

Principles and fundamentals of security methodologies of information systems - Information Security Policy

M2SSIC-Metz

Pascal Steichen

- 1 Information security policy
- 2 ISO/IEC 27002:2005
- 3 Control Framework
- 4 Producing the policy - good practices
- 5 Conclusion - summary

Information security policy

To protect its assets (information and systems) on a daily basis an organisation has to:

- organise its security by documenting the countermeasures or controls to protect the confidentiality, integrity and availability of the assets, in a security policy,

Information security policy

To protect its assets (information and systems) on a daily basis an organisation has to:

- organise its security by documenting the countermeasures or controls to protect the confidentiality, integrity and availability of the assets, in a security policy,
- with the prime goal to manage and reduce its risks.

Information security policy

To protect its assets (information and systems) on a daily basis an organisation has to:

- organise its security by documenting the countermeasures or controls to protect the confidentiality, integrity and availability of the assets, in a security policy,
- with the prime goal to manage and reduce its risks.

Asset anything that has value to the organization. ISO/IEC

Information security policy

To protect its assets (information and systems) on a daily basis an organisation has to:

- organise its security by documenting the countermeasures or controls to protect the confidentiality, integrity and availability of the assets, in a security policy,
- with the prime goal to manage and reduce its risks.

Asset anything that has value to the organization. ISO/IEC

Control means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature.
NOTE: Control is also used as a synonym for safeguard or countermeasure. ISO/IEC

An information security policy:

- defines the business rules, principles and standards defining the organisation's approach to managing information security,- provides management direction and support for information security in accordance with business requirements and relevant laws and regulations,

An information security policy:

- defines the business rules, principles and standards defining the organisation's approach to managing information security,- provides management direction and support for information security in accordance with business requirements and relevant laws and regulations,
- defines control objectives and controls intended to be implemented to meet the requirements identified by a risk assessment,

An information security policy:

- defines the business rules, principles and standards defining the organisation's approach to managing information security,- provides management direction and support for information security in accordance with business requirements and relevant laws and regulations,
- defines control objectives and controls intended to be implemented to meet the requirements identified by a risk assessment,
- needs approval by the highest level of management.

why is an ISP important ?

Because an information security policy:

- is reference base for information traitement rules and practices,

why is an ISP important ?

Because an information security policy:

- is reference base for information traitement rules and practices,
- provides management support, and is published and communicated to all employees and relevant external parties,

why is an ISP important ?

Because an information security policy:

- is reference base for information traitement rules and practices,
- provides management support, and is published and communicated to all employees and relevant external parties,
- provides a structured and methodical approach to information security,

why is an ISP important ?

Because an information security policy:

- is reference base for information traitement rules and practices,
- provides management support, and is published and communicated to all employees and relevant external parties,
- provides a structured and methodical approach to information security,
- integrates the "business" dimension,

why is an ISP important ?

Because an information security policy:

- is reference base for information traitement rules and practices,
- provides management support, and is published and communicated to all employees and relevant external parties,
- provides a structured and methodical approach to information security,
- integrates the "business" dimension,
- takes into account humans, organisational as well as technical aspects,

why is an ISP important ?

Because an information security policy:

- is reference base for information traitement rules and practices,
- provides management support, and is published and communicated to all employees and relevant external parties,
- provides a structured and methodical approach to information security,
- integrates the "business" dimension,
- takes into account humans, organisational as well as technical aspects,
- is based on the real operational situation of the organisation,

why is an ISP important ?

Because an information security policy:

- is reference base for information traitement rules and practices,
- provides management support, and is published and communicated to all employees and relevant external parties,
- provides a structured and methodical approach to information security,
- integrates the "business" dimension,
- takes into account humans, organisational as well as technical aspects,
- is based on the real operational situation of the organisation,
- limits costs and optimises ROI.

beforehand...

It is essential that an organization identifies its security requirements. There are three main sources of security requirements:

- One source is derived from assessing risks to the organization :

$$\textit{Risk} = \textit{Vulnerability} * \textit{Threat} * \textit{Impact}$$

beforehand...

