
1	The information / asset is such that: • Non-Accessibility or Unavailability would constitute a disruption in work leading to low or no business loss. • Asset can be easily replaced • These assets may be unavailable for an extended period, at little or no cost to the company, and require little or no effort when restored. • Non-availability of asset would have minimal / insignificant impact on Xebia.

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

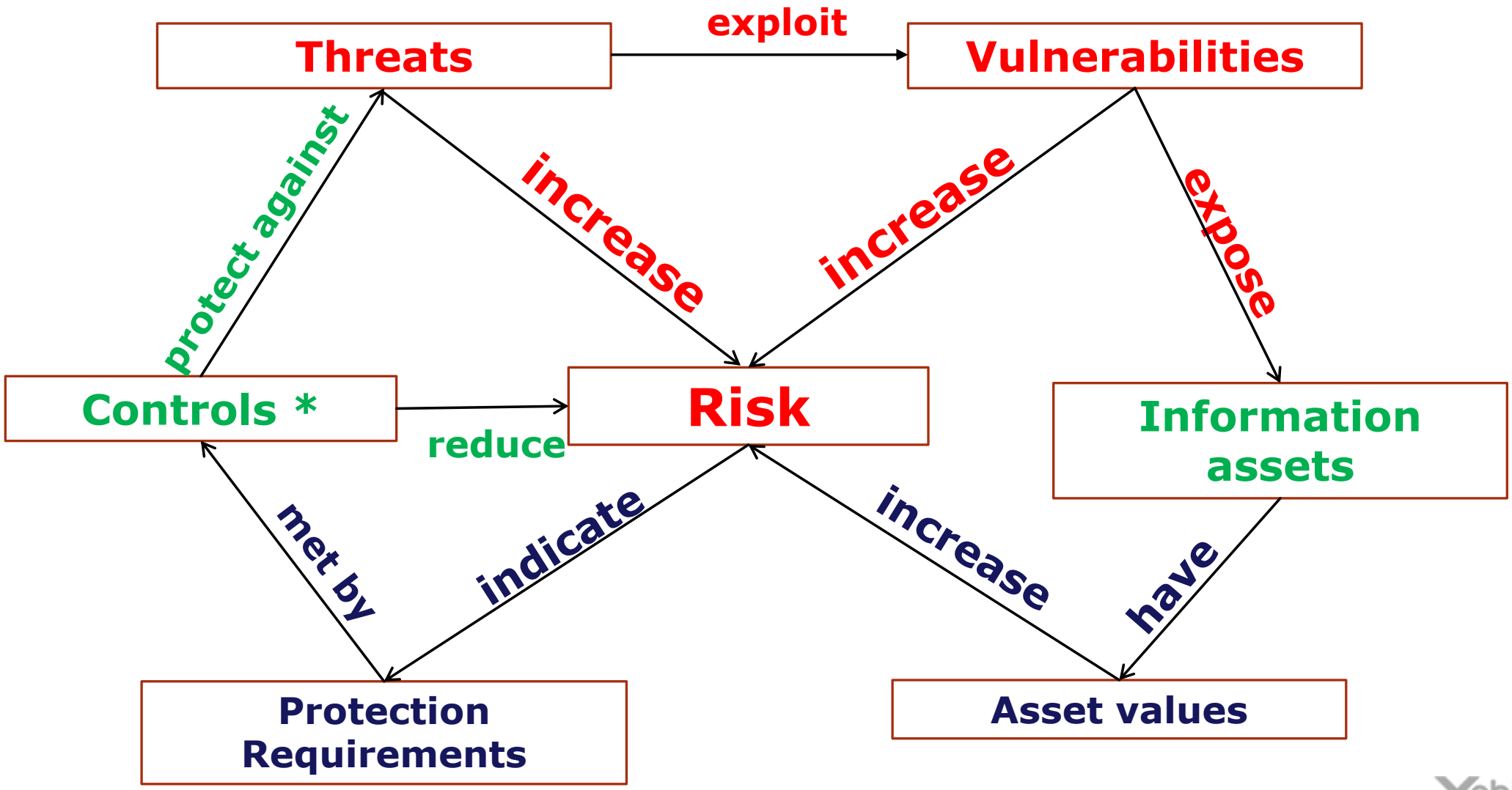
What is Risk, Threat & Vulnerability ?

- 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 organization, IT Systems or network.

