atsec information security corporation
9130 Jollyville Road, Suite 260
Austin, TX 78759
Tel: 512-615-7300
Fax: 512-615-7301
www.atsec.com

ISMS Implementation Guide

Usage note

Note: The intent of this document is to help you recognize the activities related to establishing an ISMS. This document should not be considered as professional consulting for establishing or implementing an ISMS. Use of this guide does not guarantee a successful implementation nor an implementation that is ready for certification. If you want to implement an ISMS, consider hiring a professional consultant who specializes in ISMS implementation.

Table of contents

Overview of an ISMS

Information security is the protection of information to ensure:

- Confidentiality: ensuring that the information is accessible only to those authorized to access it.
- Integrity: ensuring that the information is accurate and complete and that the information is not modified without authorization.
- Availability: ensuring that the information is accessible to authorized users when required.

Information security is achieved by applying a suitable set of controls (policies, processes, procedures, organizational structures, and software and hardware functions).

An ***Information Security Management System (ISMS)*** is way to protect and manage information based on a systematic business risk approach, to establish, implement, operate, monitor, review, maintain, and improve information security. It is an organizational approach to information security.

ISO/IEC publishes two standards that focus on an organization's ISMS:

- **The code of practice standard: ISO/IEC 27002 (ISO/IEC 17799)**. This standard can be used as a starting point for developing an ISMS. It provides guidance for planning and implementing a program to protect information assets. It also provides a list of controls (safeguards) that you can consider implementing as part of your ISMS.
- **The management system standard: ISO/IEC 27001**. This standard is the specification for an ISMS. It explains how to apply ISO/IEC 27002 (ISO/IEC 17799). It provides the standard against which certification is performed, including a list of required documents. An organization that seeks certification of its ISMS is examined against this standard.

These standards are copyright protected text and must be purchased. (For purchasing information, refer to section 1, "Purchase ISO standards.")

The standards set forth the following practices:

- All activities must follow a method. The method is arbitrary but must be well defined and documented.
- A company or organization must document its own security goals. An auditor will verify whether these requirements are fulfilled.
- All security measures used in the ISMS shall be implemented as the result of a risk analysis in order to eliminate or reduce risks to an acceptable level.
- The standard offers a set of security controls. It is up to the organization to choose which controls to implement based on the specific needs of their business.
- A process must ensure the continuous verification of all elements of the security system through audits and reviews.
- A process must ensure the continuous improvement of all elements of the information and security management system. (The ISO/IEC 27001 standard adopts the Plan-Do-Check-Act [PDCA] model as its basis and expects the model will be followed in an ISMS implementation.)

These practices form the framework within which you will establish an ISMS. The sections that follow describe the steps involved in establishing an ISMS.

Note: It is important to remember that although this guide provides examples, the implementation of an ISMS is process-based and specific to your organization. Consider using the guide and examples as a starting point of discussion within your organization, rather than as a set of templates.

1 Purchase a copy of the ISO/IEC standards

Before establishing an ISMS and drafting the various documents for your ISMS, you should purchase copies of the pertinent ISO/IEC standards, namely:

The code of practice standard: ISO/IEC 27002 (ISO/IEC17799). This standard can be used as a starting point for developing an ISMS. It provides guidance for planning and implementing a program to protect information assets. It also provides a list of controls (safeguards) that you can consider implementing as part of your ISMS.

The management system standard: ISO/IEC 27001. This standard is the specification for an ISMS. It explains how to apply ISO/IEC 27002 (ISO/IEC17799). It provides the standard against which certification is performed, including a list of required documents. An organization that seeks certification of its ISMS is examined against this standard.

You can purchase these standards from either of the following online stores:

- The ANSI online store: http://webstore.ansi.org
- The ISO Online Shop: http://www.iso.ch

2 Obtain management support

As described in ISO/IEC 27001, management plays an important role in the success of an ISMS.

What you need: Management responsibility section of ISO/IEC 27001.

Management must make a commitment to the establishment, implementation, operation, monitoring, review, maintenance, and improvement of the ISMS. Commitment must include activities such as ensuring that the proper resources are available to work on the ISMS and that all employees affected by the ISMS have the proper training, awareness, and competency.

Results: Establishment of the following items demonstrates management commitment:

- An information security policy; this policy can be a standalone document or part of an overall security manual that is used by an organization. (For additional guidance, refer to the example below.)
- Information security objectives and plans; again this information can be a standalone document or part of an overall security manual that is used by an organization (For additional guidance, refer to the example below.)
- Roles and responsibilities for information security; a list of the roles related to information security should be documented either in the organization's job description documents or as part of the security manual or ISMS description documents.
- Announcement or communication to the organization about the importance of adhering to the information security policy.
- Sufficient resources to manage, develop, maintain, and implement the ISMS.

