Information security

ISO 27001 security

Security awareness seminar

# An introduction to ISO27k

# Agenda

- What is information?
- What is information security?
- What is risk?
- Introduction to the ISO standards
- Managing information security
- Your security 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

*ISO/IEC 27002:2005*

ISO 27001 security

# Information types

Information exists in many forms:

- Printed or written on paper
- Stored electronically
- Transmitted by post or electronic means
- Visual *e.g.* videos, diagrams
- Published on the Web
- Verbal/aural *e.g.* conversations, phone calls
- Intangible *e.g.* knowledge, experience, expertise, ideas

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

*(ISO/IEC 27002:2005)*

ISO 27001 security

# Information can be …

- Created
- Owned (it is an **asset**)
- Stored
- Processed
- Transmitted/communicated
- Used (for proper or improper purposes)
- Modified or corrupted
- Shared or disclosed (whether appropriately or not)
- Destroyed or lost
- Stolen
- Controlled, secured and protected throughout its existence

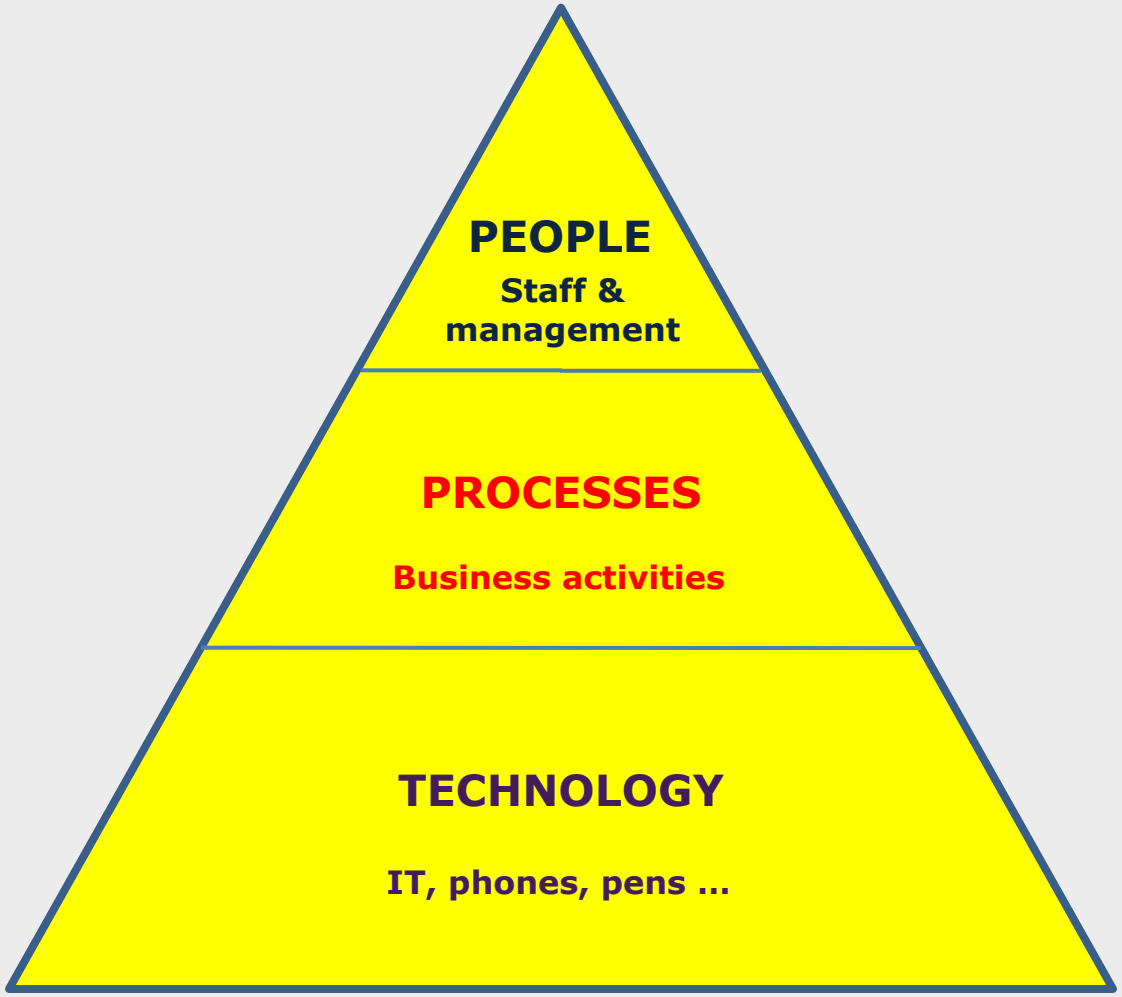
Key term

# What is information security?

- Information security is what keeps valuable information 'free of danger' (protected, safe from harm)
- It is not something you buy, it is something you do
  - It's a *process* not a *product*
- It is achieved using a combination of suitable strategies and approaches:
  - Determining the risks to information and treating them accordingly (proactive risk management)
  - Protecting **CIA** (**C**onfidentiality, **I**ntegrity and **A**vailability)
  - Avoiding, preventing, detecting and recovering from incidents
  - Securing people, processes *and* technology … not just IT!

ISO 27001 security

# Security elements




ISO 27001 security

People

# People

People who use or have an interest in our information security include:

- Shareholders / owners
- Management & staff
- Customers / clients, suppliers & business partners
- Service providers, contractors, consultants & advisors
- Authorities, regulators & judges

Our biggest **threats** arise from people (social engineers, unethical competitors, hackers, fraudsters, careless workers, bugs, flaws …), yet our biggest **asset** is our people (*e.g.* security-aware employees who spot trouble early)

