ISO 27001
Information Security Management Systems

Prepared by

Alain Kallas, ***Front Defense*** *FZ LLC*

In Collaboration with

Mideast Data Systems

Agenda

- Introduction
  - What is Information Security?
  - What is ISO 27001?
- Information Security Management System (ISMS) Requirements
  - PDCA Model
  - Risk Assessment
  - Management Responsibilities
  - Internal ISMS Audits
  - Management Review of the ISMS
  - ISMS Improvement

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Agenda

- Controls Objectives and Controls
  - Security Policy
  - Organization of Information Security
  - Asset Management
  - Human Resources Security
  - Physical and Environmental Security
  - Communications and Operations Management
  - Access Control
  - Information Systems acquisition, development and maintenance
  - Information Security Incident management
  - Business Continuity Management
  - Compliance

The Basics

- **What is Information?**

What is Information?

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

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

What is Information?

'Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation.

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

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Information – The Lifeblood

- Banks
- Software Houses
- National Security
- Charities
- Product Secrets
- Health Care
- Financial Models
- Police Records

The list is long!……..

What Can be Done with Information?

Information can be:

Created **Stored** **Destroyed?**

Processed **Transmitted**

Used – (for proper and improper purposes)

Lost! **Corrupted!**

Information Security Risks

- (Some) Categories of Information Security Risk:
  - Information theft
  - Intrusion and subversion of system resources
  - Denial of service
  - Loss
  - Corruption

Vulnerabilities

- Lack of appreciation of threats
- Staff / Contractors / Employees
- E-mail and internet access
- Physical Security
- Outsourcing
- Remote working

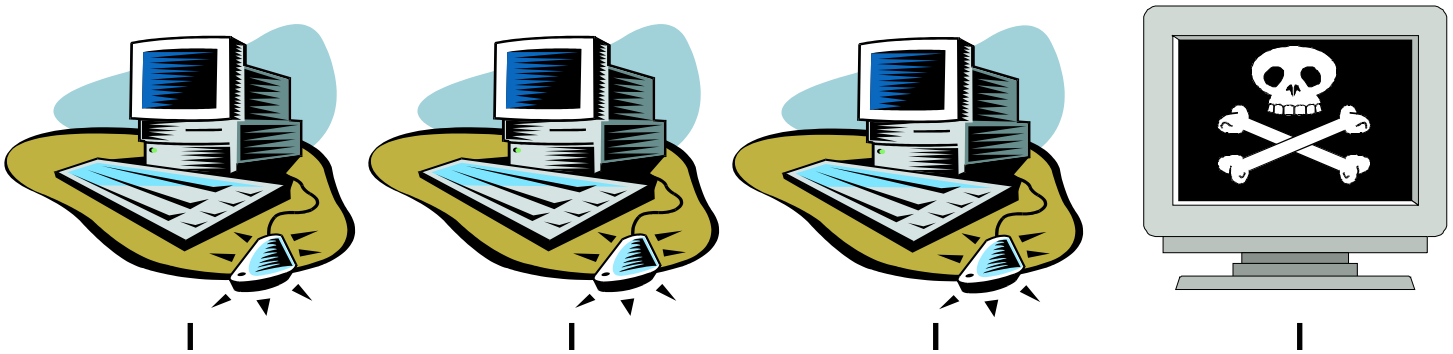
Business Risks

- **Fraud**
- **Disclosure**
- **Denial of Service**
- **Damage to Reputation**
- **Loss of Customers**
- **Shareholder/Stakeholder Relations**
- **Legal and Regulatory action**

= Damage to Image

System Access & Networks

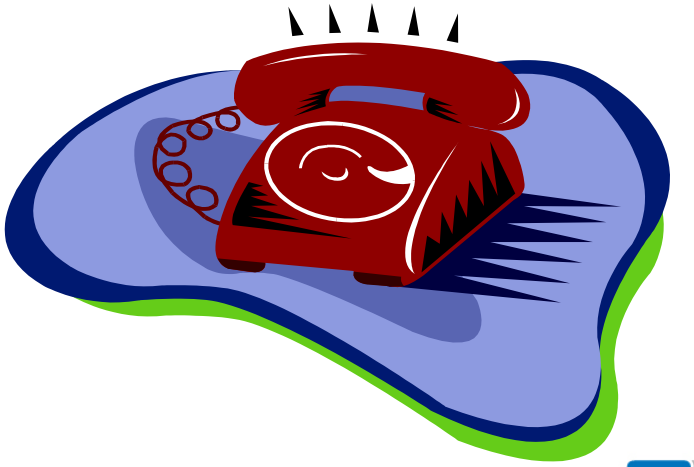
Where are the compromises coming from?



FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

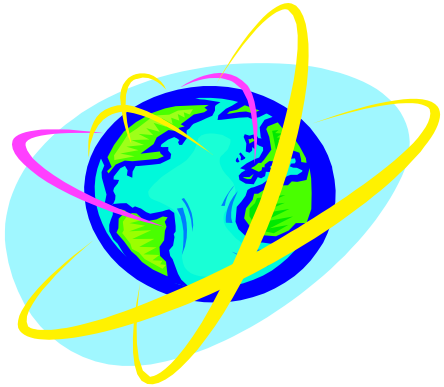
Telephone Networks and their Growth

- Global network
- Anyone can access any connected machine from any other connected machine
- Cheap and accessible



Internet and its Problems

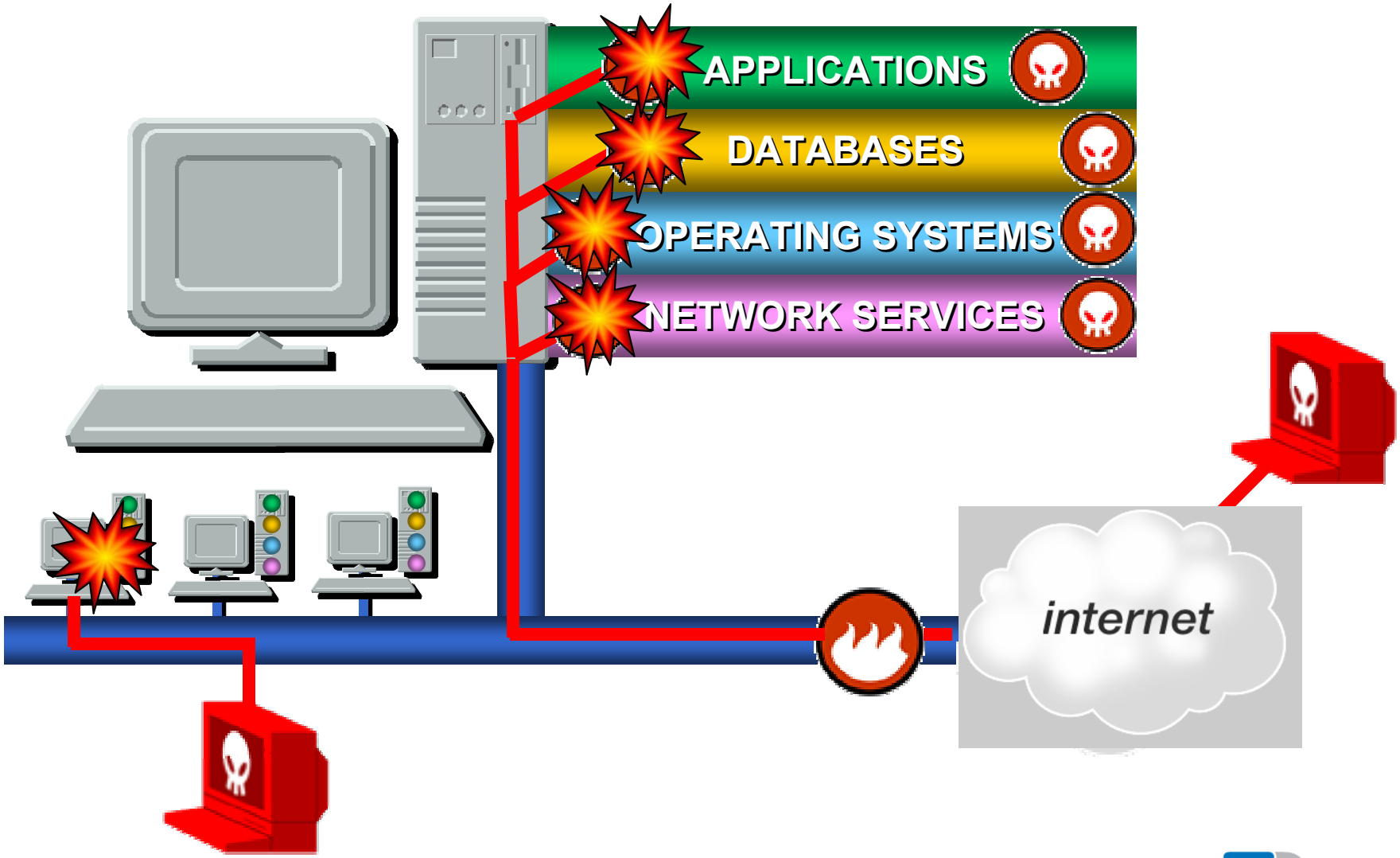
- Staggering growth rate
- Anyone can access any connected machine from any other connected machine
- Good guys and the bad guys are all connected



US defense systems were attacked.

65% of those attacks were successful.

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER



FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Cited Examples of Common Attacks

- Forged e-mail ‘from’ addresses.
- E-mail with "executable" enclosures to launch viruses and other attack programs.
- Attractive programs for download that have hidden and possibly malicious or damaging side-effects (‘Trojan horse’ programs).
- Computer boot-sector viruses to crash systems.
- Spoofing to conceal the true source of a message.
- Hijacking to masquerade as a legitimate correspondent.

Cited Examples of Common Attacks

- Password sniffing to steal a user's on-line identity.
- Interception of communications traffic or ‘eavesdropping’.
- Various forms of data or protocol flooding to crash a system or network .
- Subversion of operating systems.
- Use of default account names and passwords.
- Theft of password files and cracking of weak passwords.

Password Crackers

- People tend to use easily remembered passwords
- Passwords often have personal significance
- Use dictionaries to crack passwords
- Commercially available programmes to crack passwords

A recent test using such a program on an University NT network successfully cracked all 10,000+ passwords.

The Weakest Link

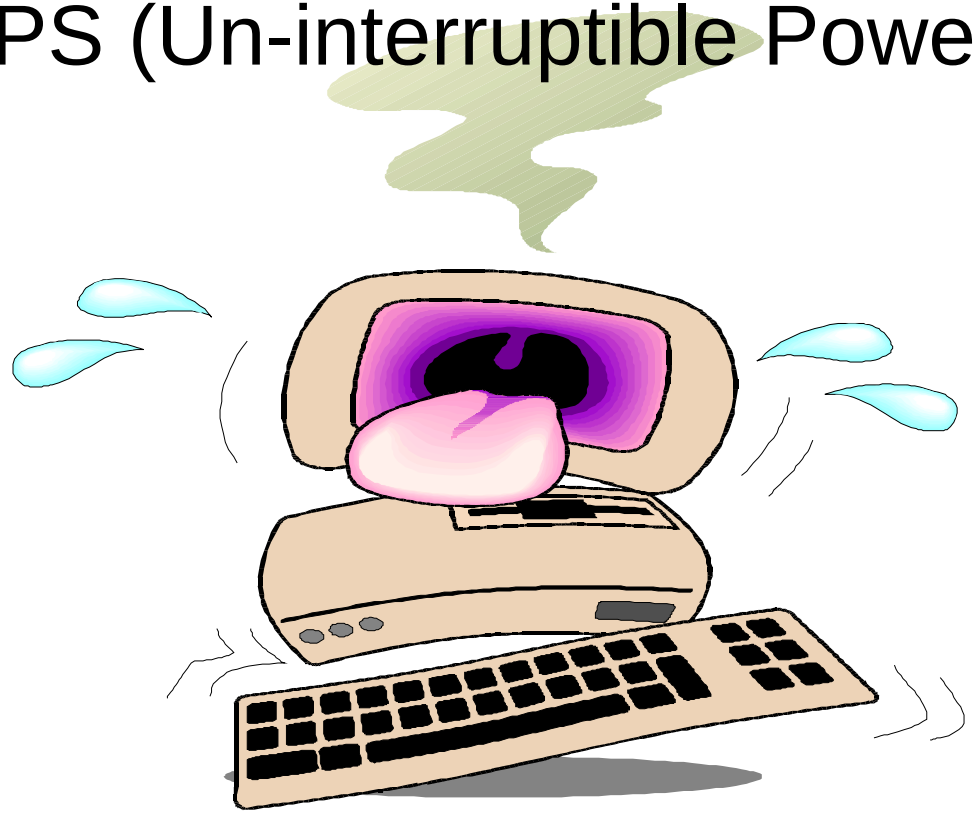
- Question:
- If you had a budget of $1,000,000 how would you crack a HIGH security system?

Bribe the staff

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Equipment Failure

- Lack of Planned Disaster Recovery and back-ups
- No UPS (Un-interruptible Power Supply)



FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Theft

Computer theft is the fastest growing crime in the UK.

Every local authority in London has been hit by computer theft.

Every £1 of IT equipment lost or stolen costs £15 in business disruption.

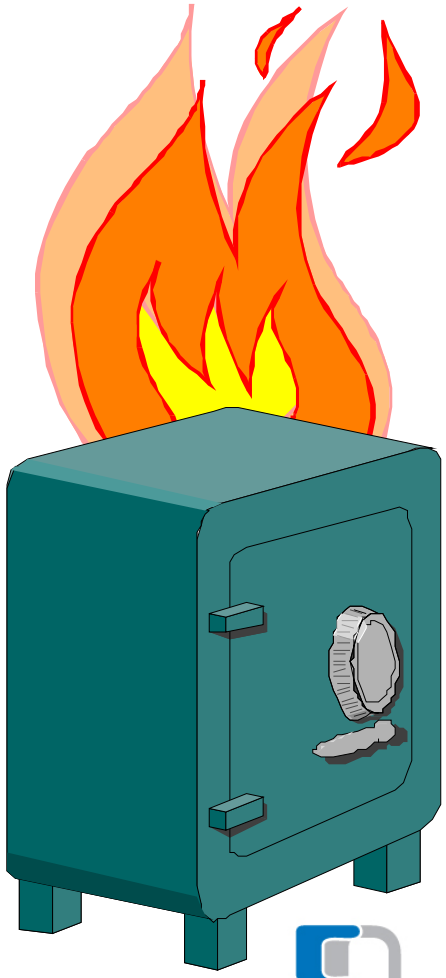
Computer theft cost British industry over £1.5 billion.