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

Relationship between Risk, Threats, and Vulnerabilities



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

Xebia

Threat Identification

- Agent

  The catalyst that performs the threat. E.g. Human, Machine, Nature

- Motive

  Something that causes the agent to act. E.g. Accidental, Intentional

- Results

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

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

S.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 Obsolence	Antiquated or outdated technologies

RISKS & THREATS

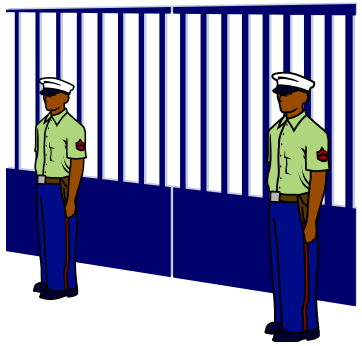
High User Knowledge of IT Systems

Theft, Sabotage, Misuse

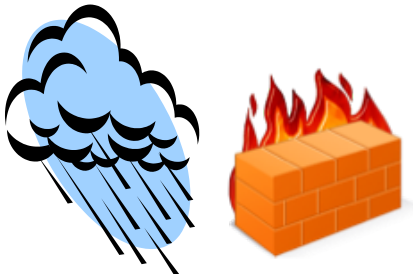
Virus Attacks

Systems & Network Failure

Lack Of Documentation



Lapse in Physical Security



Natural Calamities & Fire

Xebia

ISO 27001

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

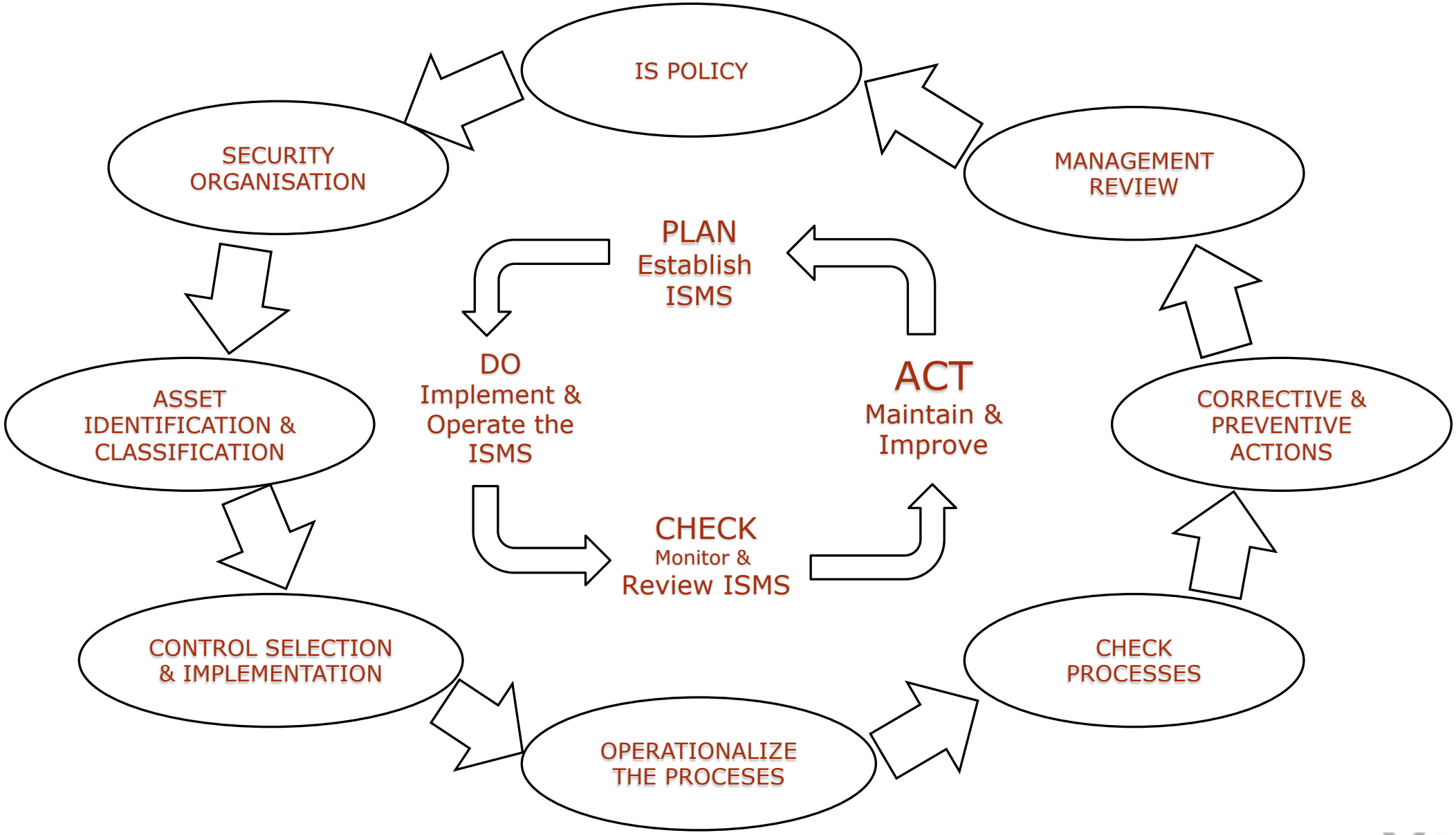
This international standard specifies the requirements for establishing; implementing, operating, monitoring, reviewing, maintaining and improving documented ISMS within the context of the organization’s overall business risks. It specifies requirements for the implementation of security controls customized 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.