ISO 27001 security

Processes

# Processes

Processes are work practices or workflows, the steps or activities needed to accomplish business objectives.

- Processes are described in procedures.
- Virtually all business processes involve and/or depend on information making information a critical business asset.

Information security policies and procedures define how we secure information appropriately and repeatedly.

ISO 27001 security

Te
ch
no
lo
gy

# Technology

## Information technologies

- Cabling, data/voice networks and equipment
- Telecommunications services (PABX, VoIP, ISDN, videoconferencing)
- Phones, cellphones, PDAs
- Computer servers, desktops and associated data storage devices (disks, tapes)
- Operating system and application software
- Paperwork, files
- Pens, ink

## Security technologies

- Locks, barriers, card-access systems, CCTV

ISO
27001
security

Value

# Information security is valuable because it …

- Protects information against various threats
- Ensures business continuity
- Minimizes financial losses and other impacts
- Optimizes return on investments
- Creates opportunities to do business *safely*
- Maintains privacy and compliance

**We all depend on information security**

ISO 27001 security

CI
A

Information security is defined

as the preservation of:

**Confidentiality**

Making information accessible only to those authorized to use it

**Integrity**

Safeguarding the accuracy and completeness of information and processing methods

**Availability**

Ensuring that information is available when required

ISO 27001 security

Impacts

# Security incidents cause …

- IT downtime, business interruption
- Financial losses and costs
- Devaluation of intellectual property
- Breaking laws and regulations, leading to prosecutions, fines and penalties
- Reputation and brand damage leading to loss of customer, market, business partner or owners' confidence and lost business
- Fear, uncertainty and doubt

ISO 27001 security

Key term

# What is risk?

Risk is the possibility that a threat exploits a vulnerability in an information asset, leading to an adverse impact on the organization