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Absence of Disaster Recovery Plan

- **No regular tape back-up stored in fireproof safes.**
- **No extra set held off-site.**
- **Back up tapes not verified and tested.**

  (50% of disc back-ups tested never work)
- **Important paper documents, e.g. contracts, not protected and/or copied.**



FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

NOTE:

If the building is unsafe the Fire Services will not let people back in. Information may be unobtainable for weeks.

This is an example of DR planning that has not been thought through.

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Non – IT

- Paper documents –
  on desks,
  in waste bins,
  left on photocopiers
- Whiteboards and flipcharts
- Telephone conversations overheard
- Conversations on public transport

What is Information Security?

‘Information security protects information from a wide range of threats in order to ensure business continuity, minimise business damage and maximise return on investment and business opportunities’.

The three basic components:

- Confidentiality
- Integrity
- Availability

Confidentiality

Ensuring that information is accessible only to those authorised to have access.

Integrity

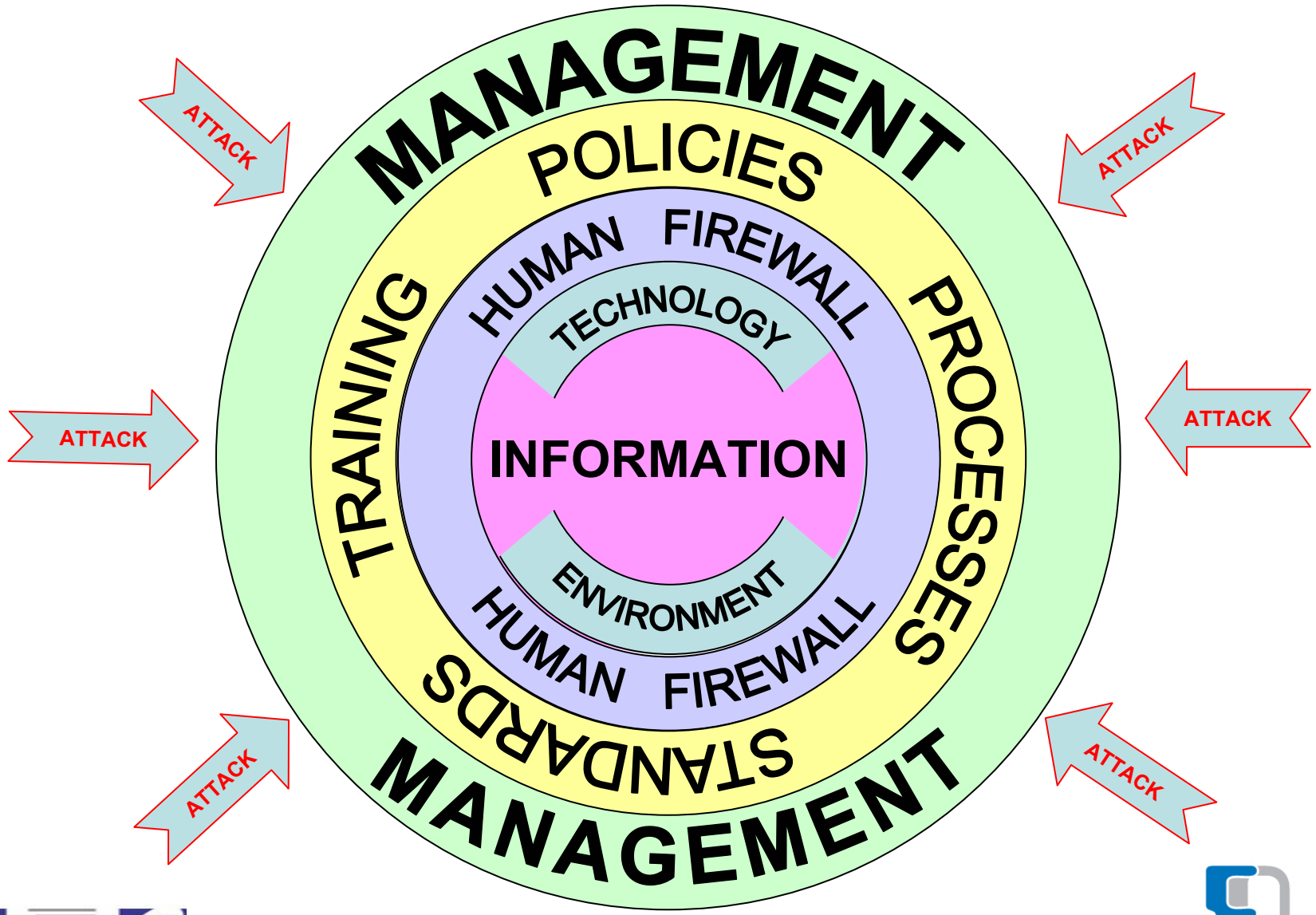
Safeguarding the accuracy and completeness of information and processing methods.

Availability

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

In some organizations, integrity and/or availability may be more important than confidentiality.

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER



FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

ISO 27001 defines best practice for Information Security Management

- Without a formal Information Security Management System such as a ISO 27001 based system, security will be breached.
- Information Security is a management process, not a technological process.

Management commitment

- Business managers need to be seen to be committed (Process Ownership)
- Expect Chief Executive/Managing Director to demonstrate commitment (Risk Management Decisions)

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Design and Implementation of an Information Security Management System

ISO 27001 Requirements

- **Section 4: Information security management system**
- **Section 5: Management responsibility**
- **Section 6: Internal ISMS audits**
- **Section 7: Management review of the ISMS**
- **Section 8: ISMS improvement**

General Requirements

- Develop, implement, maintain *and continually improve*
- Policy and *objectives*
- *PDCA*

Plan Do Check Act

- Information security policy
- Scope of the ISMS
- Risk identification and assessment
- Risk treatment plan (planning)

Plan ***Do*** Check Act

- Resources, training and awareness
- Risk treatment (control implementation)

Plan Do ***Check*** Act

- Routine checking
- Learning from others
- Audits
- Management review
- Trend analysis

Plan Do Check ***Act***

- Non-conformity
- Corrective and preventive actions

Implementation

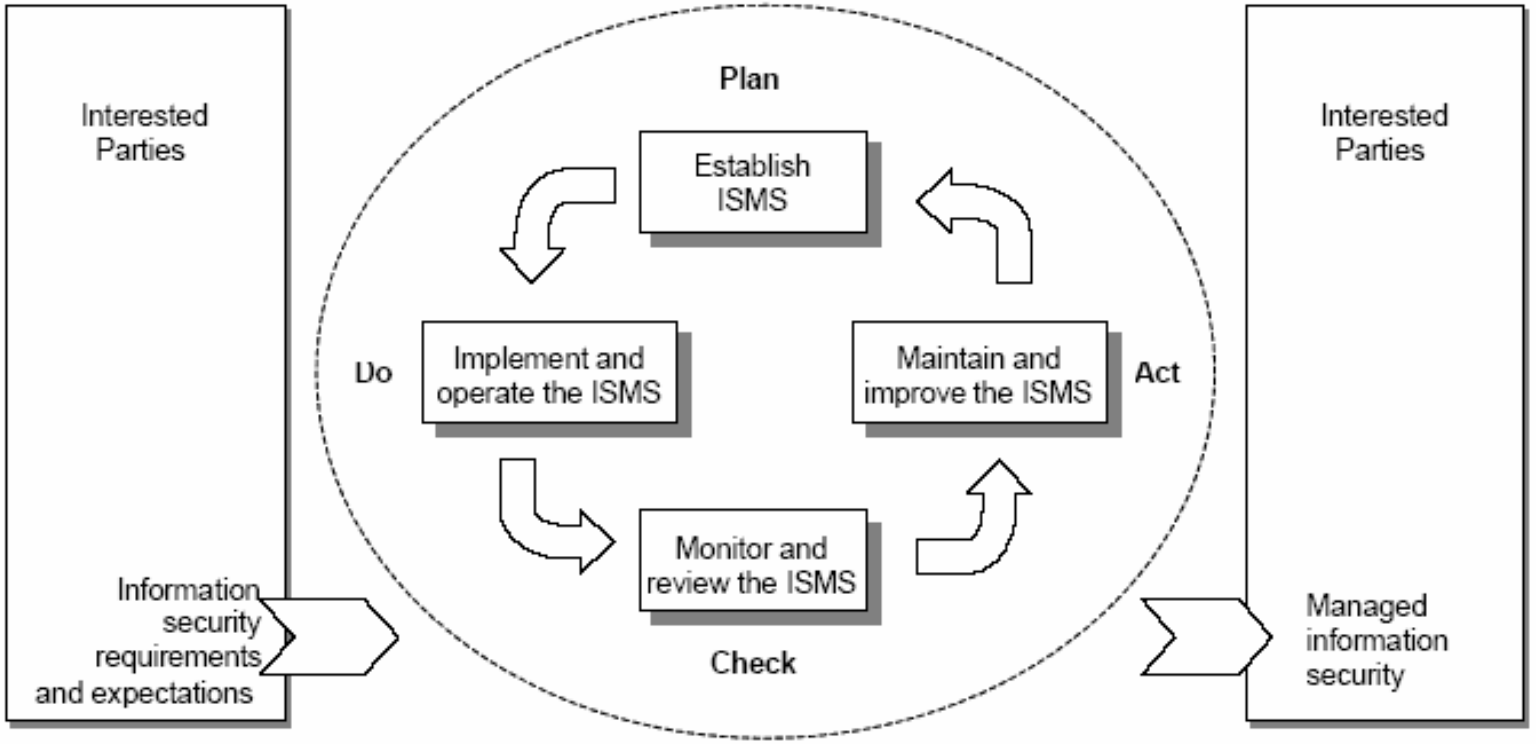


Figure 1 — PDCA model applied to ISMS processes

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

ISMS Framework

Critical success factors

- Experience has shown that the following factors are often critical to the successful implementation of information security within an organisation:

ISMS Framework

- Security policy, objectives and activities that reflect business objectives;
- An approach to implementing security that is consistent with the organizational culture;
- Visible support and commitment from management;
- A good understanding of the security requirements, risk assessment and risk management;
- Effective marketing of security to all managers and employees.

ISMS Framework

- Distribution of guidance on information security policy and standards to all employees and contractors;
- Providing appropriate training and education;
- A comprehensive and balanced system of measurement which is used to evaluate performance in information security management and feedback suggestions for improvement.

ISMS Framework

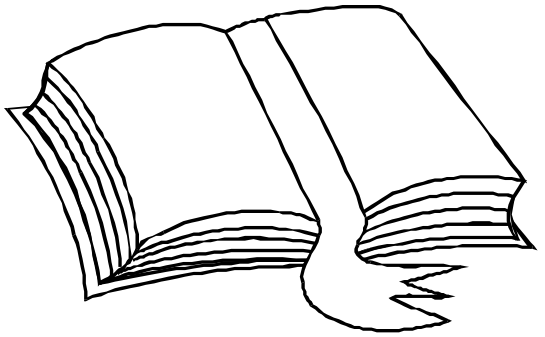
- Documentation
- Evidence of actions
  - undertaken to establish the management framework.
- Summary of the management framework
  - including policy, control objectives, implemented controls and summary of controls.

ISMS Framework

- Procedures
  - to implement the controls and describe
  - responsibilities and actions.
  - covering the management and operation of the ISMS and describing responsibilities and actions.

ISMS – Security Policy

‘A policy document shall be approved by management, published and communicated, as appropriate, to all employees’



FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

ISMS – Scope

- Does the documentation describe unambiguously the scope of the ISMS?
- Are significant exclusions from the scope clearly identified and explained?
- Boundaries/interfaces must be clearly understood (important for the management of customer/supplier/partner relationships).

The management of these relationships is often the most difficult area for consideration in the ISMS.

Scope

If the scope is limited to part of an organization, its contents and audience will most probably be different from a scope covering the entire organization.

Where the ISMS is to satisfy external customers, there may well be externally facing and internally facing policies.

Therefore it is always (?) preferable to define the scope first, which will then determine the style and content of the policy(ies).

Scope

The organization will need to present its scope for a proposed information security management system to meet the requirements of ISO 27001.

The scope shall be appropriate for the needs of customers (whether internal and/or external), and shall include the management of interfaces with all partners, suppliers and customers that may reasonably be considered to have an impact on the security of the object information.

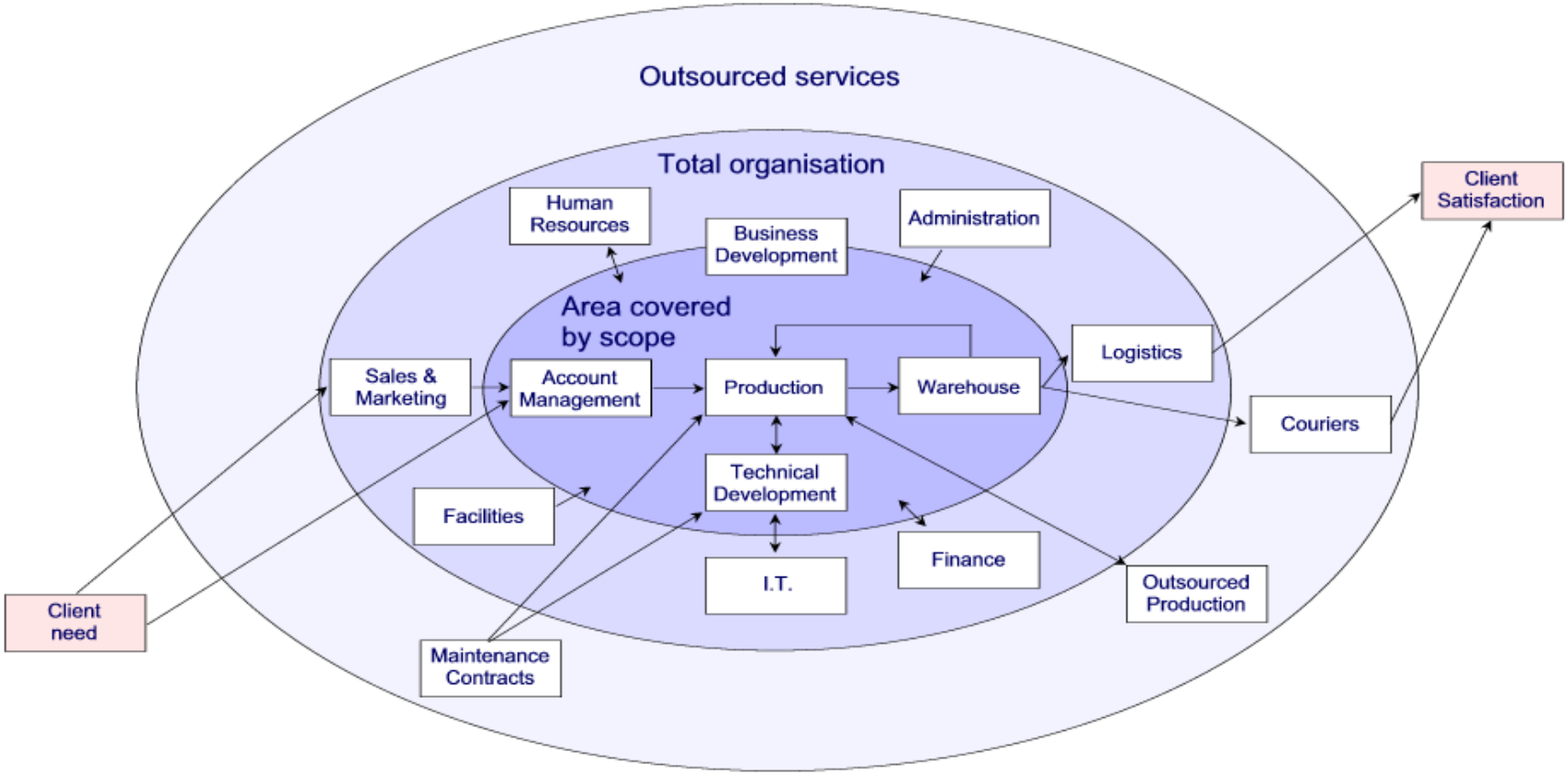
FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Scope

In the assessment of the scope, it will be expected that the organization has defined the contracts, service level agreements, memoranda of understanding and any other methods for implementing information security management across the interfaces with partners, suppliers and customers, etc.