It is essential that an organization identifies its security requirements. There are three main sources of security requirements:

- One source is derived from assessing risks to the organization :

$$Risk = Vulnerability * Threat * Impact$$

- Another source is the legal, statutory, regulatory, and contractual requirements that an organization, its trading partners, contractors, and service providers have to satisfy, and their socio-cultural environment.

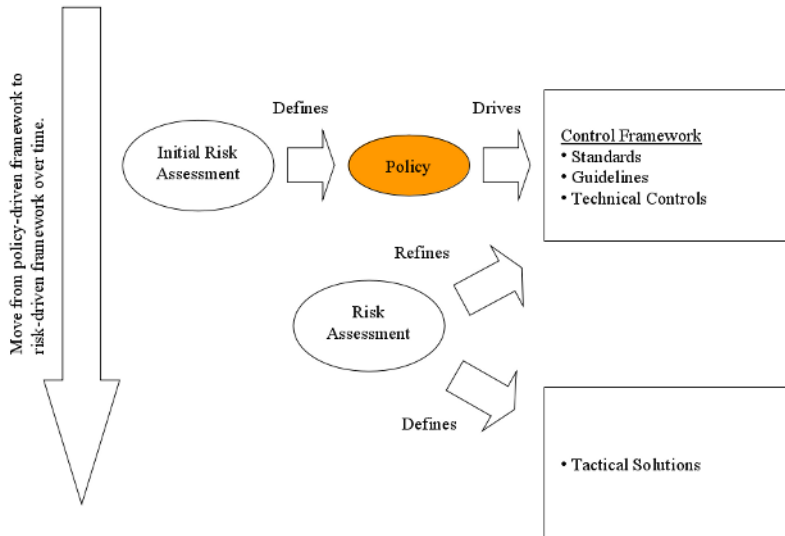
beforehand...

It is essential that an organization identifies its security requirements. There are three main sources of security requirements:

- One source is derived from assessing risks to the organization :

$$Risk = Vulnerability * Threat * Impact$$

- Another source is the legal, statutory, regulatory, and contractual requirements that an organization, its trading partners, contractors, and service providers have to satisfy, and their socio-cultural environment.
- A further source is the particular set of principles, objectives and business requirements for information processing that an organization has developed to support its operations.



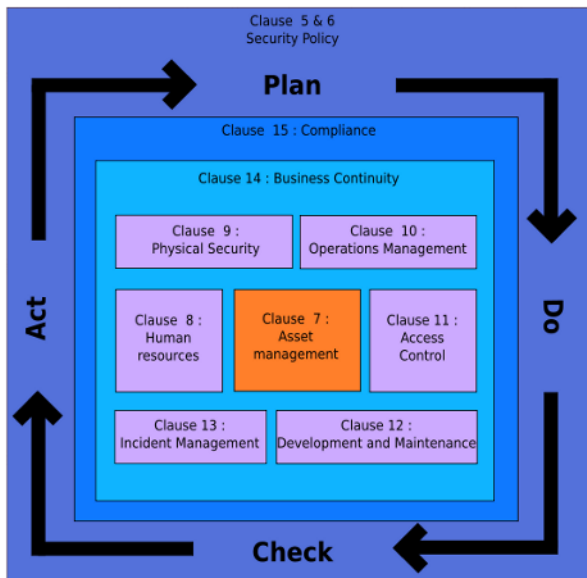
ISO/IEC 27002:2005

THE reference document about information security policies is the ISO/IEC 27002:2005 - "Information technology — Security techniques — Code of practice for information security management" (formerly known as ISO/IEC 17799 and BS7799).

Scope

"This International Standard establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined in this International Standard provide general guidance on the commonly accepted goals of information security management."

"The control objectives and controls of this International Standard are intended to be implemented to meet the requirements identified by a risk assessment. This International Standard may serve as a practical guideline for developing organizational security standards and effective security management practices and to help build confidence in inter-organizational activities."