**Threat**: something that might cause harm

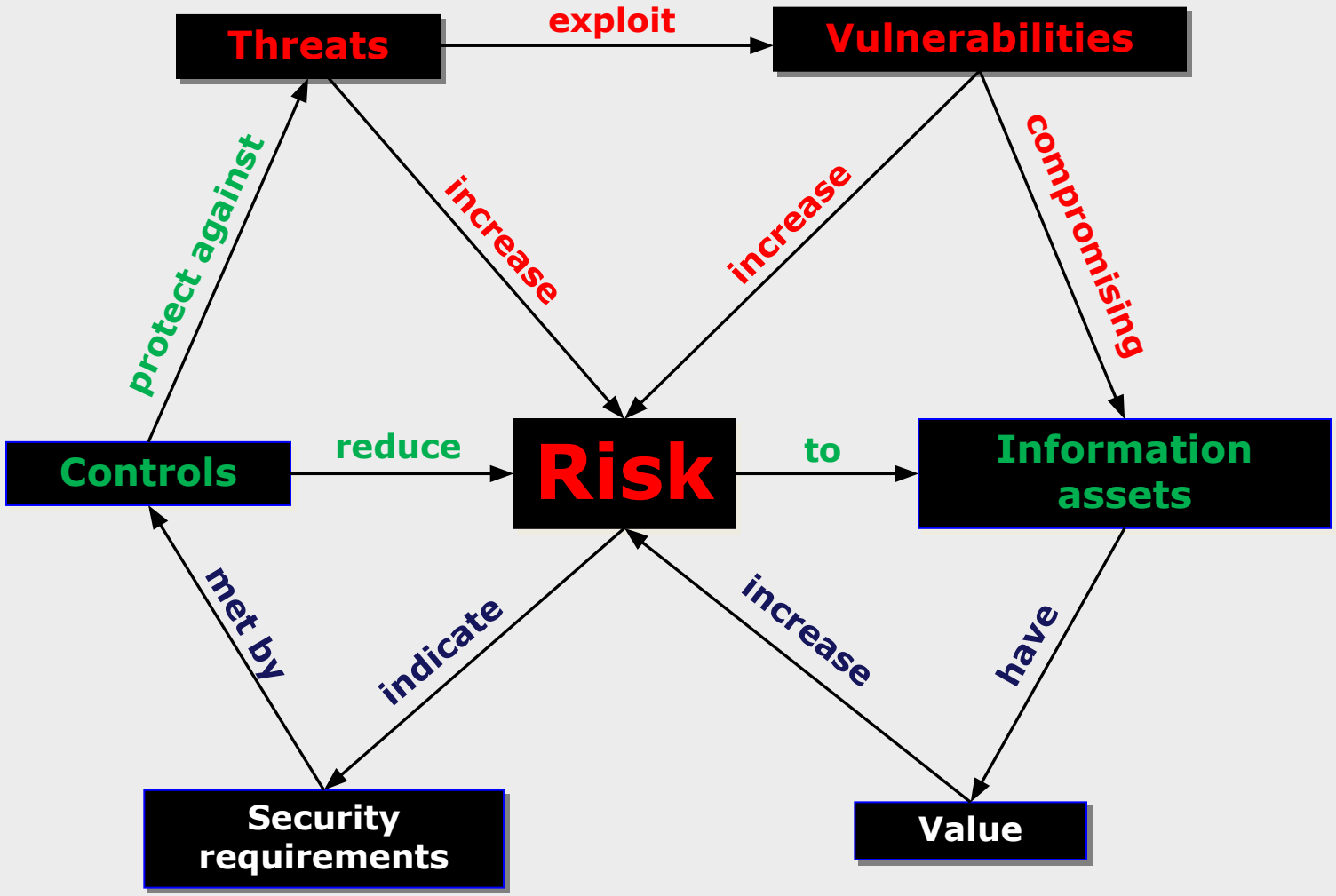
**Vulnerability**: a weakness that might be exploited

**Impact**: financial damage *etc.*

ISO 27001 security

Relationships

# Risk relationships




ISO 27001 security

Threat agent

# Threat agent

The actor that represents, carries out or catalyzes the threat

- Human
- Machine
- Nature

ISO 27001 security

Motive

# Motive

Something that causes the threat agent to act

- Implies intentional/deliberate attacks but some are accidental

ISO 27001 security

# Threat types

| Threat type | Example |
|---|---|
| Human error | Typo, wrong attachment/email address, lost laptop or phone |
| Intellectual property | Piracy, industrial espionage |
| Deliberate act | Unauthorized access/trespass, data theft, extortion, blackmail, sabotage, vandalism, terrorist/activist/criminal activity |
| Fraud | Identity theft, expenses fraud |
| System/network attack | Viruses, worms, Trojans, hacks |
| Service issue | Power cuts, network outages |
| Force of nature | Fire, flood, storm, earthquake, lightning, tsunami, volcanic eruption |
| Hardware issue | Computer power supply failure, lack of capacity |
| Software issue | Bugs or design flaws, data corruption |
| Obsolescence | iPhone 4? |

ISO 27001 security

So how *do* we secure our information assets?