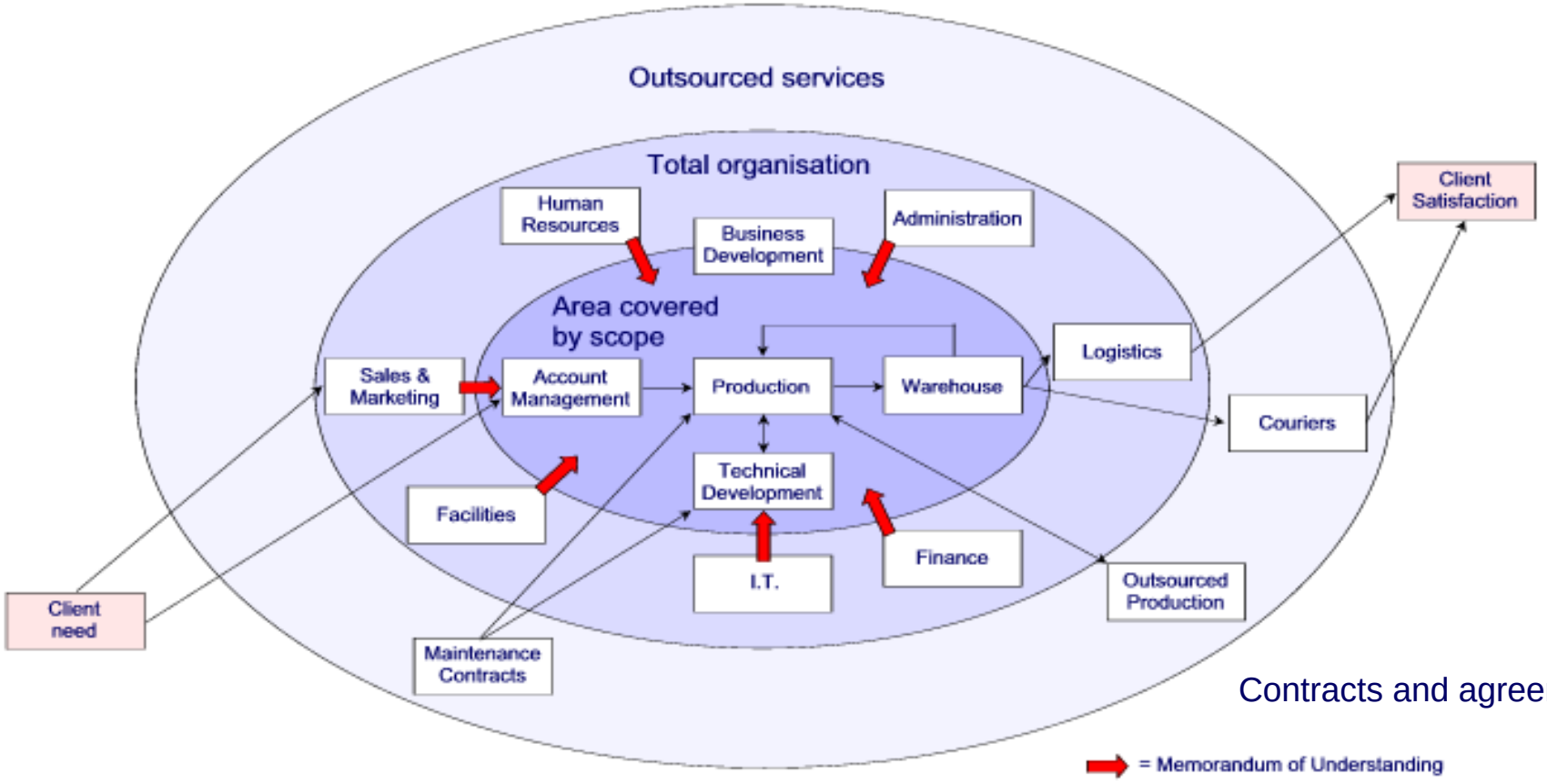
Difficulties in defining scope?

Consider the following:



FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Defining Participants



FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

ISMS – Risk Assessment

- Has a formal Risk Assessment been identified, performed and documented?
- Has the selected method of Risk Assessment been justified by an appropriate member of staff?
- Does the Risk Assessment identify the vulnerabilities of assets, the threats and potential impacts on the organization?
- Does the Risk Assessment identify potential losses of CIA on assets?
- Is Risk Assessment conducted at appropriate intervals and when changes occur to the system/ organization?

Security Risks

- A Security risk is the potential that a given threat will exploit vulnerabilities to cause loss or damage to an asset or group of assets. Examples are?

Not always IT!

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Risk Assessment

- ISO 27001 requires a Risk Assessment to be carried out to identify threats to assets.

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Asset Value and Potential Impacts

What is the value of an asset?
(in the event of an incident)

Assets

- Examples of assets associated with information systems are:
  - Information assets – data files, user manuals etc.
  - Paper documents – contracts, guidelines etc.
  - Software assets – application & systems software etc.
  - Physical assets – computer, magnetic media etc.
  - People – customers, personnel etc.
  - Company image and reputation
  - Services – communications, technical etc.

The value(s)

The value(s) will be measured in terms of impact on the organization, its suppliers, partners, customers and other interested parties in the event of a breach of security affecting confidentiality, integrity or availability.

The value(s) of the assets shall be established relevant to the context in which they are employed/ exist.

Context Specific Asset Values

More meaningful values need to be defined relative to impact of a security breach. Care should be exercised as judgements are subjective, and too much ‘granularity’ or ‘weighting’ may give the perception of a pseudo-scientific approach.

Generally, 4 ratings e.g ‘Very high’, ‘High’, ‘Medium’ and ‘Low’ will be adequate for the purpose of ranking risks.

Context Specific Asset Values

Only the process owners (or their customers) can realistically define asset values, as it is important to make the judgement for each context in which an information asset exists or is used.

Risk Assessment

The organization will demonstrate that it has identified a suitable risk assessment method and conducted a risk assessment covering all assets identified.

Evaluating Methods

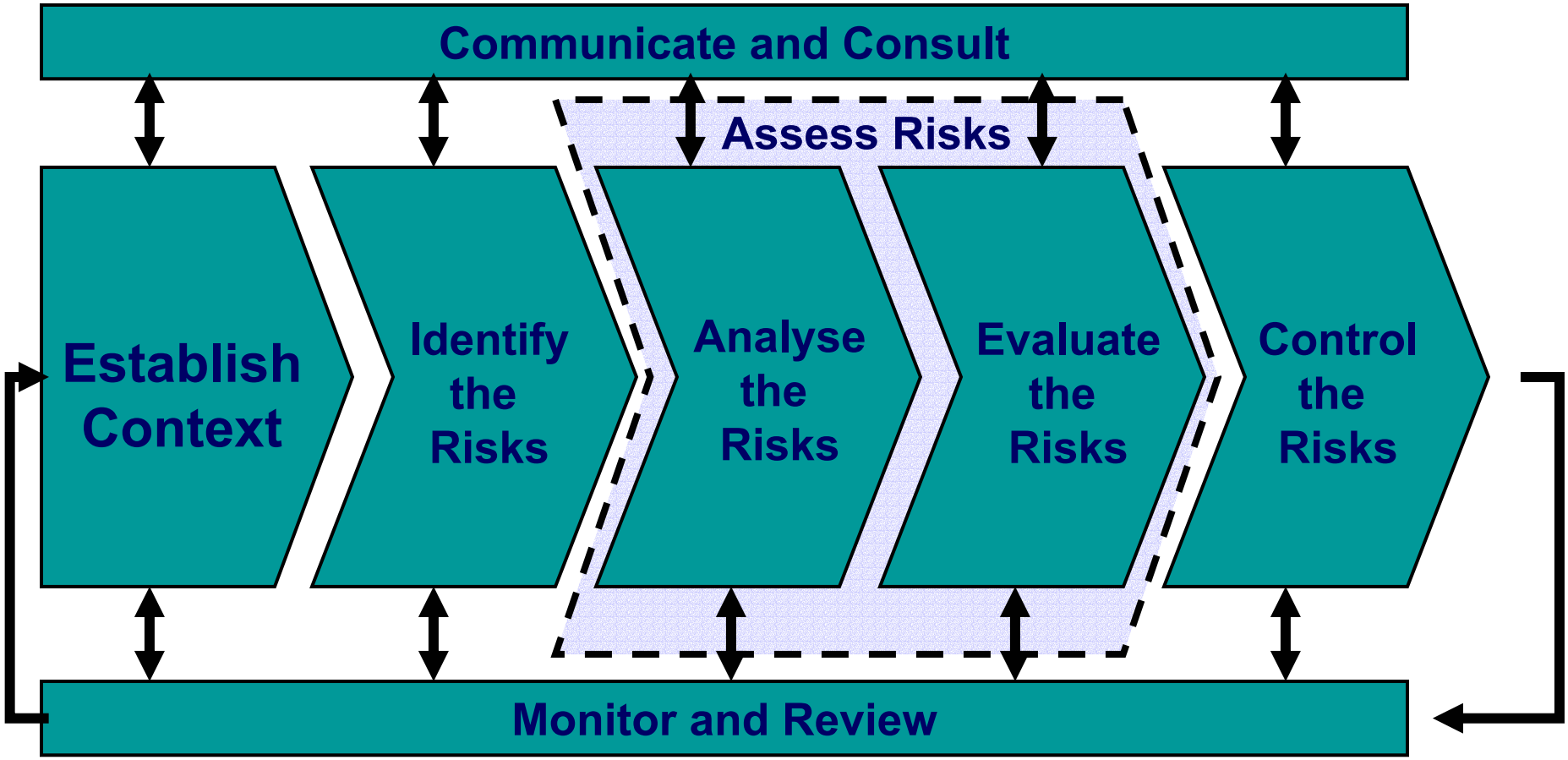
Considerations:

- Does it identify vulnerabilities and threats?
- Does it attempt to evaluate probabilities of threats occurring?
- Would someone else using the same data come up
  with the same results?
- Is the process repeatable and sustainable?
- Does it allow for analysis of impact of changes?

Deliverables from any risk assessment

- The process should identify any significant risk to all identified assets in the context of use.
- The process should provide a comprehensive report to management.
- The report should rank the risks according to potential impact on the organization and its customers.
- It should identify any quick wins where it is possible to reduce risks substantially, quickly and cost effectively.
- It should, where possible, identify alternative solutions with pro's and con's.

Risk Assessment Process



FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Risk Identification

Vulnerabilities are weaknesses associated with information assets. These weaknesses may be exploited by a threat causing a security breach that may result in loss,damage or harm to these
assets.

Threats

A threat has the potential to cause an unwanted incident which may result in harm to a system or organization and its assets

Threats

- Assets are subject to many kinds of threats which exploit vulnerabilities, examples of which are?

Vulnerabilities

A vulnerability in itself does not cause harm, it is merely a condition or set of conditions that may allow a threat to affect an asset

Vulnerabilities

- Vulnerabilities are weaknesses associated with an organization's assets, examples are?

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Evaluate the Risks

The objective of analysis is to separate the minor risks from the major risks, and provide data to assist in the evaluation and control of risk.

Risk analysis involves consideration of the source of the risk, determination of the consequence and the likelihood of those consequences occurring.

Probability

- What is the probability of an incident?

An organization certified to ISO 27001 was struck by lightning shortly before the assessment.

Another company certified to ISO 27001 was ram-raided. They were able to meet customer commitments thanks to their ISMS.

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Probability

This is often subjective and will need to be evaluated with the asset owner and probably with expert assistance. The main questions you need to ask are:

What is the likelihood of this happening?

How often will it happen?