Security Policy

The policy document should contain statements concerning:

- a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing;

Security Policy

The policy document should contain statements concerning:

- a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing;
- a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives;

Security Policy

The policy document should contain statements concerning:

- a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing;
- a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives;
- a framework for setting control objectives and controls, including the structure of risk assessment and risk management;

- a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization

- a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization
 - compliance with legislative, regulatory, and contractual requirements;

- a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization
 - compliance with legislative, regulatory, and contractual requirements;
 - security education, training, and awareness requirements;

- a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization
 - compliance with legislative, regulatory, and contractual requirements;
 - security education, training, and awareness requirements;
 - business continuity management;

- a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization
 - compliance with legislative, regulatory, and contractual requirements;
 - security education, training, and awareness requirements;
 - business continuity management;
 - consequences of information security policy violations;

- a definition of general and specific responsibilities for information security management, including reporting information security incidents;

- a definition of general and specific responsibilities for information security management, including reporting information security incidents;
- references to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with.

- a definition of general and specific responsibilities for information security management, including reporting information security incidents;
- references to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with.
- and get periodic or if significant changes occur reviews.

Organizing Information Security

- Management commitment to information security

Organizing Information Security

- Management commitment to information security
- Information security co-ordination (CISO/RSSI)

Organizing Information Security

- Management commitment to information security
- Information security co-ordination (CISO/RSSI)
- Allocation of information security responsibilities (data owners)

Organizing Information Security

- Management commitment to information security
- Information security co-ordination (CISO/RSSI)
- Allocation of information security responsibilities (data owners)
- Confidentiality or non-disclosure agreements (reflecting the organization's needs)

Organizing Information Security

- Management commitment to information security
- Information security co-ordination (CISO/RSSI)
- Allocation of information security responsibilities (data owners)
- Confidentiality or non-disclosure agreements (reflecting the organization's needs)
- Contact with authorities and special interest groups

Organizing Information Security

- Management commitment to information security
- Information security co-ordination (CISO/RSSI)
- Allocation of information security responsibilities (data owners)
- Confidentiality or non-disclosure agreements (reflecting the organization's needs)
- Contact with authorities and special interest groups
- Independent review of information security

Organizing Information Security

- Management commitment to information security
- Information security co-ordination (CISO/RSSI)
- Allocation of information security responsibilities (data owners)
- Confidentiality or non-disclosure agreements (reflecting the organization's needs)
- Contact with authorities and special interest groups
- Independent review of information security
- External parties (customers, partners, third parties...)

Asset Management

- Responsibility for assets

Asset Management

- Responsibility for assets
- Information classification

Human Resources Security

- Roles and responsibilities

Human Resources Security

- Roles and responsibilities
- Screening

Human Resources Security

- Roles and responsibilities
- Screening
- Terms and conditions of employment

Human Resources Security

- Roles and responsibilities
- Screening
- Terms and conditions of employment
- Information security awareness, education, and training

Human Resources Security

- Roles and responsibilities
- Screening
- Terms and conditions of employment
- Information security awareness, education, and training
- Disciplinary process

Human Resources Security

- Roles and responsibilities
- Screening
- Terms and conditions of employment
- Information security awareness, education, and training
- Disciplinary process
- Termination

Human Resources Security

- Roles and responsibilities
- Screening
- Terms and conditions of employment
- Information security awareness, education, and training
- Disciplinary process
- Termination
 - Return of assets

Human Resources Security

- Roles and responsibilities
- Screening
- Terms and conditions of employment
- Information security awareness, education, and training
- Disciplinary process
- Termination
 - Return of assets
 - Removal of access rights

Physical and Environmental Security

- Physical security perimeter and areas

Physical and Environmental Security

- Physical security perimeter and areas
- Equipment security

Physical and Environmental Security

- Physical security perimeter and areas
- Equipment security
 - Security of equipment off-premises

Physical and Environmental Security

- Physical security perimeter and areas
- Equipment security
 - Security of equipment off-premises
 - Secure disposal or re-use of equipment

Communications and Operations Management

- Change management

Communications and Operations Management

- Change management
- Separation of development, test, and operational facilities

Communications and Operations Management

- Change management
- Separation of development, test, and operational facilities
- Third party service delivery management