In addition, management will participate in the ISMS Plan-Do-Check-Act [PDCA] process, as described in ISO/IEC 27001 by:

- Determining the acceptable level of risk. Evidence of this activity can be incorporated into the risk assessment documents, which are described later in this guide. (See steps 6 through 8.)
- Conducting management reviews of the ISMS at planned intervals. Evidence of this activity can be part of the approval process for the documents in the ISMS.

- Ensuring that personnel affected by the ISMS are provided with training, are competent for the roles and responsibilities they are assigned to fulfill, and are aware of those roles and responsibilities. Evidence of this activity can be through employee training records and employee review documents.

Example:

This example shows a possible policy statement with goals and objectives.

Security Policy

Protection of company assets is vital to the success of our business. To this end, we have established an information security management system that operates all the processes required to identify the information we need to protect and how we must protect it.

Because the needs of our business change, we recognize that our management system must be continually changed and improved to meet our needs. To this effect, we are continually setting new objectives and regularly reviewing our processes.

Objectives

It is the policy of our company to ensure:

- Information is only accessible to authorized persons from within or outside the company.
- Confidentiality of information is maintained.
- Integrity of information is maintained throughout the process.
- Business continuity plans are established, maintained, and tested.
- All personnel are trained on information security and are informed that compliance with the policy is mandatory.
- All breaches of information security and suspected weaknesses are reported and investigated.
- Procedures exist to support the policy, including virus control measures, passwords, and continuity plans.
- Business requirements for availability of information and systems will be met.
- The Information Security Manager is responsible for maintaining the policy and providing support and advice during its implementation.
- All managers are directly responsible for implementing the policy and ensuring staff compliance in their respective departments.

This policy has been approved by the company management and shall be reviewed by the management review team annually:

Signature: _____ Date: _____

Title: _____

Figure 1: Example of Security Policy

3 Determine the scope of the ISMS

When management has made the appropriate commitments, you can begin to establish your ISMS.

In this step, you should determine the extent to which you want the ISMS to apply to your organization.

What you need:

You can use several of the "result" documents that were created as part of step 2, such as:

- The information security policy
- The information security objectives and plans
- The roles and responsibilities that are related to information security and were defined by the management

In addition, you will need:

- Lists of the areas, locations, assets, and technologies of the organization that will be controlled by the ISMS.

While reviewing these lists, you might want to answer questions similar to the following:

- What areas of your organization will be covered by the ISMS?
- What are the characteristics of those areas; its locations, assets, technologies to be included in the ISMS?
- Will you require your suppliers to abide by your ISMS?
- Are there dependencies on other organizations? Should they be considered?

Your goals will be to cover the following:

- the processes used to establish the scope and context of the ISMS.
- the strategic and organizational context

Important: Keep your scope manageable. Consider including only parts of the organization, such as a logical or physical grouping within the organization. Large organizations might need several Information Security Management Systems in order to maintain manageability. For example, they might have one ISMS for their Finance department and the networks used by that department and a separate ISMS for their Software Development department and systems.

Results: A documented scope for your ISMS.

When you have determined the scope, you will need to document it, usually in a few statements or paragraphs. The documented scope often becomes one of the first sections of your organization's Security Manual. Or, it might remain a standalone document in a set of ISMS documents that you plan to maintain.

Often the scope, the security policy, and the security objectives are combined into one document.

For additional guidance, refer to the following example.

Example:

Scope and Purpose

The company is committed to protecting its information and that of its customers. To achieve this goal, the company has implemented an Information Security Management System in accordance with ISO/IEC 27001: 2005.

The company's ISMS is applicable to the following areas of the business:

- Finance department
- Internal IT systems and networks used for back-end business (such as e-mail, timesheets, contract development and storage, and report writing)

(**Note:** IT systems on which company software is developed and stored are part of the Software Development ISMS. Refer to the Software Development Security Manual for more information.)

Figure 2: Example of Scope Statements

4 Identify applicable legislation

After you have determined the scope, identify any regulatory or legislative standards that apply to the areas you plan to cover with the ISMS. Such standards might come from the industry in which your organization works or from state, local, or federal governments, or international regulatory bodies.

What you need: Up-to-date regulatory or legislative standards that might be applicable to your organization.

You might find it helpful to have input and review from lawyers or specialists who are knowledgeable about the standards.

Results: Additional statements in the scope of the ISMS. If your ISMS will incorporate more than two or three legislative or regulatory standards, you might also create a separate document or appendix in the Security Manual that lists all of the applicable standards and details about the standards.

Example: The text added to the scope statement as a result of identifying applicable legislation is shown in the following example in italics.