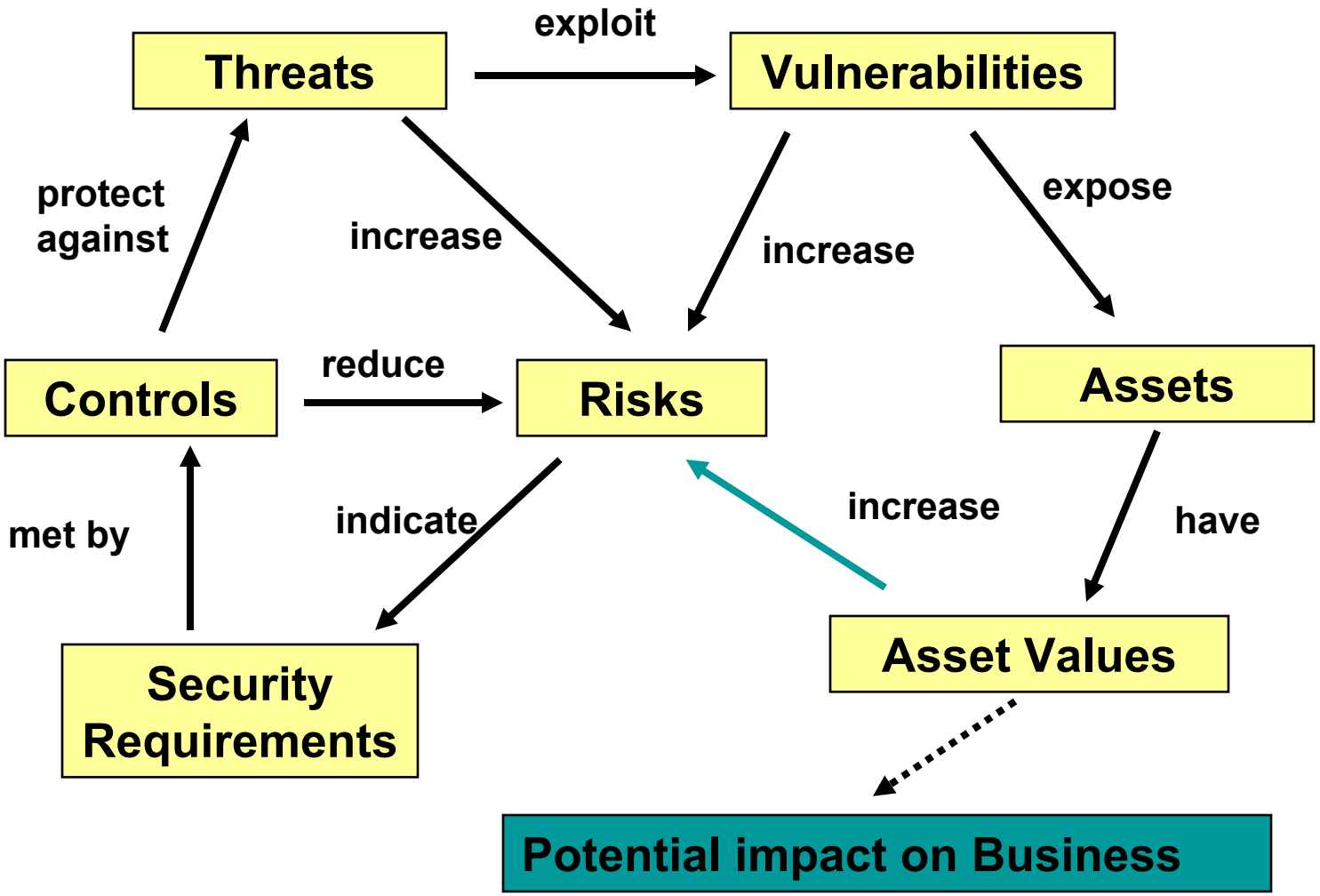
When will it happen?

Expectation

The organization will rank the risks and identify any measures that may be employed to provide ‘quick wins’ to reduce any of the perceived risks.

Note: ‘quick wins’ may include simple expedients such as controlling physical access by locking doors.

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER



FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

ISMS – Risk Treatment

- Has the organization's approach to Risk Treatment been defined?
- Has the required acceptable level been defined?
- Are (control) options produced for management decisions?

If the requirement has not been implemented, why not?

- Risk, not justified by risk exposure
- Budget, financial constraints
- Environment, influence on safeguards; climate, space etc.
- Technology, some measures are not technically feasible
- Culture, sociological constraints
- Time, some requirements cannot be implemented now
- N/A, not applicable
- Others

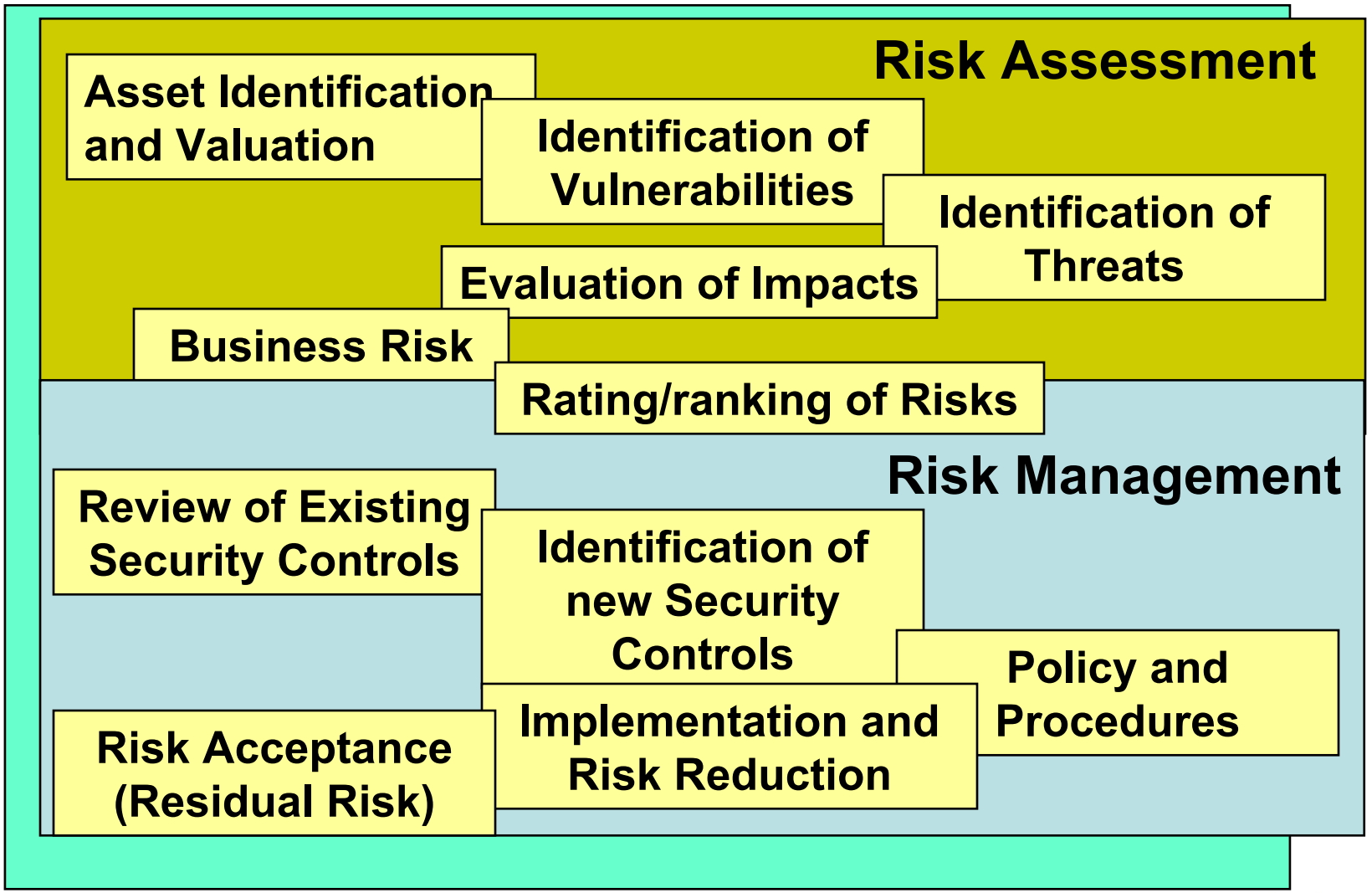
Risk Treatment – Plan

- Applying controls
- Accepting the risk
- Avoiding the risk
- Transferring the risk

Acceptable Level of Risk

- It is not possible to achieve total security
- There will always be residual risk
- What degree of residual risk is acceptable to the organization?

Risk Assessment Process



ISMS – Controls

- Are selected controls based on Risk Assessment results?
- Is it clear from the Risk Assessment which controls are baseline measures, which are mandatory and which may be considered optional?
- Do controls reflect the organization's risk management strategy?

Controls

- Effective Security generally requires combinations of the following:

ISMS – Statement of Applicability

- Has a Statement of Applicability (SoA) been prepared which identifies the reason for selection of appropriate controls and identifies excluded controls?

Note:
This is the key document for assessment.
It is the linking document between ISO 27001 and the ISMS. It will be referenced from the certification.

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

The Statement of Applicability

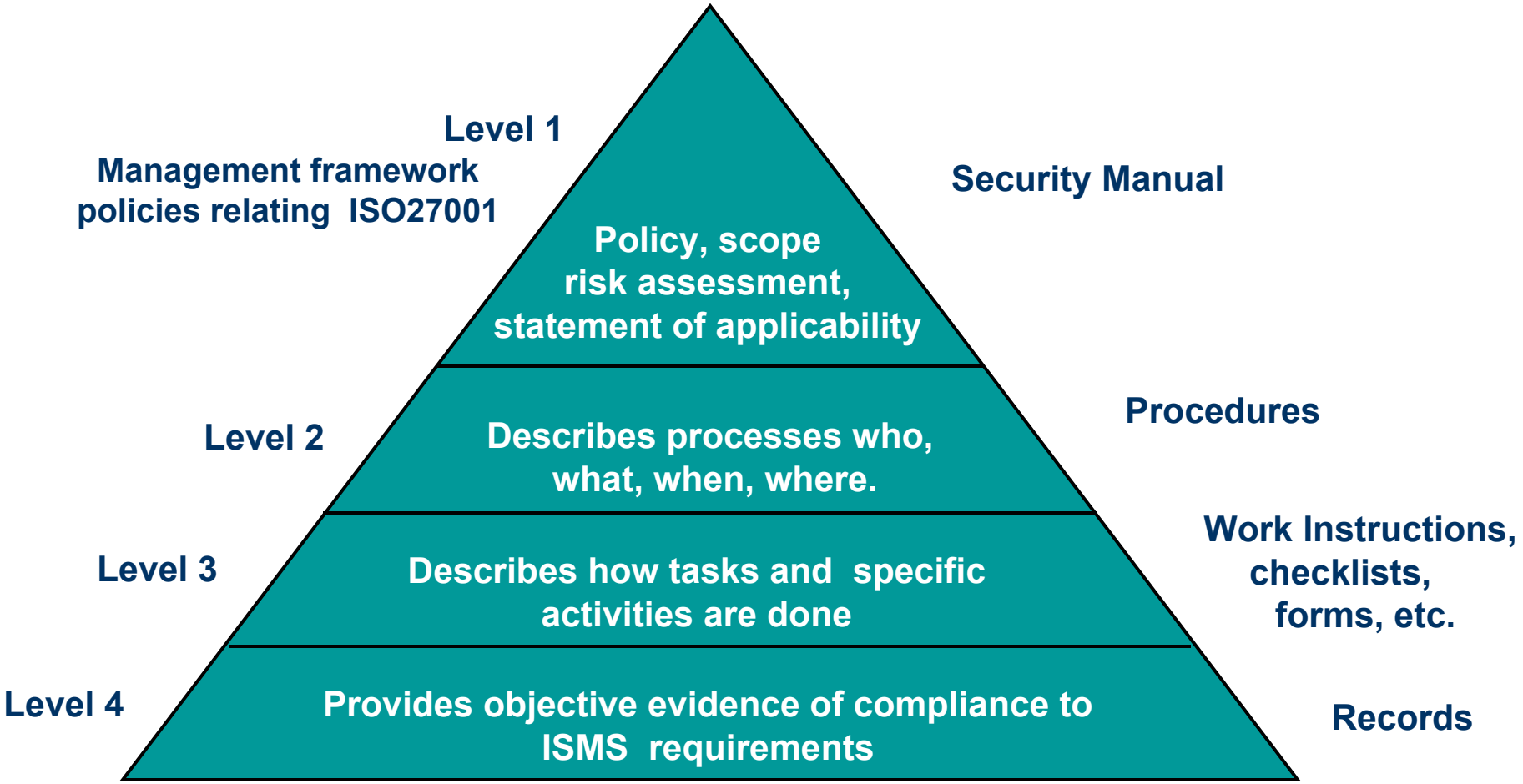
By its nature of being a ‘selective’ standard (i.e. apart from Security Policy, there are no mandatory controls), the requirement for a statement of applicability is essential.

The Statement of Applicability may be used by a customer to evaluate the information security management system.

The Statement of Applicability is the key document in the third party assessment process.

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

ISMS Documentation



FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Documentation Requirements

General

ISMS shall include:

- Documented security policy and objectives
- Scope of the ISMS
- Risk assessment report
- Risk treatment plan

Documentation Requirements

Documents needed for:

- Effective planning, operation & control
- Records
- Statement of Applicability (SoA)

[exclusions shall be recorded]

Control of Documents

Documented procedures shall be established to define the controls needed to:

- Approve documents for adequacy prior to issue
- Review and update as necessary & re-approve
- Changes & the current revision status of documents are identified
- Relevant versions of applicable documents are available at point of use

Control of Documents

- Legible and readily identifiable
- Documents of external origin are identified
- Distribution of documents is controlled
- Prevent the unintended use of obsolete documents
- Apply suitable identification if retained for any purpose

Control of Records

- Records established and maintained to provide evidence of conformity to requirements and to the effective operation of the ISMS shall be controlled
- Records may be manual or automatic

Control of Record

A documented procedure shall be established to define the controls need for:

- Identification, storage, protection, retrieval, retention time, disposition
- Legal requirements need to be considered & overseas?
- Records need to be: legible, readily identifiable and retrievable
- Performance of the process security incidents
- Extent of records – management decide

Management responsibility

Management commitment

Management shall provide evidence of its commitment by:

- Communicating the importance of meeting security objectives, legal & regulatory requirements and continual improvement
- Establishing – security policy, objectives & plans
- Conducting management reviews
- Deciding the level of residual risk

Management responsibility

Provision of resources – to:

- Set up and maintain the ISMS
- Security procedures support the business requirements
- Identify & address legal, regulatory and contractual requirements
- Adequate security of implemented controls,
- Carry out reviews
- Improve the process

Management responsibility

Training, Awareness and Competency

Personnel assigned responsibilities in the ISMS shall be *competent*.

- Provide training
- Evaluate effectiveness of training
- Ensure employees are aware
- Maintain records of education, experience and qualifications

Management Review of the ISMS

Top management shall review at planned intervals etc.