Communications and Operations Management

- Change management
- Separation of development, test, and operational facilities
- Third party service delivery management
- Protection against malicious and mobile code

Communications and Operations Management

- Change management
- Separation of development, test, and operational facilities
- Third party service delivery management
- Protection against malicious and mobile code
- Back-up

Communications and Operations Management

- Change management
- Separation of development, test, and operational facilities
- Third party service delivery management
- Protection against malicious and mobile code
- Back-up
- Network security management

Communications and Operations Management

- Change management
- Separation of development, test, and operational facilities
- Third party service delivery management
- Protection against malicious and mobile code
- Back-up
- Network security management
- Management of removable media

Communications and Operations Management

- Change management
- Separation of development, test, and operational facilities
- Third party service delivery management
- Protection against malicious and mobile code
- Back-up
- Network security management
- Management of removable media
- Information exchange policies and procedures

Communications and Operations Management

- Change management
- Separation of development, test, and operational facilities
- Third party service delivery management
- Protection against malicious and mobile code
- Back-up
- Network security management
- Management of removable media
- Information exchange policies and procedures
- Electronic messaging

Communications and Operations Management

- Change management
- Separation of development, test, and operational facilities
- Third party service delivery management
- Protection against malicious and mobile code
- Back-up
- Network security management
- Management of removable media
- Information exchange policies and procedures
- Electronic messaging
- On-Line Transactions

Communications and Operations Management

- Change management
- Separation of development, test, and operational facilities
- Third party service delivery management
- Protection against malicious and mobile code
- Back-up
- Network security management
- Management of removable media
- Information exchange policies and procedures
- Electronic messaging
- On-Line Transactions
- Publicly available information

Communications and Operations Management

- Change management
- Separation of development, test, and operational facilities
- Third party service delivery management
- Protection against malicious and mobile code
- Back-up
- Network security management
- Management of removable media
- Information exchange policies and procedures
- Electronic messaging
- On-Line Transactions
- Publicly available information
- Monitoring

Access Control

- User access management

Access Control

- User access management
 - User password management

Access Control

- User access management
 - User password management
- Clear desk and clear screen policy

Access Control

- User access management
 - User password management
- Clear desk and clear screen policy
- Network access control

Access Control

- User access management
 - User password management
- Clear desk and clear screen policy
- Network access control
 - User authentication for external connections

Access Control

- User access management
 - User password management
- Clear desk and clear screen policy
- Network access control
 - User authentication for external connections
 - Segregation in networks

Access Control

- User access management
 - User password management
- Clear desk and clear screen policy
- Network access control
 - User authentication for external connections
 - Segregation in networks
- Operating system access control

Access Control

- User access management
 - User password management
- Clear desk and clear screen policy
- Network access control
 - User authentication for external connections
 - Segregation in networks
- Operating system access control
 - User identification and authentication

Access Control

- User access management
 - User password management
- Clear desk and clear screen policy
- Network access control
 - User authentication for external connections
 - Segregation in networks
- Operating system access control
 - User identification and authentication
 - Password management system

Access Control

- User access management
 - User password management
- Clear desk and clear screen policy
- Network access control
 - User authentication for external connections
 - Segregation in networks
- Operating system access control
 - User identification and authentication
 - Password management system
- Mobile computing and communications

Information Systems Acquisition, Development and Maintenance

- Security requirements analysis and specification

Information Systems Acquisition, Development and Maintenance

- Security requirements analysis and specification
- Correct processing in applications

Information Systems Acquisition, Development and Maintenance

- Security requirements analysis and specification
- Correct processing in applications
- Cryptographic controls

Information Systems Acquisition, Development and Maintenance

- Security requirements analysis and specification
- Correct processing in applications
- Cryptographic controls
- Security in development and support processes

Information Systems Acquisition, Development and Maintenance

- Security requirements analysis and specification
- Correct processing in applications
- Cryptographic controls
- Security in development and support processes
- Technical Vulnerability Management