Features of ISO 27001:2013

- 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 organizations worldwide have been certified
- 14 Clauses, 35 Control objectives, 114 controls

Xebia

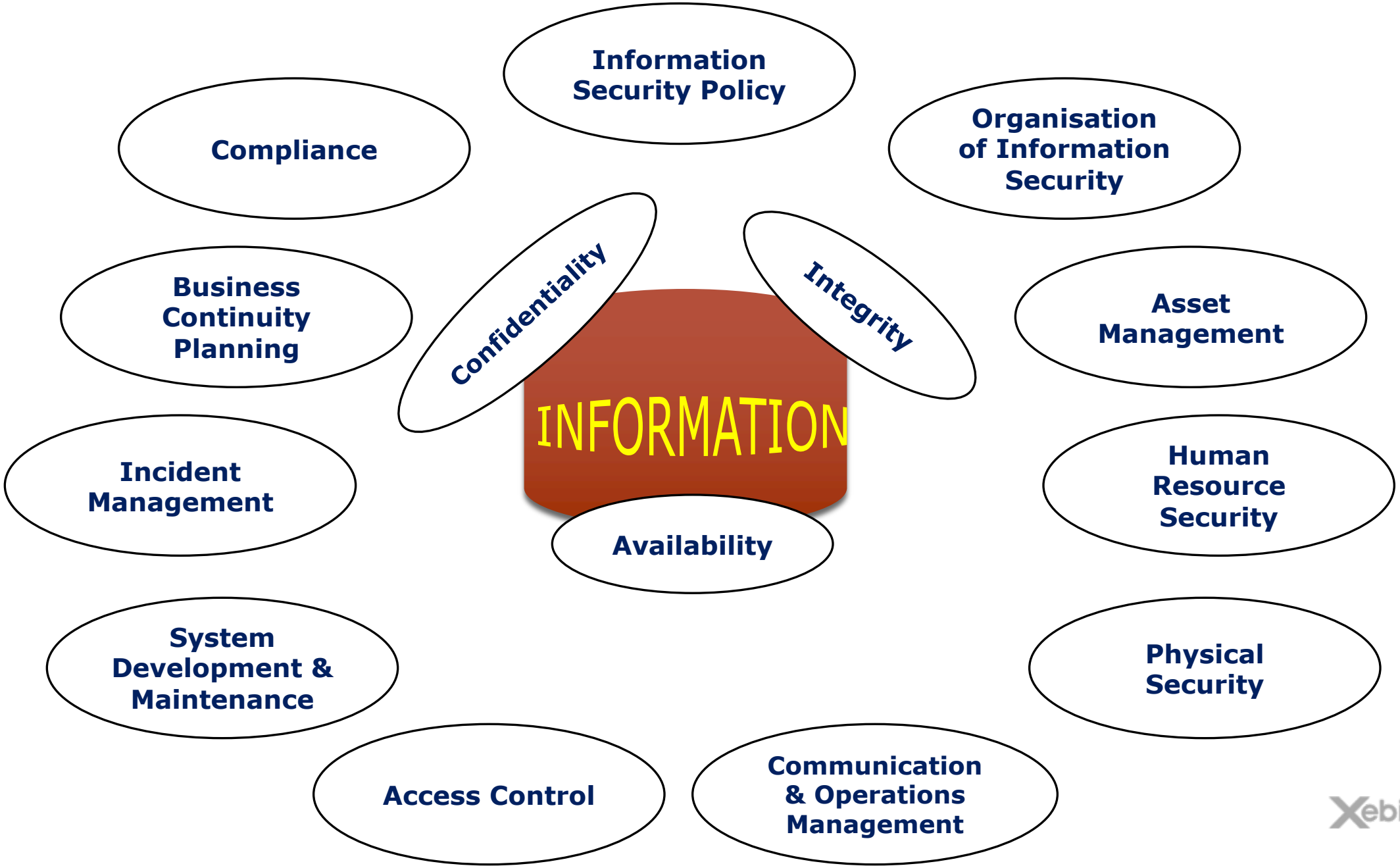

IS POLICY
SECURITY ORGANISATION
MANAGEMENT REVIEW
PLAN
Establish ISMS
DO
Implement & Operate the ISMS
ACT
Maintain & Improve
CHECK
Monitor & Review ISMS
ASSET IDENTIFICATION & CLASSIFICATION
CORRECTIVE & PREVENTIVE ACTIONS
CONTROL SELECTION & IMPLEMENTATION
CHECK PROCESSES
OPERATIONALIZE THE PROCESES