- Review input
- Review output

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Management Review of the ISMS

Internal ISMS Audits

- Management shall ensure audits are conducted at planned intervals

ISMS Improvements

Continual improvement

- Seek continual improvement
- Improve the effectiveness of the ISMS through:
    - Security policy
    - Security objectives
    - Results of security reviews
    - Security audits
    - Corrective actions
    - Preventive actions
    - Management review

ISMS Improvements

Corrective action

- Shall take actions to eliminate causes of nonconformities, in order to prevent recurrence.
- Documented procedure within the ISMS shall define:
  - Identifying nonconformities
  - Determining the causes
  - Evaluating the need for action to prevent re-occurrence
  - Determining & implementing corrective action
  - Recording the results
  - Reviewing actions for effectiveness

ISMS Improvements

Preventive action

- Determine actions to guard against future nonconformities
- Documented procedure shall define:

  Identifying potential nonconformities and their causes

  Determining & implementing preventive actions

  Recording the results

  Reviewing preventive actions taken

  Identifying changed risks

  Ensuring attention on significantly changed risks

Re-evaluating the system

The organization must realise that risk assessment and risk management are not one-off events and the ISMS must make clear in the management and operational procedures how the system is to be re-evaluated and updated.

Overview of Controls from ISO 27001

Control Objectives and Controls

‘Not all the controls described will be relevant to every situation, nor can they take account of local environmental or technological constraints, or be present in a form that suits every potential user in an organization’.

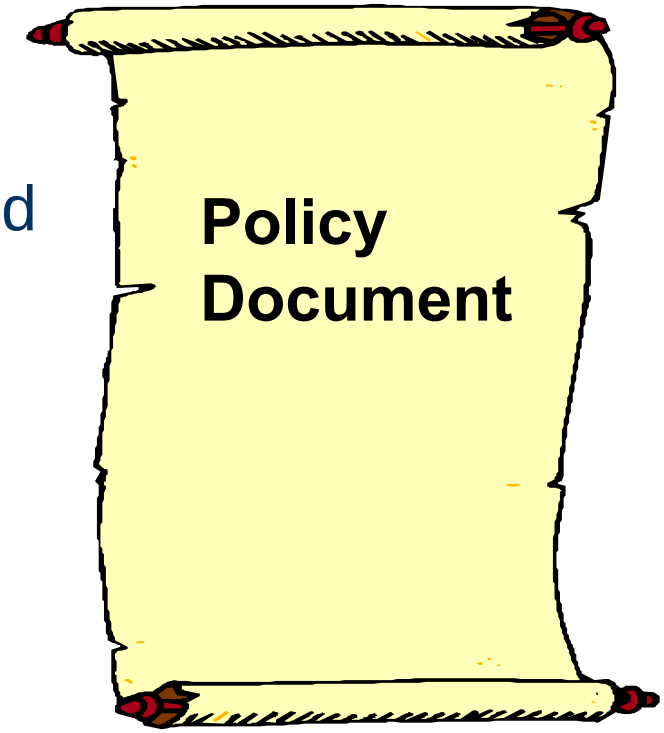
ISO 27001 CONTROLS

- Security Policy
- Organisation of Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Info sys acquisition, development & maintenance
- Information security incident management
- Business Continuity Management
- Compliance

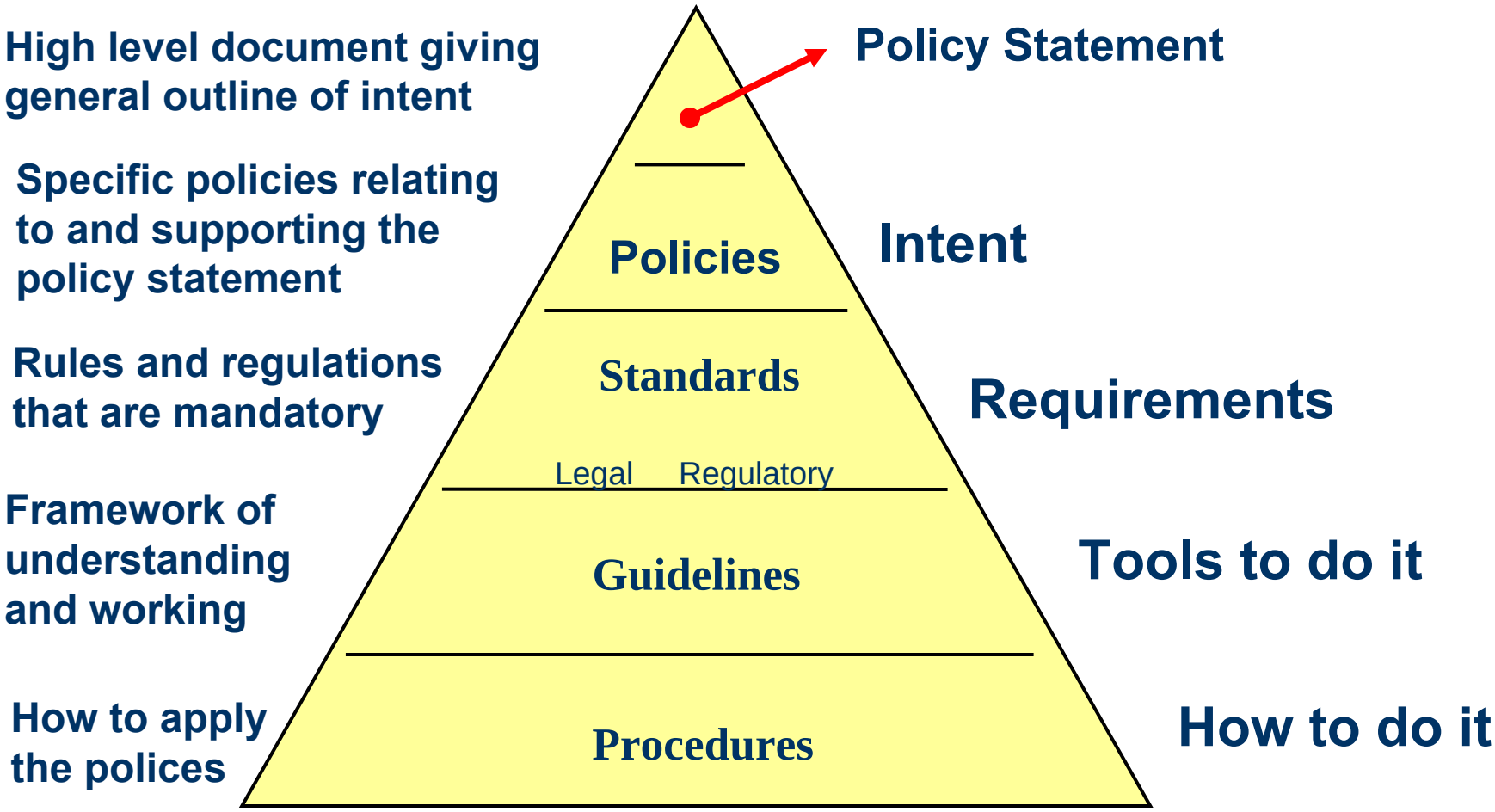
Information Security Policy Document

Objective –

To provide management direction and support for information security.



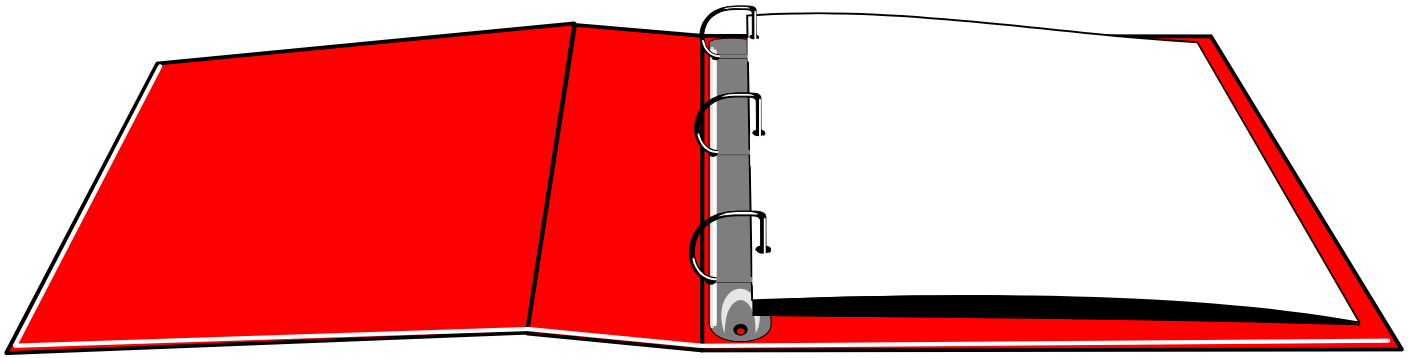
FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER



FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Security Policy

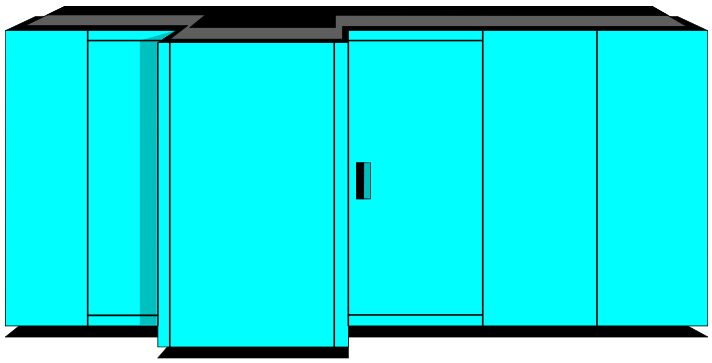
- Essential
- Without this the security will be fragmented and most likely ineffective (and will not meet the requirements of ISO 27001)



FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Requirement

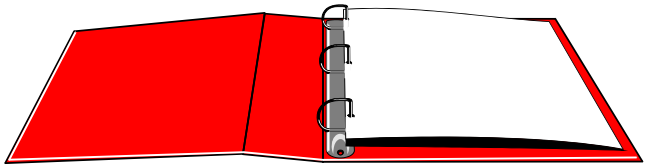
- Policy should leave no doubt that every individual member of staff will be held accountable under the policy



FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Policy types

- Small organizations may only need one policy.
- Large organizations may need different ones for different parts of the organization or even different systems.



Policy Content

- Simple and to-the-point
- Top-level policy on one sheet of paper
- Lower level policy available to all

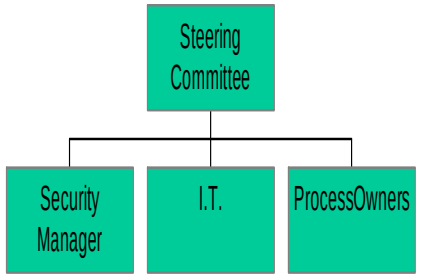
FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

ISO 27001 CONTROLS

- **Organisation of Information Security:**

  - **To manage information security within the organization.**
  - **To maintain the security of the organization information and information processing facilities that are accessed by external parties.**

Information Security Infrastructure

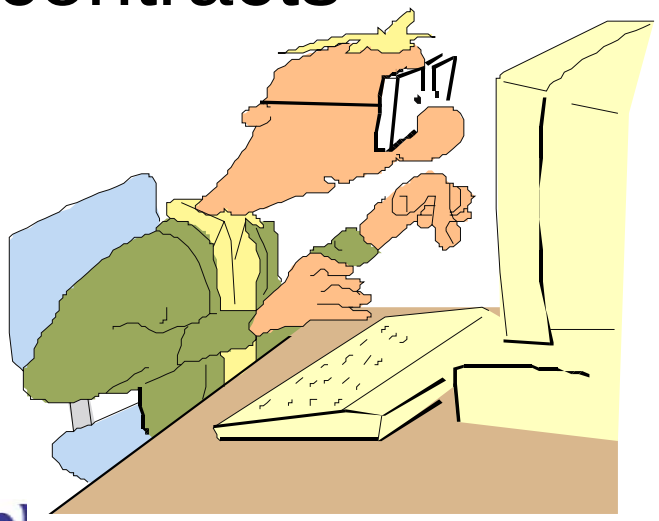


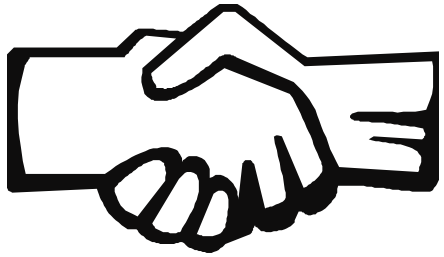
- Management information security forum
- Information security co-ordination
- Allocation of information security responsibilities
- Authorisation process for information processing facilities
- Specialist information security advice
- Co-operation between organizations
- Independent review of information security

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Security of Third Party Access

- Identification of risks from third party access
- Security requirements in third party contracts

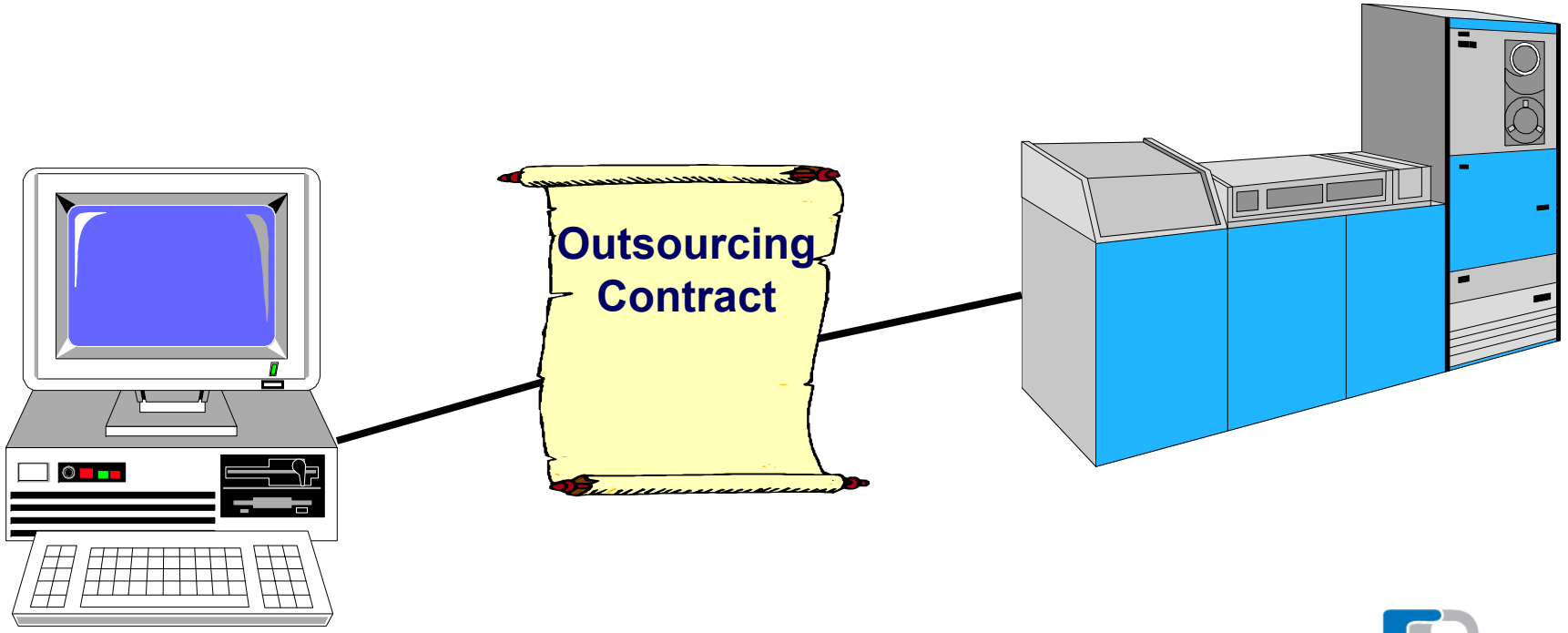




FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Outsourcing

- Security requirements in outsourcing contracts



FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

ISO 27001 CONTROLS

- **Asset Management:**
  - **To achieve and maintain appropriate protection of organizational assets.**
  - **To ensure that information receives an appropriate level of protection.**

Asset Classification and Control

Objective:

To maintain appropriate protection of organizational assets

- Accountability for assets
- Information classification

Assets

What are assets?