Information Security Incident Management

- Reporting information security events and weaknesses

Information Security Incident Management

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

Business Continuity Management

- Developing and implementing continuity plans including information security

Business Continuity Management

- Developing and implementing continuity plans including information security
- Testing, maintaining and re-assessing business continuity plans

Compliance

- Compliance with legal requirements

Compliance

- Compliance with legal requirements
 - Intellectual property rights (IPR)

Compliance

- Compliance with legal requirements
 - Intellectual property rights (IPR)
 - Data protection and privacy of personal information

Compliance

- Compliance with legal requirements
 - Intellectual property rights (IPR)
 - Data protection and privacy of personal information
- Compliance with security policies and standards and technical compliance

Compliance

- Compliance with legal requirements
 - Intellectual property rights (IPR)
 - Data protection and privacy of personal information
- Compliance with security policies and standards and technical compliance
- Information systems audit

Control Framework

The control framework provides the routine response to known risks as part of the information security process, by combining the following, to mitigate those known risks to an acceptable level:

- security policies,

Control Framework

The control framework provides the routine response to known risks as part of the information security process, by combining the following, to mitigate those known risks to an acceptable level:

- security policies,
- procedures,

Control Framework

The control framework provides the routine response to known risks as part of the information security process, by combining the following, to mitigate those known risks to an acceptable level:

- security policies,
- procedures,
- standards

Control Framework

The control framework provides the routine response to known risks as part of the information security process, by combining the following, to mitigate those known risks to an acceptable level:

- security policies,
- procedures,
- standards
- and architecture

The meaning of acceptable will vary from organisation to organisation:

- there is no preset control framework for your organisation,

The meaning of acceptable will vary from organisation to organisation:

- there is no preset control framework for your organisation,
- ISO/IEC 27002:2005 (or others) are only guides that need to be adapted.

A typical control framework can be broken down into the following components:

- The Policies (policy statements).

A typical control framework can be broken down into the following components:

- The Policies (policy statements).
- The Procedures.

A typical control framework can be broken down into the following components:

- The Policies (policy statements).
- The Procedures.
- (Guidelines & Work instructions)

A typical control framework can be broken down into the following components:

- The Policies (policy statements).
- The Procedures.
- (Guidelines & Work instructions)
- The Standards.

A typical control framework can be broken down into the following components:

- The Policies (policy statements).
- The Procedures.
- (Guidelines & Work instructions)
- The Standards.
- (Security architectures).

A typical control framework can be broken down into the following components:

- The Policies (policy statements).
- The Procedures.
- (Guidelines & Work instructions)
- The Standards.
- (Security architectures).
- Other documentation.

Policy statements

These are the highlevel (strategic) documents generally addressing a number of controls (often structured according to the 11 chapters of the 27002), spread across various areas of activity.

Example: Access control Policy (chap. 11 of 27002)

Procedures

Procedures further detail aspects of the policy statements describing

- realistic processes

Example: Remote Access Control Procedure (part of chap. 11.4 of 27002)

Procedures

Procedures further detail aspects of the policy statements describing

- realistic processes
- covering daily management activities

Example: Remote Access Control Procedure (part of chap. 11.4 of 27002)

Procedures

Procedures further detail aspects of the policy statements describing

- realistic processes
- covering daily management activities
- and defining responsibilities.

Example: Remote Access Control Procedure (part of chap. 11.4 of 27002)

Guidelines & Work instructions

Sometimes, procedures don't provide enough detail to get the job done. This is particularly true for highly complex tasks that require detailed step-by-step instructions.

Work instructions provide more detail. As a consequence, such instructions are often tightly bound to a particular implementation.

Guidelines are useful for providing advice in a less formal way - there is no requirement to sign-off guidelines.

Example: Acces Control Instructions for mobile devices

Standards

Information security standards translate policy/procedure requirements into operational instructions.

Example: List of authorized remote access mechanisms/tools

Security architectures

- Most medium and large organisation have a complex IT infrastructure that has evolved over time.

Example: Remote Acces Architecture

Security architectures

- Most medium and large organisation have a complex IT infrastructure that has evolved over time.
- Each of these systems has an associated security model.