ISO 27001 security

# A brief history of ISO27k

## 1990's

- Information Security Management Code of Practice produced by a UK government-sponsored working group
- Based on the security policy used by Shell
- Became British Standard BS7799

## 2000's

- Adopted by ISO/IEC
- Became ISO/IEC 17799 (later renumbered ISO/IEC 27002)
- ISO/IEC 27001 published & certification scheme started

## Now

- Expanding into a suite of information security standards (known as "ISO27k")
- Updated and reissued every few years

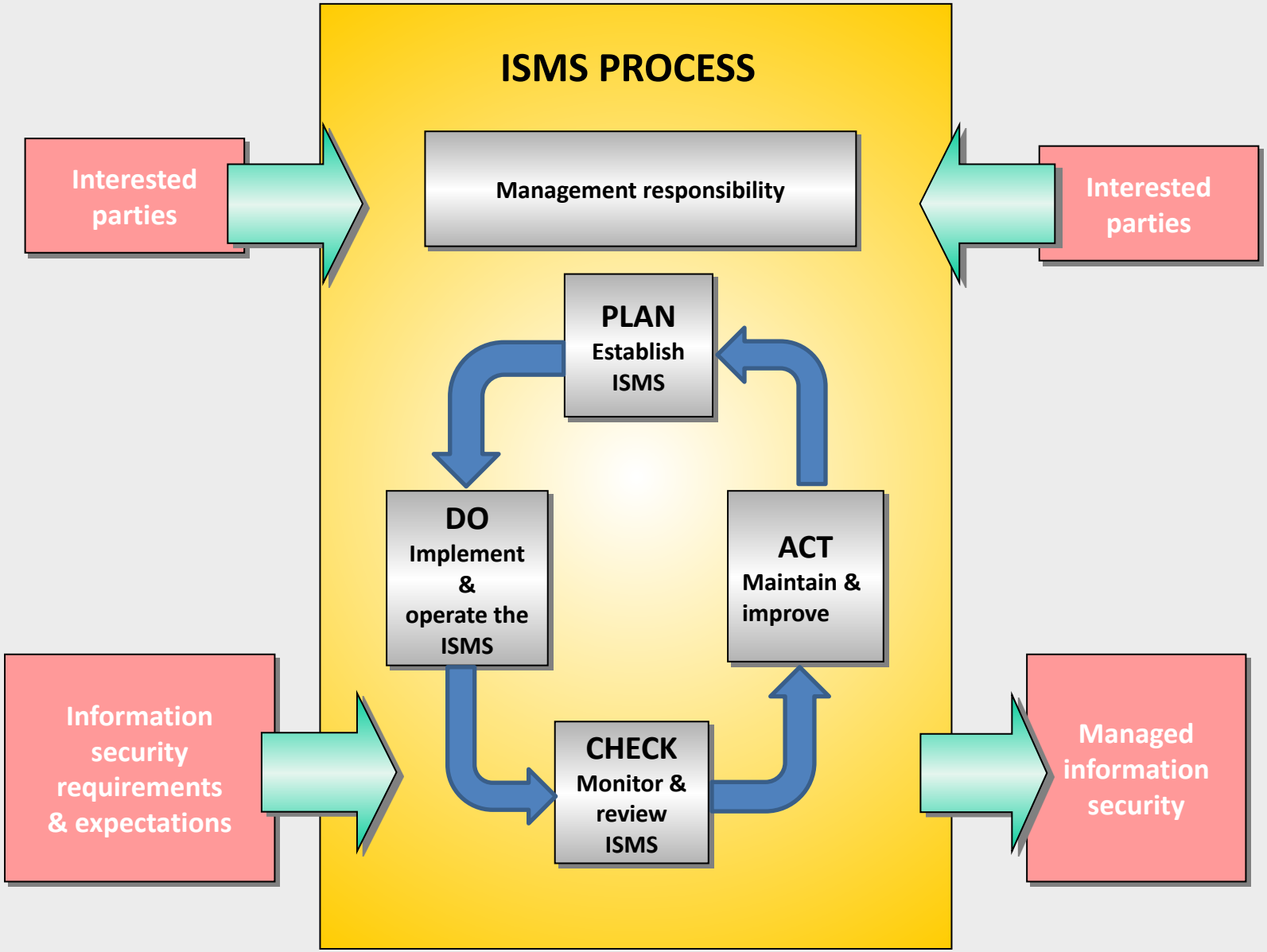
ISO 27001

# ISO 27001

- Concerns the management of *information* security, not just IT/technical security
- Formally specifies a management system
- Uses Plan, Do, Check, Act (PDCA) to achieve, maintain and improve alignment of security with risks
- Covers all types of organizations (e.g. commercial companies, government agencies, not-for-profit organizations) and all sizes
- Thousands of organizations worldwide have been certified compliant