BENEFITS

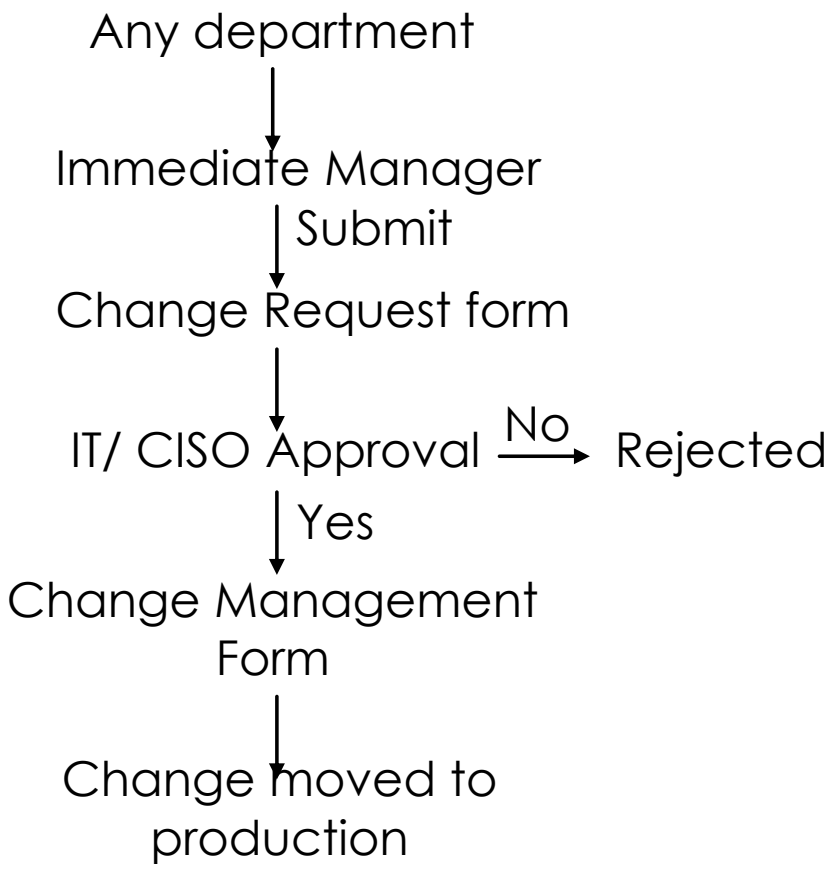
- **At the organizational level** : Commitment
- **At the legal level**: Compliance
- **At the operating level**: Risk management
- **At the commercial level**: Credibility and confidence
- **At the financial level**: Reduced costs
- **At the human level**: Improved employee awareness