Example: Remote Acces Architecture

Security architectures

- Most medium and large organisation have a complex IT infrastructure that has evolved over time.
- Each of these systems has an associated security model.
- The goal of a security architecture is to combine processes and tools into a framework that mitigates risk.

Example: Remote Acces Architecture

Other documentation

Examples of the types of documents that the department will be involved with include:

- Legal & regulatory documentation, including contracts

Other documentation

Examples of the types of documents that the department will be involved with include:

- Legal & regulatory documentation, including contracts
- Security monitoring data and security reports

Other documentation

Examples of the types of documents that the department will be involved with include:

- Legal & regulatory documentation, including contracts
- Security monitoring data and security reports
- Log files, access control lists (physical and/or logical)

Other documentation

Examples of the types of documents that the department will be involved with include:

- Legal & regulatory documentation, including contracts
- Security monitoring data and security reports
- Log files, access control lists (physical and/or logical)
- Project plans and status reports

Other documentation

Examples of the types of documents that the department will be involved with include:

- Legal & regulatory documentation, including contracts
- Security monitoring data and security reports
- Log files, access control lists (physical and/or logical)
- Project plans and status reports
- Financial plans and budgets

Other documentation

Examples of the types of documents that the department will be involved with include:

- Legal & regulatory documentation, including contracts
- Security monitoring data and security reports
- Log files, access control lists (physical and/or logical)
- Project plans and status reports
- Financial plans and budgets
- Vendor-related documentation and licences

Other documentation

Examples of the types of documents that the department will be involved with include:

- Legal & regulatory documentation, including contracts
- Security monitoring data and security reports
- Log files, access control lists (physical and/or logical)
- Project plans and status reports
- Financial plans and budgets
- Vendor-related documentation and licences
- Documentation owned by other operational units

DO's and DON'Ts

- DO:

DO's and DON'Ts

- DO:
 - Keep the volume of documentation down to a strict minimum.

DO's and DON'Ts

- DO:
 - Keep the volume of documentation down to a strict minimum.
 - Check regularly to see that documentation is being used.

DO's and DON'Ts

- DO:
 - Keep the volume of documentation down to a strict minimum.
 - Check regularly to see that documentation is being used.
 - Ensure that documents are reviewed and approved by all concerned parties.

DO's and DON'Ts

- DO:
 - Keep the volume of documentation down to a strict minimum.
 - Check regularly to see that documentation is being used.
 - Ensure that documents are reviewed and approved by all concerned parties.
 - Take time to organise the way documents are stored and retrieved

DO's and DON'Ts

- DO:
 - Keep the volume of documentation down to a strict minimum.
 - Check regularly to see that documentation is being used.
 - Ensure that documents are reviewed and approved by all concerned parties.
 - Take time to organise the way documents are stored and retrieved
 - create a well-structured set of directories.

DO's and DON'Ts

- DO:
 - Keep the volume of documentation down to a strict minimum.
 - Check regularly to see that documentation is being used.
 - Ensure that documents are reviewed and approved by all concerned parties.
 - Take time to organise the way documents are stored and retrieved
 - create a well-structured set of directories.
- DON'T:

DO's and DON'Ts

- DO:
 - Keep the volume of documentation down to a strict minimum.
 - Check regularly to see that documentation is being used.
 - Ensure that documents are reviewed and approved by all concerned parties.
 - Take time to organise the way documents are stored and retrieved
 - create a well-structured set of directories.
- DON'T:
 - Try to document everything.

DO's and DON'Ts

- DO:
 - Keep the volume of documentation down to a strict minimum.
 - Check regularly to see that documentation is being used.
 - Ensure that documents are reviewed and approved by all concerned parties.
 - Take time to organise the way documents are stored and retrieved
 - create a well-structured set of directories.
- DON'T:
 - Try to document everything.
 - Document material that is already in user guides (e.g. successive screen shots).

DO's and DON'Ts

- DO:
 - Keep the volume of documentation down to a strict minimum.
 - Check regularly to see that documentation is being used.
 - Ensure that documents are reviewed and approved by all concerned parties.
 - Take time to organise the way documents are stored and retrieved
 - create a well-structured set of directories.
- DON'T:
 - Try to document everything.
 - Document material that is already in user guides (e.g. successive screen shots).
 - Try to have sign-off on everything! Restrict yourself to approving key documents.