Must be those relevant to the scope of the Information Security Management System

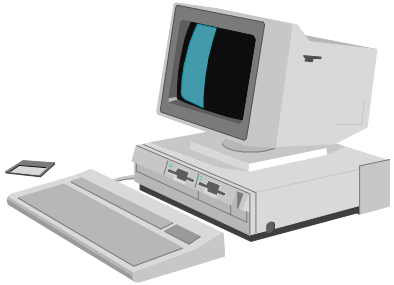
Assets

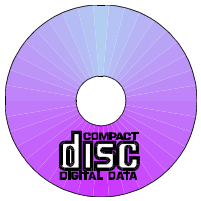
An Asset is something an organization assigns value to, examples include:

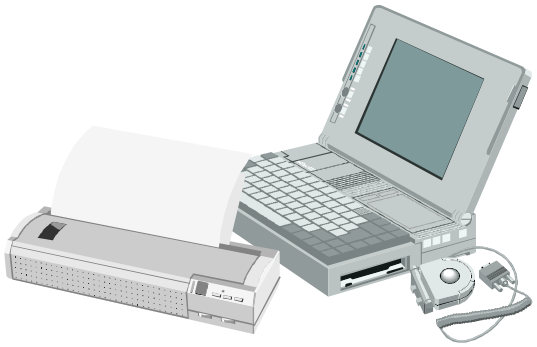
- Information assets
- Paper documents
- Software assets
- Physical assets
- People
- Company image and reputation
- Services

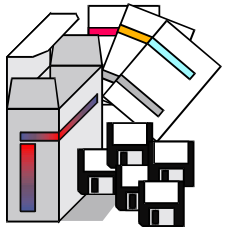
Accountability for Assets

Inventory of assets







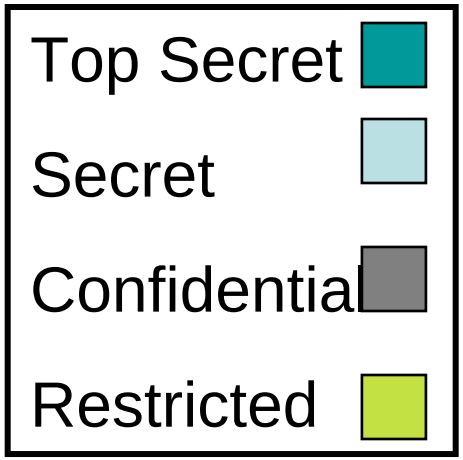


FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Information Classification

- Classification guidelines
- Information labelling and handling

‘Protectively Marked’



ISO 27001 CONTROLS

- **Human Resources Security:**

  - **Prior to employment.**
  - **During employment.**
  - **Termination or change of employment.**

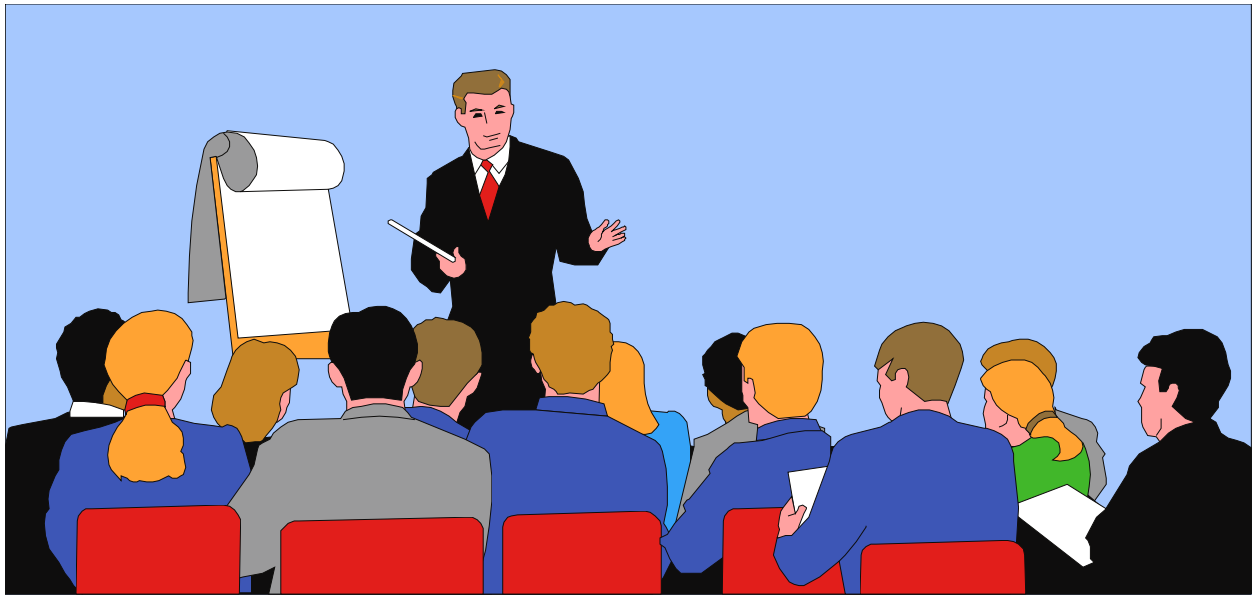
Security in Job Definition and Resourcing

- Including security in job responsibilities
- Personnel screening and policy
- Confidentiality agreements
- Terms and conditions of employment

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

User Training

- Information security education and training



ISO 27001 CONTROLS

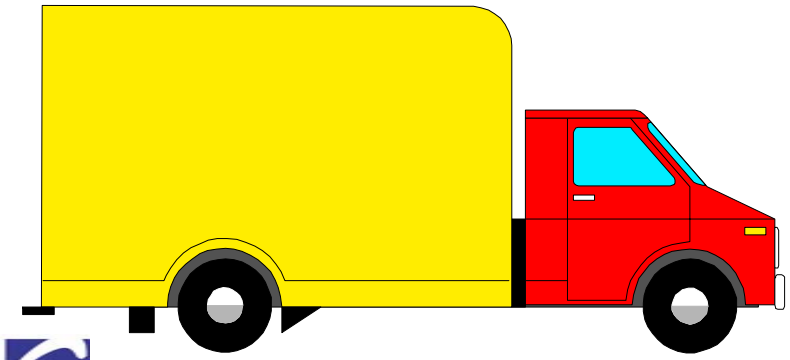
- **Physical and Environmental Security:**

  - **To prevent unauthorized physical access, damage and interference to the organizations premises and information.**
  - **To prevent loss, damage, theft or compromise of assets and interruption to the organization activities.**

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Secure Areas

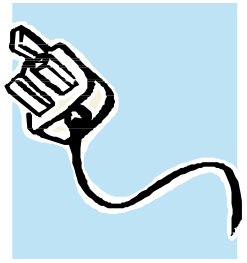
- Physical security perimeter
- Physical entry controls
- Securing offices, rooms and facilities
- Working in secure areas
- Isolated delivery and loading areas



FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Equipment Security

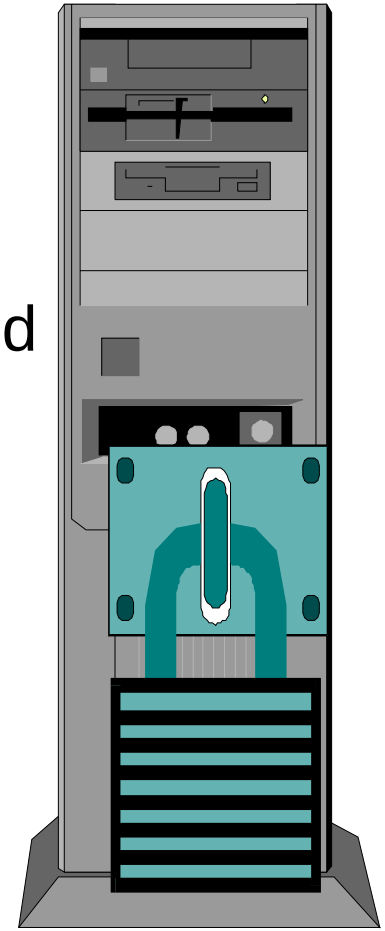
- Equipment siting and protection
- Power supplies
- Cabling security
- Equipment maintenance
- Security of equipment off-premises
- Secure disposal or re-use of equipment



FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Controls

- PCs can be stolen
- Fileservers are not much bigger
- Physical access controls may be required
- Visitors/contractors may need escorting



FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

General Controls

- Clear desk and clear screen policy
- Removal of property

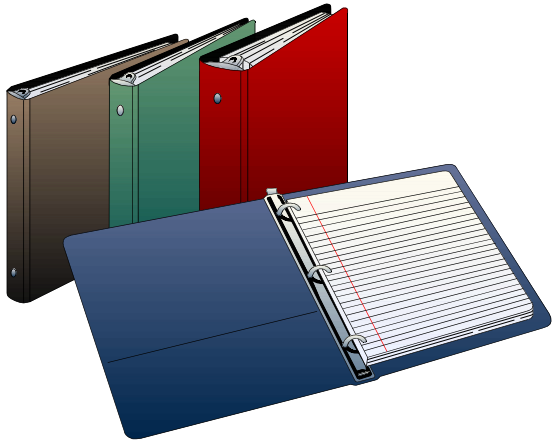
FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

ISO 27001 CONTROLS

- **Communications and Operations Management:**
  - **Operational procedures and responsibilities.**
  - **Third party service delivery management.**
  - **System planning and acceptance.**
  - **Protection against malicious and mobile code.**
  - **Back-up.**
  - **Network security management.**
  - **Media handling.**
  - **Exchange of information.**
  - **Electronic commerce services.**
  - **Monitoring.**

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Operational Procedures and Responsibilities

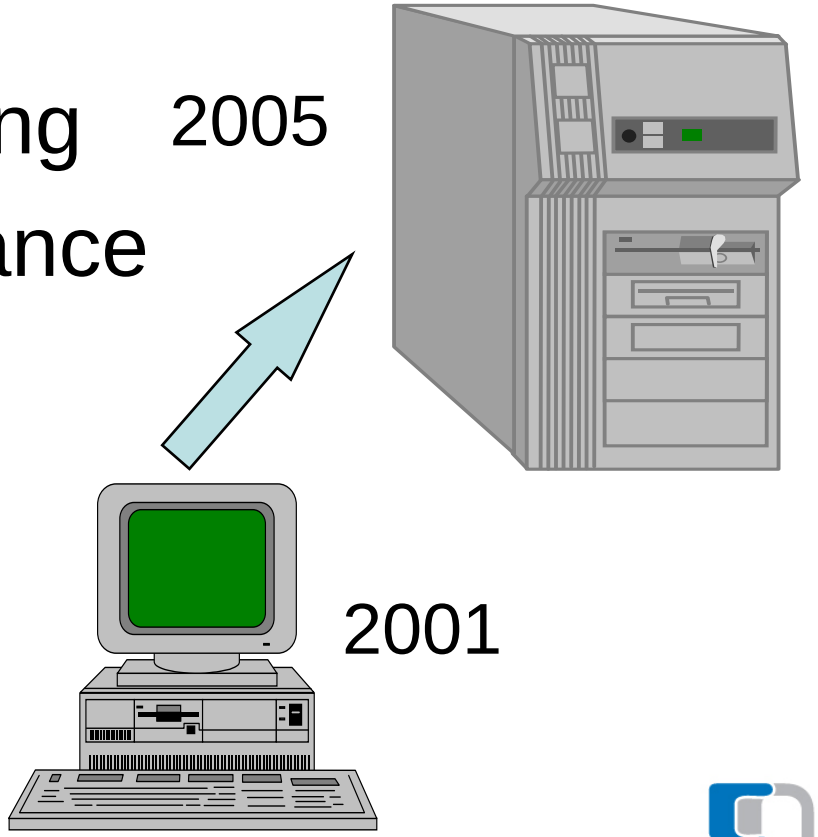


- Documented operating procedures
- Operational change control
- Incident management procedures
- Segregation of duties
- Separation of development and operational facilities
- External facilities management