Xebia

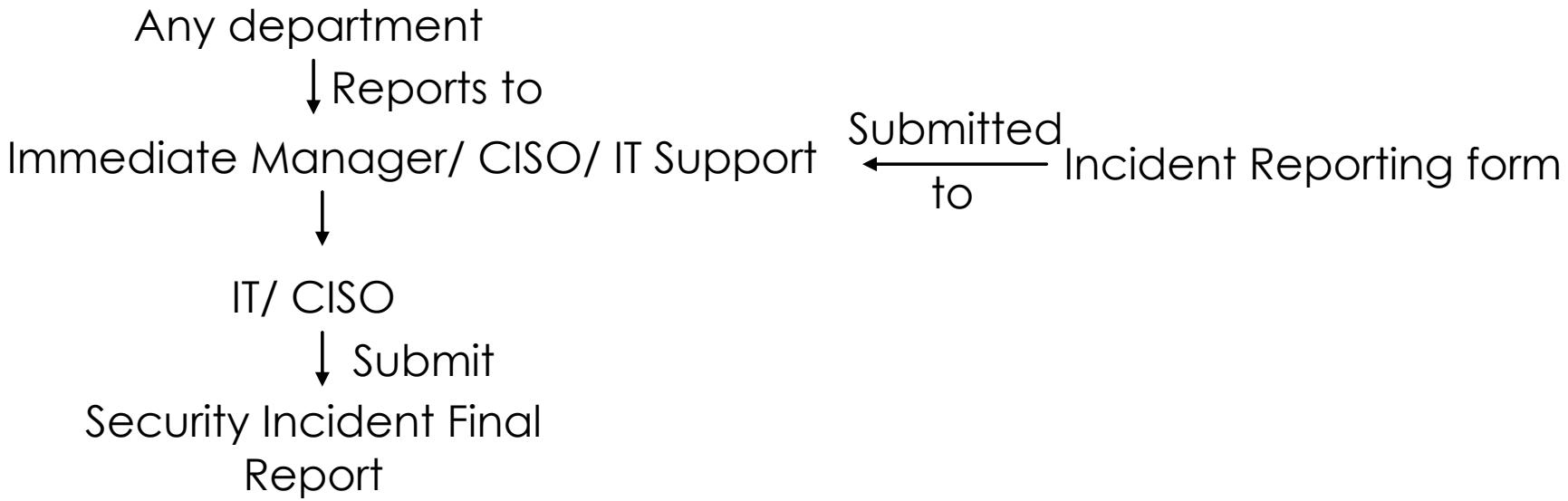
USER RESPONSIBILITIES


Information Security Policy
Compliance
Organisation of Information Security
Business Continuity Planning
Confidentiality
Integrity
Asset Management
INFORMATION
Incident Management
Human Resource Security
Availability
System Development & Maintenance
Physical Security
Access Control
Communication & Operations Management

CHANGE MANAGEMENT



INCIDENT MANAGEMENT



Business Continuity Planning

Torrential Rains

- Step 1: Monitor weather advisories
- Step 2: Notify on-site employees
- Step 3: Call local radio and TV stations to broadcast weather closing information for employees at home
- Step 4: Place closing sign on all affected location offices
- Step 5: Arrange for snow and ice removal

Floods

- Step 1: Monitor flood advisories
- Step 2: Determine flood potential to location
- Step 3: Determine employees at risk
- Step 4: Pre-stage emergency power generating equipment
- Step 5: Assess damage

Cyclones

- Step 1: Listen to Hurricane advisories
- Step 2: Shut down all equipment
- Step 3: Check gas, water and electrical lines for damage
- Step 4: Evacuate area, if flooding is possible
- Step 5: Do not use landline telephones, in the event of severe lightning
- Step 6: Assess damage

Earthquakes

- Step 1: Shut down utilities
- Step 2: Evacuate building if necessary
- Step 3: Account for all personnel
- Step 4: Determine impact of organization disruption
- Step 5: Gather at assembly area
- Step 6: Account for all personnel
- Step 7: Search for missing personnel
- Step 8: Asses damage

Fires

- Step 1: Evacuate personnel on alarm, as necessary
- Step 2: Shut down utilities
- Step 3: Attempt to suppress fire in early stages
- Step 4: Notify fire department.
- Step 5: Gather at assembly area
- Step 6: Account for all personnel
- Step 7: Search for missing personnel
- Step 8: Asses damage

Document Classification And labelling

- **Information can be classified into four categories:**

Classification	Examples
Public	Public press releases Marketing Materials after release External vacancy notices
Internal	Training materials Email and phone directories Customer contact details
Confidential	Financial and budgets Employee personnel data Source Code Non-disclosure agreements with clients\vendors
Restricted	Legal proceedings and investigations Merger and acquisition activities High level strategic planning

Assets usage policy

- Anti-virus must be installed on each laptop
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less, or by logging-off or locking the workstation.
- Report any theft of Xebia's assets to the immediate manager/supervisors.

- Introduction of malicious programs into the network or server
- Revealing your account password to others or allowing use of your account by others.
- Sending Spam via e-mail, text messages, pages, instant messages, voice mail, or other forms of electronic communication.
- Opening e-mail attachments received from unknown senders, which may contain viruses, malware, or Trojan horse code.

Xebia

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” / “Tailgating”
- Bring and use pen drives, zip drives, ipods, other storage devices unless and otherwise authorized to do so

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

Xebia

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

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

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
  - ✓ Remove the mail.
  - ✓ Inform the security help desk
  - ✓ Inform the same to server administrator
  - ✓ 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

Xebia

Security Incidents

Report Security Incidents (IT) to Helpdesk through

- E-mail: itsupportindia@xebia.com
- Telephone extension: 238

Examples:

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 organization
- Do not attempt to interfere with, obstruct or prevent anyone from reporting incidents

Xebia

Other 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, IT Act 2000 etc.
  - 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 yourself updated on information security aspects

THANK YOU

Xebia