DO's and DON'Ts

- DO:
 - Keep the volume of documentation down to a strict minimum.
 - Check regularly to see that documentation is being used.
 - Ensure that documents are reviewed and approved by all concerned parties.
 - Take time to organise the way documents are stored and retrieved
 - create a well-structured set of directories.
- DON'T:
 - Try to document everything.
 - Document material that is already in user guides (e.g. successive screen shots).
 - Try to have sign-off on everything! Restrict yourself to approving key documents.
 - Use documents to communicate when you should be talking face-to-face.

Producing the policy - good practices

- Don't Become a Paper Dragon

Producing the policy - good practices

- Don't Become a Paper Dragon
- Involving The Right People

Producing the policy - good practices

- Don't Become a Paper Dragon
- Involving The Right People
 - it is important to involve all concerned parties from the start.

Producing the policy - good practices

- Don't Become a Paper Dragon
- Involving The Right People
 - it is important to involve all concerned parties from the start.
- Policies must respect the company culture

- NEVER develop policy statements in isolation.

- NEVER develop policy statements in isolation.
- Consider working in an iterative fashion, asking for feedback at each step.

- NEVER develop policy statements in isolation.
- Consider working in an iterative fashion, asking for feedback at each step.
 - Using skeleton documents can be very effective.

- NEVER develop policy statements in isolation.
- Consider working in an iterative fashion, asking for feedback at each step.
 - Using skeleton documents can be very effective.
 - Start with section titles and a rough description of what needs to go in each section.

- NEVER develop policy statements in isolation.
- Consider working in an iterative fashion, asking for feedback at each step.
 - Using skeleton documents can be very effective.
 - Start with section titles and a rough description of what needs to go in each section.
 - Circulate for comments and suggestions.

- NEVER develop policy statements in isolation.
- Consider working in an iterative fashion, asking for feedback at each step.
 - Using skeleton documents can be very effective.
 - Start with section titles and a rough description of what needs to go in each section.
 - Circulate for comments and suggestions.
 - Flesh the policy out section by section.

- NEVER develop policy statements in isolation.
- Consider working in an iterative fashion, asking for feedback at each step.
 - Using skeleton documents can be very effective.
 - Start with section titles and a rough description of what needs to go in each section.
 - Circulate for comments and suggestions.
 - Flesh the policy out section by section.
 - Use open questions and provide alternatives.

- NEVER develop policy statements in isolation.
- Consider working in an iterative fashion, asking for feedback at each step.
 - Using skeleton documents can be very effective.
 - Start with section titles and a rough description of what needs to go in each section.
 - Circulate for comments and suggestions.
 - Flesh the policy out section by section.
 - Use open questions and provide alternatives.
 - Listen to people's objections and encourage them to identify solutions to their own issues.

- Planning - Producing a policy statement is a strategic objective.

- Planning - Producing a policy statement is a strategic objective.
 - The different types of activity need to be identified, prioritised and estimated.

- Planning - Producing a policy statement is a strategic objective.
 - The different types of activity need to be identified, prioritised and estimated.
 - Roles and responsibilities for the project need to be defined and agreed with those concerned.

- Planning - Producing a policy statement is a strategic objective.
 - The different types of activity need to be identified, prioritised and estimated.
 - Roles and responsibilities for the project need to be defined and agreed with those concerned.
 - Resources from other areas need to be reserved in advance.

- Planning - Producing a policy statement is a strategic objective.
 - The different types of activity need to be identified, prioritised and estimated.
 - Roles and responsibilities for the project need to be defined and agreed with those concerned.
 - Resources from other areas need to be reserved in advance.
 - Dependencies and possible contention for resources need to be identified up front.

- Planning - Producing a policy statement is a strategic objective.
 - The different types of activity need to be identified, prioritised and estimated.
 - Roles and responsibilities for the project need to be defined and agreed with those concerned.
 - Resources from other areas need to be reserved in advance.
 - Dependencies and possible contention for resources need to be identified up front.
 - Decision points need to be clearly identified.