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

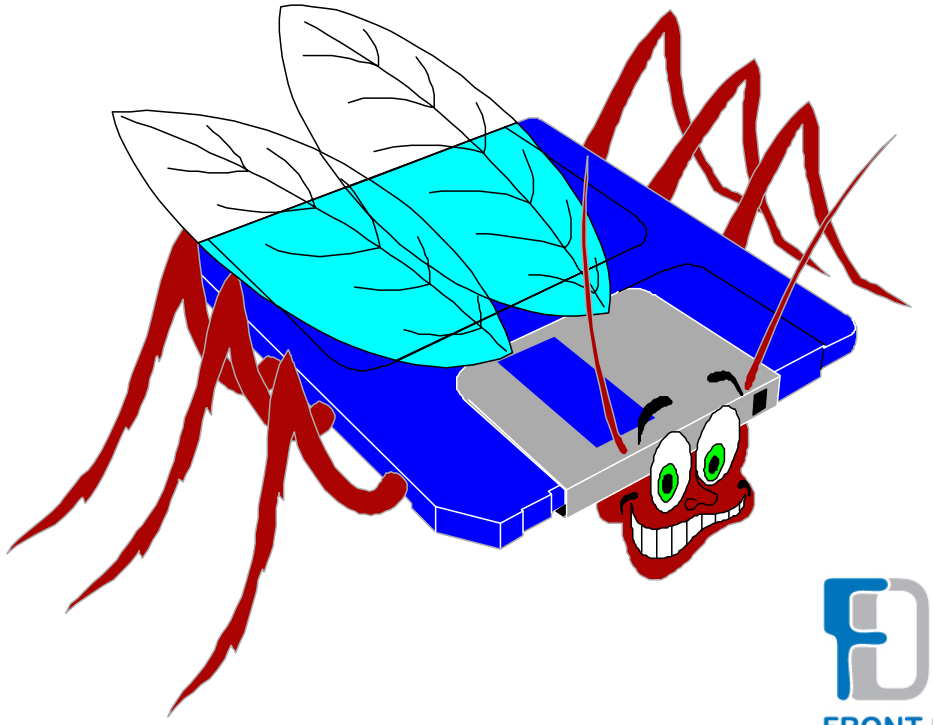
System Planning and Acceptance

- Capacity planning
- System acceptance



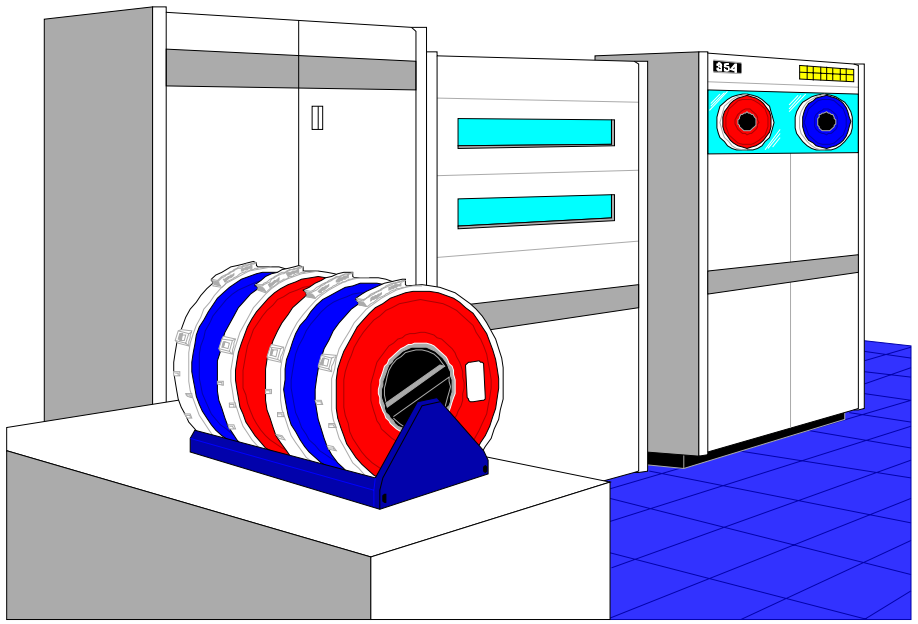
Protection Against Malicious Software

- Controls against malicious software



Housekeeping

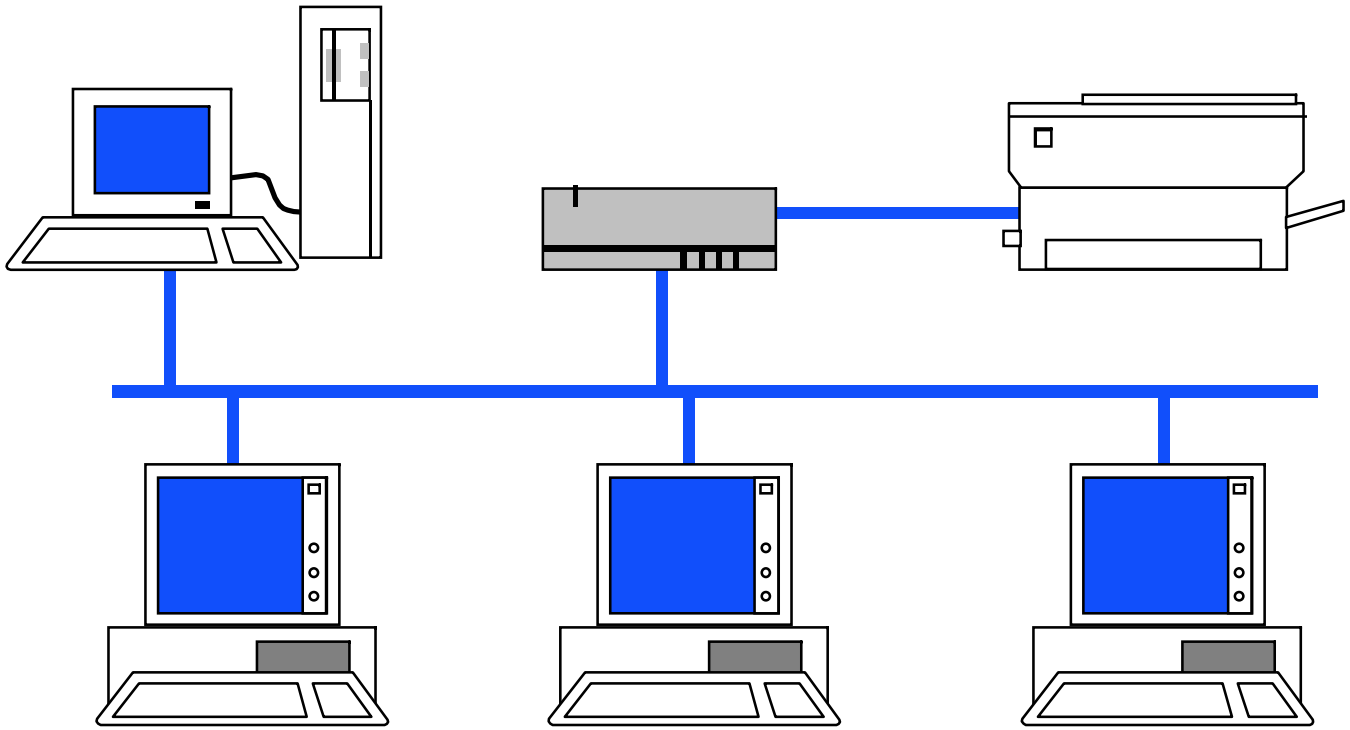
- Information back-up
- Operator logs
- Fault logging



FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

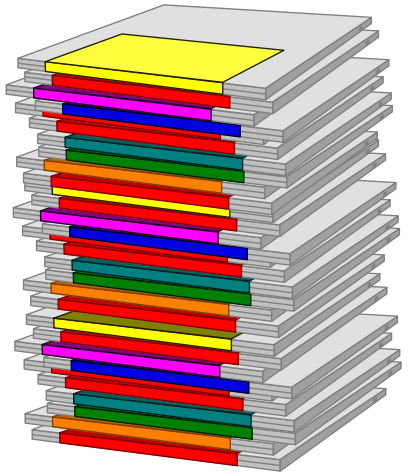
Network Management

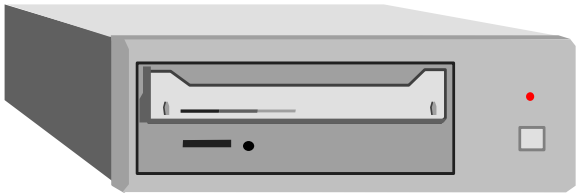
- Network controls



Media Handling and Security

- Management of removable computer media
- Disposal of media
- Information handling procedures
- Security of system documentation

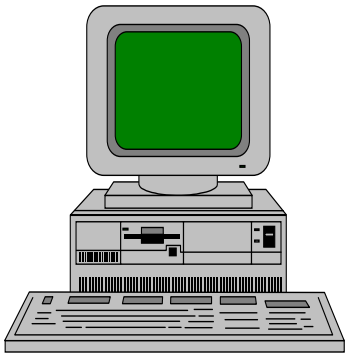


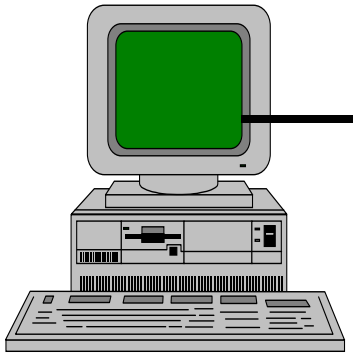


FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Exchanges of Information and Software

- Information and software exchange
- Security of media in transit
- Electronic commerce security
- Security of electronic mail
- Security of electronic office systems
- Publicly available systems
- Other forms of information exchange





FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Controls
e.g. Software patches

- Software patches are frequently released to correct software bugs and/or to plug potential security weaknesses discovered.
- They are often free and may be downloaded from supplier's web site.
- Organizations often ignore these.

Note: Loading a patch may cause a problem if not tested for compatibility with other software.

Importance of back-ups for operating systems, applications and data.

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

ISO 27001 CONTROLS

- **Access Control:**
  - **Business requirement for access control.**
  - **User access management.**
  - **User responsibilities.**
  - **Network access control.**
  - **Operating system access control.**
  - **Application and information access control.**
  - **Mobile computing and teleworking.**

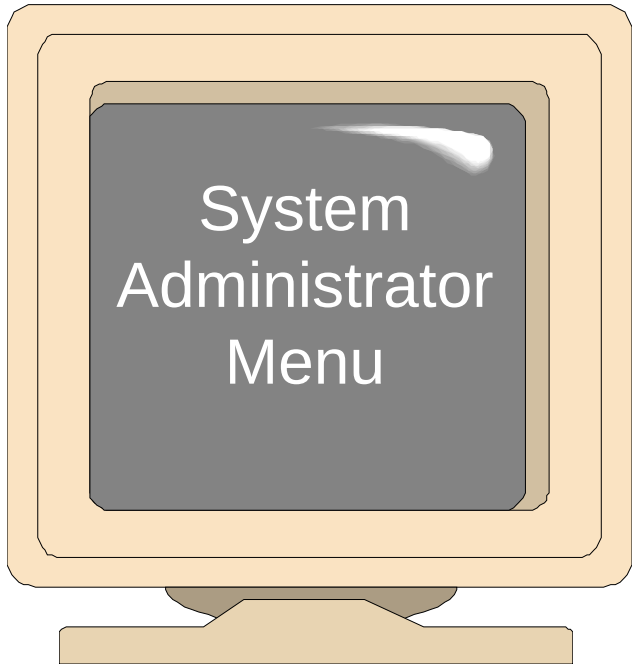
Business Requirements for Access Control

- Access control policy

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

User Access Management

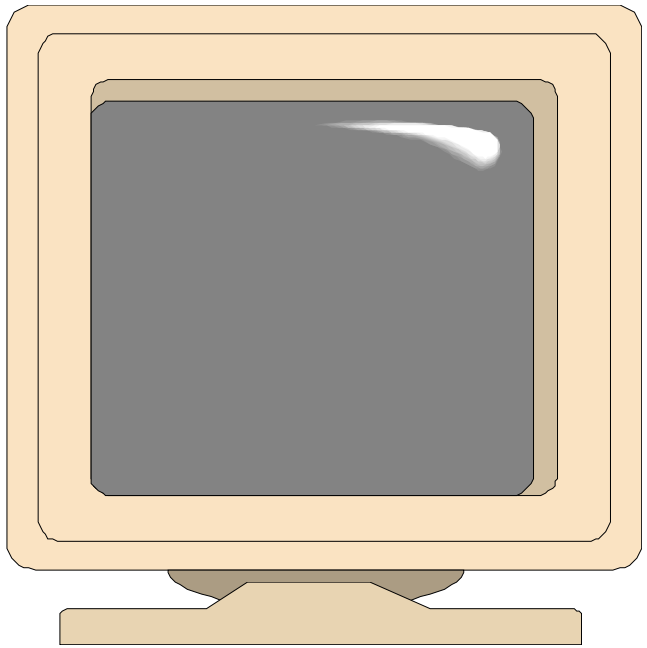
- User registration
- Privilege management
- User password management
- Review of user access rights



FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

User Responsibilities

- Password use
- Unattended user equipment



Network Access Control

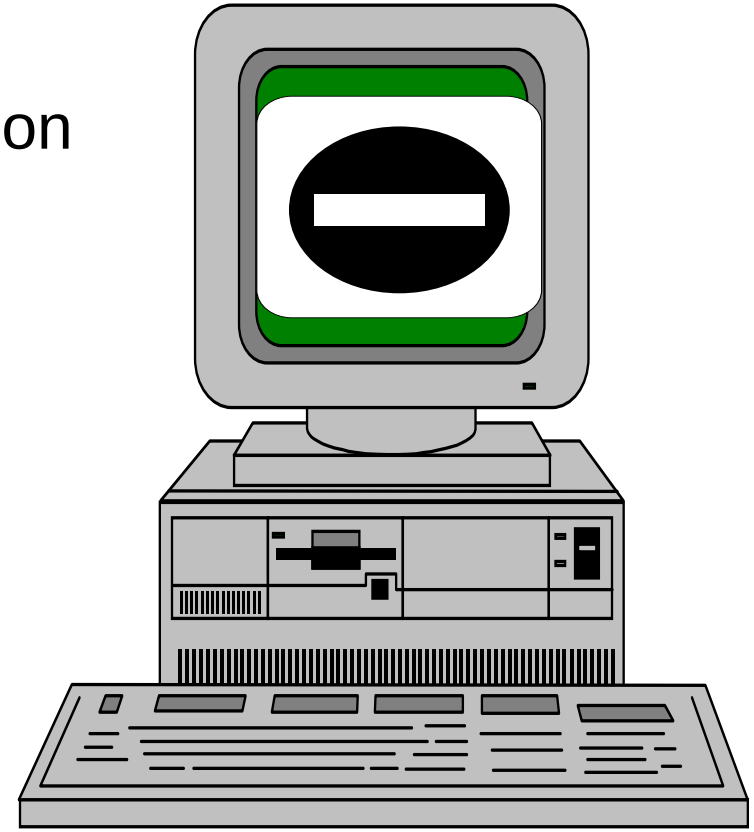
- Policy on use of network services
- Enforced path
- User authentication for external connections
- Node authentication
- Remote diagnostic port protection
- Segregation in networks
- Network connection control
- Network routing control
- Security of network services

Operating System Access Control

- Automatic terminal identification
- Terminal log-in procedures
- User identification and authentication
- Password management system
- Use of system facilities
- Duress alarm to safeguard users
- Terminal time-out
- Limitation of connection time