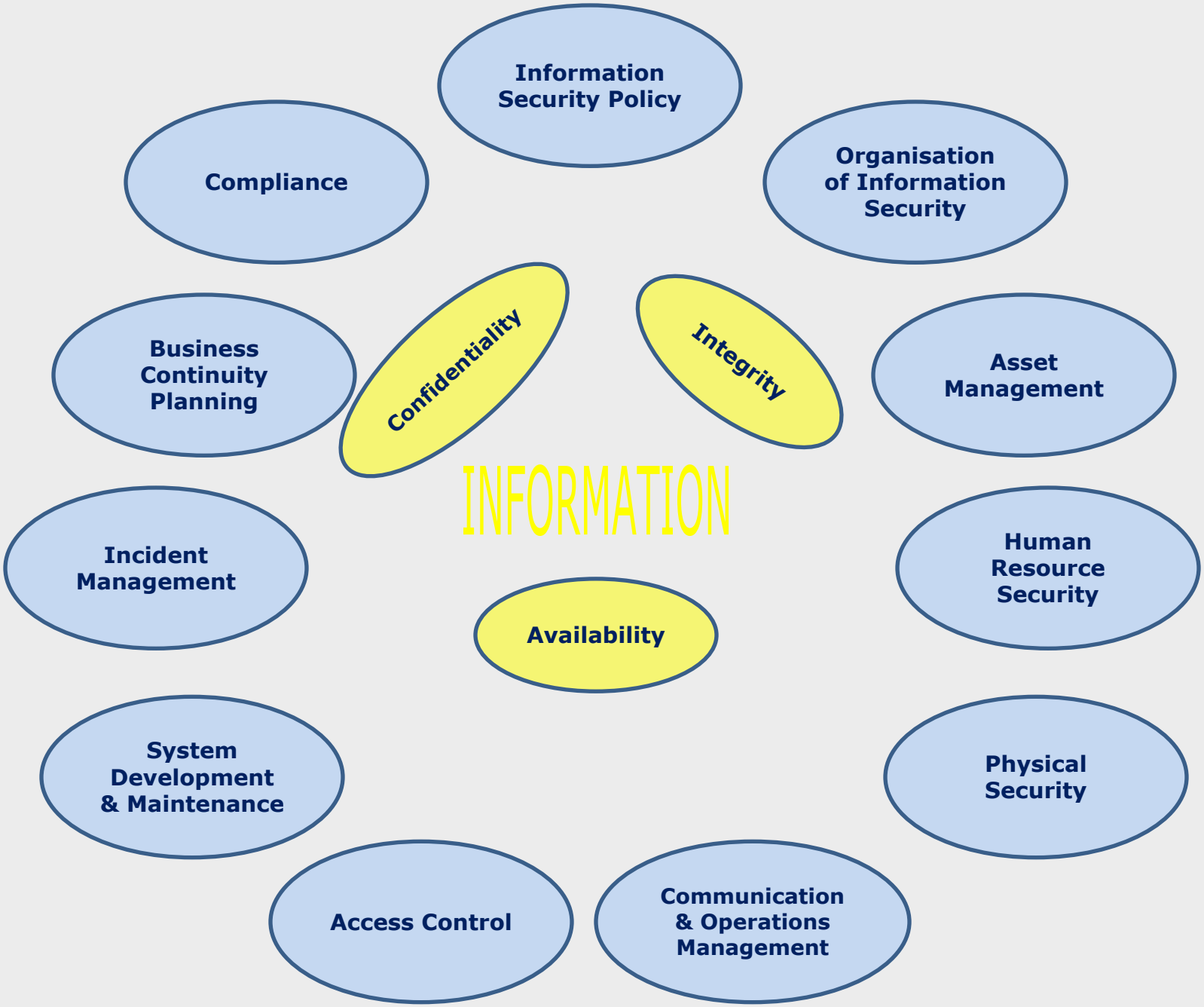
PD
CA

# Plan-Do-Check-Act




ISO 27001 security

# CONTROL CLAUSES




ISO 27001 security

# CONTROL CLAUSES

- **Information security policy** - management direction
- **Organization of information security** - management framework for implementation
- **Asset management** – assessment, classification and protection of valuable information assets
- **HR security** – security for joiners, movers and leavers
- **Physical & environmental security** - prevents unauthorised access, theft, compromise, damage to information and computing facilities, power cuts