- Planning - Producing a policy statement is a strategic objective.
 - The different types of activity need to be identified, prioritised and estimated.
 - Roles and responsibilities for the project need to be defined and agreed with those concerned.
 - Resources from other areas need to be reserved in advance.
 - Dependencies and possible contention for resources need to be identified up front.
 - Decision points need to be clearly identified.
 - This should all be summarised in a formal project plan.

- Planning - Producing a policy statement is a strategic objective.
 - The different types of activity need to be identified, prioritised and estimated.
 - Roles and responsibilities for the project need to be defined and agreed with those concerned.
 - Resources from other areas need to be reserved in advance.
 - Dependencies and possible contention for resources need to be identified up front.
 - Decision points need to be clearly identified.
 - This should all be summarised in a formal project plan.
- Aim for milestones at regular intervals to show progress.

- Planning - Producing a policy statement is a strategic objective.
 - The different types of activity need to be identified, prioritised and estimated.
 - Roles and responsibilities for the project need to be defined and agreed with those concerned.
 - Resources from other areas need to be reserved in advance.
 - Dependencies and possible contention for resources need to be identified up front.
 - Decision points need to be clearly identified.
 - This should all be summarised in a formal project plan.
- Aim for milestones at regular intervals to show progress.
- Sign-Off is Critical

- Planning - Producing a policy statement is a strategic objective.
 - The different types of activity need to be identified, prioritised and estimated.
 - Roles and responsibilities for the project need to be defined and agreed with those concerned.
 - Resources from other areas need to be reserved in advance.
 - Dependencies and possible contention for resources need to be identified up front.
 - Decision points need to be clearly identified.
 - This should all be summarised in a formal project plan.
- Aim for milestones at regular intervals to show progress.
- Sign-Off is Critical
 - Management Sign-Off: It is a good idea to include a statement from the executive board that supports the policy and explains any consequences of not adhering to it.

- Planning - Producing a policy statement is a strategic objective.
 - The different types of activity need to be identified, prioritised and estimated.
 - Roles and responsibilities for the project need to be defined and agreed with those concerned.
 - Resources from other areas need to be reserved in advance.
 - Dependencies and possible contention for resources need to be identified up front.
 - Decision points need to be clearly identified.
 - This should all be summarised in a formal project plan.
- Aim for milestones at regular intervals to show progress.
- Sign-Off is Critical
 - Management Sign-Off: It is a good idea to include a statement from the executive board that supports the policy and explains any consequences of not adhering to it.
 - Staff Sign-Off: Having staff formally agree to the policy can be very useful when the policy is not respected and there are serious consequences.

- Publication

- Publication
- Diffusion

- Publication
- Diffusion
 - Publish on the company intranet

- Publication
- Diffusion
 - Publish on the company intranet
 - Use mouse mats, posters, ...

- Publication
- Diffusion
 - Publish on the company intranet
 - Use mouse mats, posters, ...
 - Think about interactive methods.

- Publication
- Diffusion
 - Publish on the company intranet
 - Use mouse mats, posters, ...
 - Think about interactive methods.
- Prepare via awareness raising actions

Conclusion - summary

A global information security process/approach can follow these steps:

- 1 Risk assessment/analysis

Conclusion - summary

A global information security process/approach can follow these steps:

- 1 Risk assessment/analysis
- 2 Awareness raising campaign

Conclusion - summary

A global information security process/approach can follow these steps:

- 1 Risk assessment/analysis
- 2 Awareness raising campaign
- 3 Security policy

Conclusion - summary

A global information security process/approach can follow these steps:

- ① Risk assessment/analysis
- ② Awareness raising campaign
- ③ Security policy
- ④ ISMS (Information Security Management System)

Conclusion - summary

A global information security process/approach can follow these steps:

- 1 Risk assessment/analysis
- 2 Awareness raising campaign
- 3 Security policy
- 4 ISMS (Information Security Management System)
- 5 ISMS - Certification