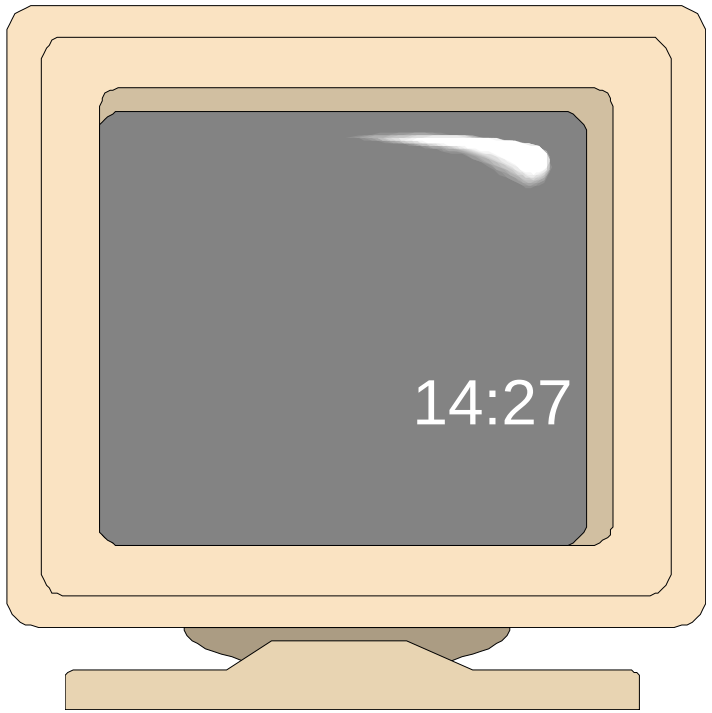
Application Access Control

- Information access restriction
- Sensitive system isolation



Monitoring System Access and Use

- Event logging
- Monitoring system use
- Clock synchronisation



FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Mobile Computing and Teleworking

- Mobile computing
- Teleworking

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

ISO 27001 CONTROLS

- **Info sys acquisition, development & maintenance**

  - **Security requirements of information systems.**
  - **Correct processing in applications.**
  - **Cryptographic controls.**
  - **Security of system files.**
  - **Security in development and support processes.**
  - **Technical Vulnerability Management.**

Security Requirements of Systems

- Security requirements analysis and specification

Specification

;oiu;u;p’pjoiu;oiuiu;iou;oiu;oiuoipoipo

#po#po#[po#[po[po#[po[pophn ji

Hhhuhiu hiuyhuy8

J o’oiiuyfuytdyiuy;9uyouo;iui j;oij;

Ijijweifjerhf

uuhiuyrhqe wu24i5yiufu24

O#popo[po[ppo[po#[o#o#o#[o#o#o#h ilugiuiugi

O[popo[po[po

Business Case

;oiu;u;p’pjoiu;oiuiu;iou;oiu;oiuoipoipo

#po#po#[po#[po[po#[po[pophn ji

Hhhuhiu hiuyhuy8 iouo;iu;oiruoi

J o’oiiuyfuytdyiuy;9uyouo;iui j;oij;

Ijijweifjerhf ;ij;oirj;qiruqoriqur;

uuhiuyrhqeii; io;iu wu24i5yiufu24

O#popo[po[ppo[po#[o#o#o#[o#o#o#h ilugiuiugi uoiuoi iouoiu;oiu;o9iu

O[popo[po[pou;oi

Security Requirements

;oiu;u;p’pjoiu;oiuiu;iou;oiu;oiuoipoi po

#po#po#[po#[po[po#[po[pophn ji

Hhhuhiu hiuyhuy8 iouo;iu;oiruoi

J o’oiiuyfuytdyiuy;9uyouo;iui j;oij;

Ijijweifjerhf ;ij;oirj;qiruqoriqur;

uuhiuyrhqeii; io;iu wu24i5yiufu24

O#popo[po[ppo[po#[o#o#o#[o#o#o #hilugiuiugi uoiuoi iouoiu;oiu;o9iu

O[popo[po[pou;oi

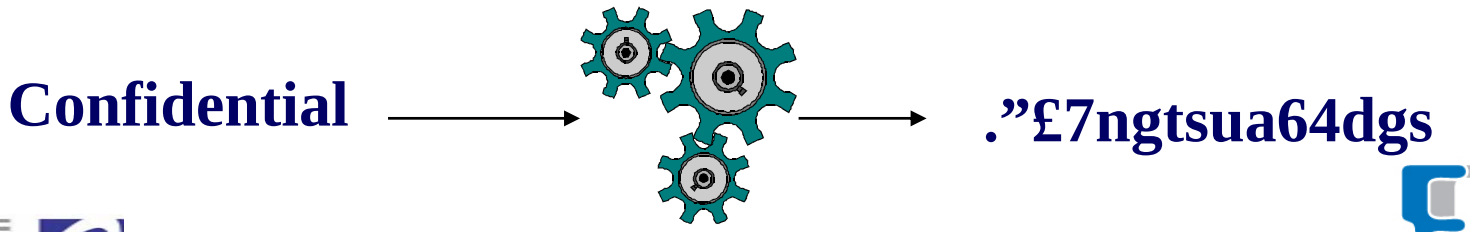
FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Security in Application Systems

- Input data validation
- Control of internal processing
- Message authentication
- Output data validation

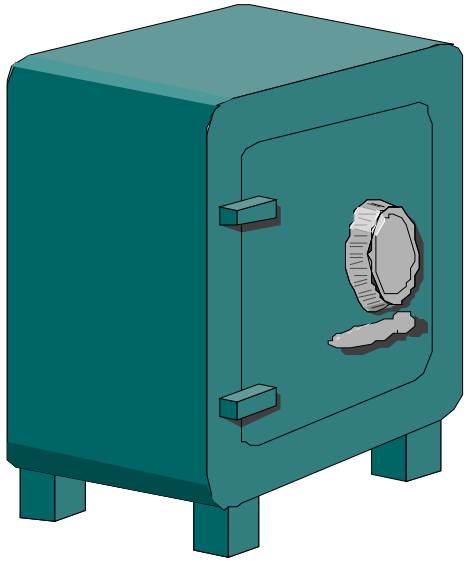
Cryptographic Controls

- Policy on use of cryptographic controls
- Encryption
- Digital signatures
- Non-repudiation services
- Key management



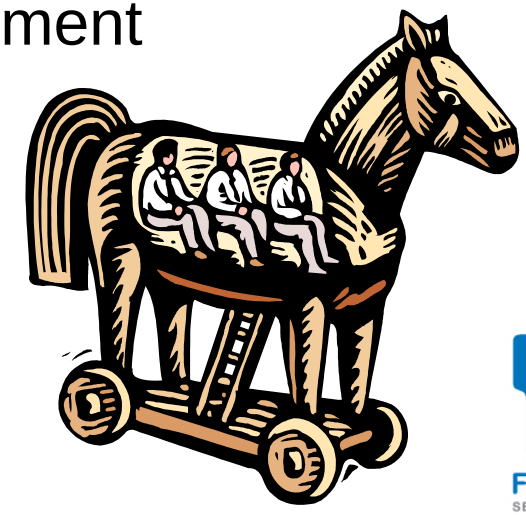
Security of System Files

- Control of operational software
- Protection of system test data
- Access control to program source library



Security in Development and Support Processes

- Change control procedures
- Technical review of operating system changes
- Restrictions on changes to software packages
- Covert channels and Trojan code
- Outsourced software development



FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

ISO 27001 CONTROLS

- **Information security incident management**

  - **Reporting information security events and weaknesses.**
  - **Management of information security incidents and improvements.**

Reporting Security Incidents

Objective:

To minimize the damage from security incidents and malfunctions and to monitor and learn from such incidents

- Definition
- Procedure

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Responding to Security Incidents and Malfunctions

- Reporting security incidents
- Reporting security weaknesses
- Reporting software malfunctions
- Learning from incidents
- Disciplinary process

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

ISO 27001 CONTROLS

- **Business continuity management:**

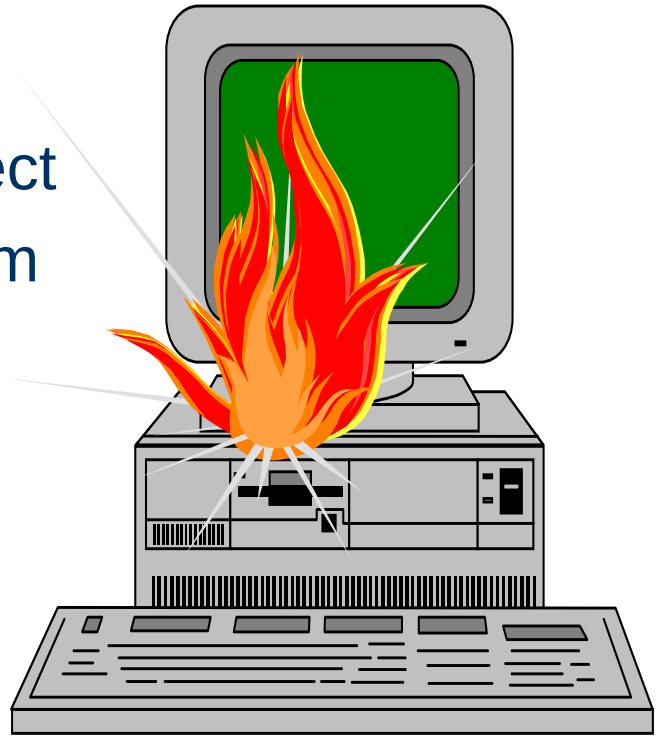
  - **To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.**

Business Continuity Management

Objective –

To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

- Key steps to business continuity



FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Aspects of Business Continuity Management

- Business continuity management process
- Business continuity and impact analysis
- Writing and implementing continuity plans
- Business continuity planning framework
- Testing, maintaining and re-assessing business continuity plans

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

ISO 27001 CONTROLS

- **Compliance:**

  - **Compliance with legal requirements.**
  - **Compliance with security policies and standards, and technical compliance.**
  - **Information systems audit considerations.**

Compliance with Legal Requirements

- Identification of applicable legislation
- Intellectual property rights (IPR)
- Safeguarding of organizational records
- Data protection and privacy of personnel information
- Prevention of misuse of information processing facilities
- Regulation of cryptographic controls
- Collection of evidence

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Intellectual Property Rights

Objective -

To avoid breaches of copyright through prevention of copying without owner's consent.

- Restrictions on copying
- License agreements
- Policy compliance
- Contract requirements

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Safeguarding of Organizational Records

Objective –

Prevention of loss, destruction and falsification of important records.

- Retention
- Storage
- Disposal

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Data Protection and Privacy of Personal Information

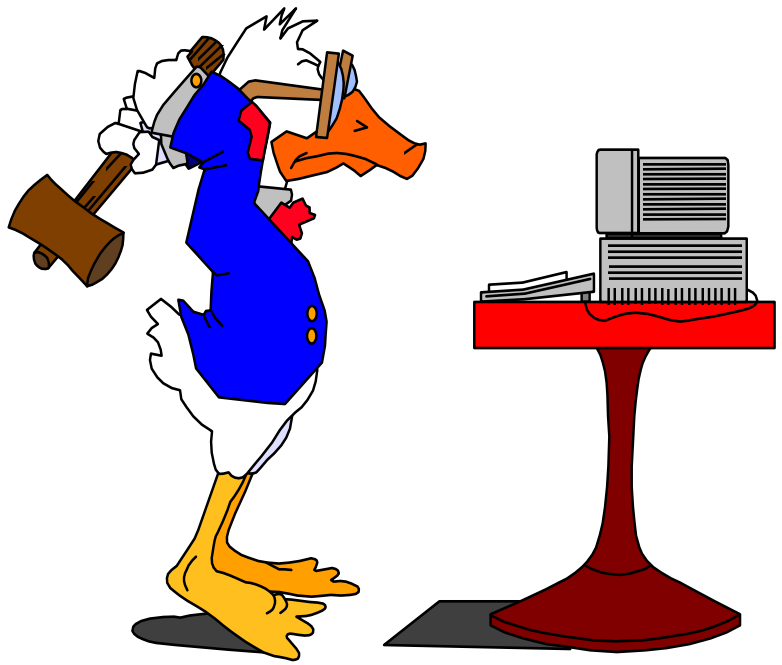
Objective –

Compliance with Data Protection Legislation in those countries where applicable.

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Prevention of Misuse of Information Processing Facilities

- Use of e-mail and the world wide web
- Use of system and information for private work
- Loading up personal software



FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Regulation of Cryptographic Controls

- Consideration of national and international laws
- Business case to define their use
- Good key management controls required

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Evidence

- Legal requirements, software, data protection
- Operator/user logs
- Security reviews
- Housekeeping

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Reviews of Security Policy and Technical Compliance

- Compliance with security policy
- Technical compliance checking

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

System Audit Considerations

- System audit controls
- Protection of system audit tools

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Note

'Not all the controls described will be relevant to every situation, nor can they take account of local environmental or technological constraints, or be present in a form that suits every potential user in an organization'

Assessment and Certification

- **The Process**
- **Maintenance**

Assessment Stages

Pre-assessment (optional)

Documentation Audit

Implementation Audit

Pre-certification

Continuing Assessment

3-Year Re-assessment

Post-certification

CERTIFICATION BENEFITS

- **Opportunity to identify and fix weaknesses**
- **Senior Management take ownership of information Security**
- **Provides confidence to trading partners and customers**
- **Focused staff responsibilities**
- **Independent review of your information Security Management System**

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

GLOBAL REGISTRATIONS

Japan	1080*	Czech Republic	6	Bahrain	1
UK	215	Poland	5	Chile	1
India	131	Spain	5	Colombia	1
Taiwan	64	Brazil	4	Egypt	1
Germany	48	Greece	4	France	1
Italy	40	Iceland	4	Lebanon	1
Korea	35	Argentina	3	Lithuania	1
USA	26	Kuwait	3	Luxemburg	1
Netherlands	22	Mexico	3	Macau	1
China	18	Saudi Arabia	3	Macedonia	1
Hong Kong	18	UAE	3	Morocco	1
Australia	17	Belgium	2	Qatar	1
Finland	15	Canada	2	Romania	1
Hungary	14	Croatia	2	Russian Federation	1
Ireland	11	Denmark	2	Slovenia	1
Norway	11	Isle of Man	2	South Africa	1
Singapore	11	Malaysia	2	Turkey	1
Austria	8	Philippines	2	Total	1882
Switzerland	8	Slovak Republic	2		
Sweden	7	Thailand	2		

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

FRONT DEFENSE
SECURITY SOLUTIONS PROVIDER

Any Questions?

Thank you for your participation

Front Defense FZ LLC

Dubai Internet City

Tel: +971-4-367 6767, Fax: +971-4-368 8072

P.O Box 500419, Dubai - UAE

Email: info@frontdefense.com