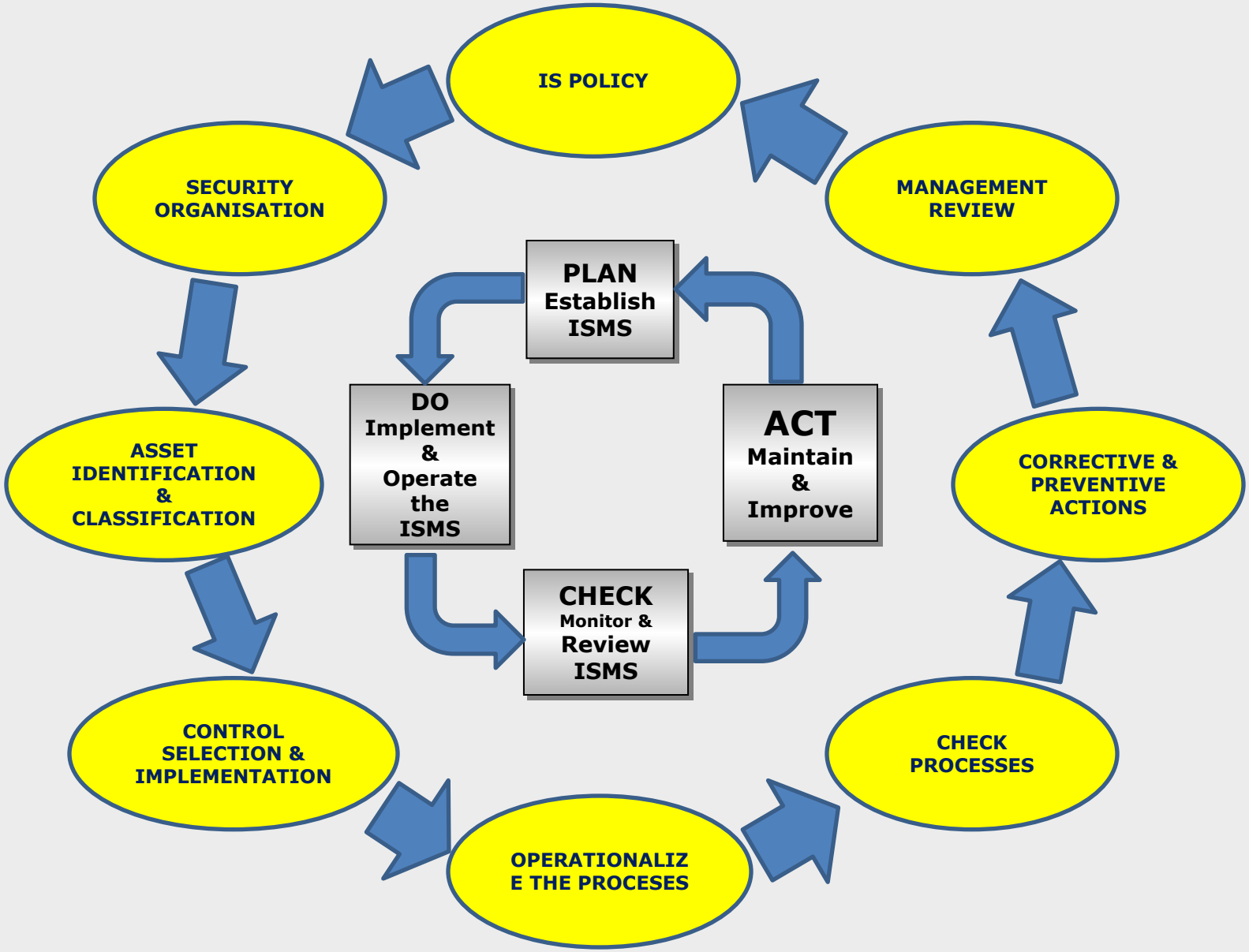
ISO 27001 security

CONTROL CLAUSES

- **Communications & operations management** - ensures the correct and secure operation of IT
- **Access control** – restrict unauthorized access to information assets
- **Information systems acquisition, development & maintenance** – build security into systems
- **Information security incident management –** deal sensibly with security incidents that arise
- **Business continuity management** – maintain essential business processes and restore any that fail
- **Compliance** - avoid breaching laws, regulations, policies and other security obligations

ISO 27001 security

# IMPLEMENTATION PROCESS CYCLE




ISO 27001 security

# Benefits

- Demonstrable commitment to security by the organization
- Legal and regulatory compliance
- Better risk management
- Commercial credibility, confidence, and assurance
- Reduced costs
- Clear employee direction and improved awareness

ISO 27001 security

Sc
op
e

# ISMS scope

- Data center & DR site
- All information assets throughout the organization

ISO 27001 security

Key documents

# Key ISMS documents

- High level **corporate security policy**
- Supporting policies *e.g.* physical & environmental, email, HR, incident management, compliance *etc.*
- Standards *e.g*. Windows Security Standard
- Procedures and guidelines
- Records *e.g.* security logs, security review reports, corrective actions

ISO 27001 security

VISION & MISSION

# Information security vision

*Vision*

The organization is acknowledged as an industry leader for information security.

*Mission*

To design, implement, operate, manage and maintain an Information Security Management System that complies with international standards, incorporating generally-accepted good security practices

ISO 27001 security

W
ho

# Who is responsible?

- Information Security Management Committee
- Information Security Manager/CISO and Department
- Incident Response Team
- Business Continuity Team
- IT, Legal/Compliance, HR, Risk and other departments
- Audit Committee

- Last but not least, you!

*Bottom line:*

**Information security is *everyone's* responsibility**

ISO 27001 security

Po
lic
y

# Corporate Information Security Policy


**Policy is signed by the CEO and mandated by top management**

**Find it on the intranet**

ISO
27001
security

INFO ASSET CLASSIFICATION

# Information Asset Classification

**CONFIDENTIAL**:
If this information is leaked outside the organization, it will result in major financial and/or image loss. Compromise of this information may result in serious non-compliance (*e.g.* a privacy breach). 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 required.
*Examples:* customer contracts, pricing rates, trade secrets, personal information, new product development plans, budgets, financial reports (prior to publication), passwords, encryption keys.

**INTERNAL USE ONLY:**
Leakage or disclosure of this information outside the organization is unlikely to cause serious harm but may result in some financial loss and/or embarrassment.
*Examples:* circulars, policies, training materials, general company emails, security policies and procedures, corporate intranet.

**PUBLIC:**
This information can be freely disclosed to anyone although publication must usually be explicitly approved by Corporate Communications or Marketing.
*Examples:* marketing brochures, press releases, website.

ISO 27001 security

Classification

# Confidentiality

**Confidentiality of information concerns the protection of sensitive (and often highly valuable) information from unauthorized or inappropriate disclosure.**

| Confidentiality level | Explanation |
|---|---|
| High | Information which is very sensitive or private, of great value to the organization and intended for specific individuals only. The unauthorized disclosure of such information can cause severe harm such as legal or financial liabilities, competitive disadvantage, loss of brand value *e.g.* merger and acquisition related information, marketing strategy |
| Medium | Information belonging to the company and not for disclosure to public or external parties. The unauthorized disclosure of this information may harm to the organization somewhat e.g. organization charts, internal contact lists. |
| 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 |

ISO 27001 security

USE R RESP ONSI BILI TIES

# Physical security

## Do

- Read and follow security policies and procedures
- Display identity cards while on the premises
- Challenge or report anyone without an ID card
- Visit the intranet Security Zone or call IT Help/Service Desk for advice on most information security matters

## Do not


- Allow unauthorized visitors onto the premises
- Bring weapons, hazardous/combustible materials, recording devices *etc*., especially in secure areas
- Use personal IT devices for work purposes, unless explicitly authorized by management

ISO 27001 security

# Password Guidelines

- Use long, complicated passphrases - whole sentences if you can
- Reserve your strongest passphrases for high security systems (don't re-use the same passphrase everywhere)
- Use famous quotes, lines from your favorite songs, poems *etc*. to make them memorable

- Use short or easily-guessed passwords
- Write down passwords or store them in plain text
- Share passwords over phone or email

USER RESPONSIBILITIES

# Internet usage

- Use the corporate Internet facilities *only* for legitimate and authorized business purposes

- Avoid websites that would be classed as obscene, racist, offensive or illegal – anything that would be embarrassing
- Do not access online auction or shopping sites, except where authorized by your manager
- Don't hack!
- Do not download or upload commercial software or other copyrighted material without the correct license and permission from your manager


Warning: Internet usage is routinely logged and monitored. Be careful which websites you visit and what you disclose.

ISO 27001 security

# E-mail usage

- Use corporate email for business purposes only
- Follow the email storage guidelines
- If you receive spam email, simply delete it. If it is offensive or you receive a lot, call the IT Help/Service Desk

- Do not use your corporate email address for personal email
- Do not circulate chain letters, hoaxes, inappropriate jokes, videos *etc.*
- Do not send emails outside the organization unless you are authorized to do so
- Be very wary of email attachments and links, especially in unsolicited emails (most are virus-infected)

# Security incidents

- Report information security incidents, concerns and near-misses to IT Help/Service Desk:
  - Email …
  - Telephone …
  - Anonymous drop-boxes …
- Take their advice on what to do

- Do not discuss security incidents with anyone outside the organization
- Do not attempt to interfere with, obstruct or prevent anyone else from reporting incidents

# Responsibilities

- ✔ Ensure your PC is getting antivirus updates and patches
- ✔ Lock your keyboard (Windows-L) before leaving your PC unattended, and log-off at the end of the day
- ✔ Store laptops and valuable information (paperwork as well as CDs, USB sticks *etc.*) securely under lock and key
- ✔ Keep your wits about you while traveling:
  - Keep your voice down on the cellphone
  - Be discreet about your IT equipment
- ✔ Take regular information back ups
- ✔ Fulfill your security obligations:
  - Comply with security and privacy laws, copyright and licenses, NDA (Non Disclosure Agreements) and contracts
  - Comply with corporate policies and procedures
- ✔ Stay up to date on information security:
  - Visit the intranet Security Zone when you have a moment

ISO 27001 security


ISO 27001 security