Scope and Purpose

The company is committed to protecting its information and that of its customers. To achieve this goal, the company has implemented an Information Security Management System in accordance with ISO/IEC 27001: 2005 *and the rules and regulations that are part of OSHA Public Law 91-596 84 STAT. 1950.*

The company's ISMS is applicable to the following areas of the business:

- Finance department
- Internal IT systems and networks used for back-end business (such as e-mail, timesheets, contract development and storage, and report writing)
  (**Note:** IT systems and networks on which company software is developed and stored are part of the Software Development ISMS. Refer to the Software Development Security Manual for more information.)

Figure 3: Example of Additional Scope Text

5 Define a method of risk assessment

Risk assessment is the process of identifying risks by analyzing threats to, impacts on, and vulnerabilities of information and information systems and processing facilities, and the likelihood of their occurrence. Choosing a risk assessment method is one of the most important parts of establishing an ISMS.

To meet the requirements of ISO/IEC 27001, you will need to define and document a method of risk assessment and then use it to assess the risk to your identified information assets, make decisions about which risks are intolerable and therefore need to be mitigated, and manage the residual risks through carefully considered policies, procedures, and controls.

ISO/IEC 27001 does not specify the risk assessment method you should use; however, it does state that you must use a method that enables you to complete the following tasks:

- Evaluate risk based on levels of confidentiality, integrity, and availability.

  Some risk assessment methods provide a matrix that defines levels of confidentiality, integrity, and availability and provide guidance as to when and how those levels should be applied, as shown in the following table:

Impact of Loss ►	LOW	MEDIUM	HIGH
Confidentiality Ensuring that information is accessible only to those authorized to have access	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Safeguarding the accuracy and completeness of information and processing methods	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring that authorized users have access to information and associated assets when required	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Figure 4: Example of CIA Value Table

- Set objectives to reduce risk to an acceptable level
- Determine criteria for accepting risk
- Evaluate risk treatment options.

There are many risk assessment methods you can choose from, such as those that are prevalent in your industry. For example, if your company is in the oil industry, you might find there are risk assessment methods related to that industry.

What you will need:

If you are unfamiliar with risk assessment methods, you might want to refer to these published examples:

- ISO/IEC 13335 (Management of information and communications technology security)
- NIST SP 800-30 (Risk Management Guide for Information Technology Systems) http://csrc.nist.gov/publications/nistpubs/
- Risk assessment methods that are specific to the industry of your organization.

Results:

When you have completed this step, you should have a document that explains how your organization will assess risk, including:

- the organization's approach to information security risk management
- criteria for information security risk evaluation and the degree of assurance required

Note: In subsequent steps, which are described in this guide, you will add more information to this document, which will define the assets that need to be protected, the risks associated with each of those assets, and a list of the controls that will be used to reduce or eliminate the risks.

For additional guidance, refer to the following example.

Example: This example provides a possible outline for a risk assessment document that defines the risk assessment methodology.

Table of Contents

Figure 5: Example of the Contents of a Risk Assessment Methodology Document

6 Create an inventory of information assets to protect

To identify risks and the levels of risks associated with the information you want to protect, you first need to make a list of all of your information assets that are covered in the scope of the ISMS.

What you will need:

You will need the scope that you defined in step 3 and input from the organization that is defined in your scope regarding its information assets.

Result:

When you have completed this step, you should have a list of the information assets to be protected and an owner for each of those assets. You might also want to identify where the information is located and how critical or difficult it would be to replace.

This list should be part of the risk assessment methodology document that you created in the previous step.

Because you will need this list to document your risk assessment, you might want to group the assets into categories and then make a table of all the assets with columns for assessment information and the controls you choose to apply. (You will perform these activities in subsequent steps of this guide.)

The following example shows an asset table.

Example:

Risk Assessment

Asset	Details	Owner	Location	CIA profile	Replacement value	Risk Summary	Risk Value	Control	Sufficient control?
Strategic Informa-tion	Medium and long term plans	CEO	CEO PC		High				
Project plans	Short term plans.	CEO	CEO PC		Medium				

Figure 6: Example of Asset Table with Placeholder Columns for Assessment Information

7 Identify risks

Next, for each asset you defined in the previous step, you will need to identify risks and classify them according to their severity and vulnerability. In addition, you will need to identify the impact that loss of confidentiality, integrity, and availability may have on the assets.

To begin identifying risks, you should start by identifying actual or potential threats and vulnerabilities for each asset.

A threat is something that could cause harm. For example, a threat could be any of the following:

- A declaration of the intent to inflict harm or misery
- Potential to cause an unwanted incident, which may result in harm to a system or organization and its assets
- Intentional, accidental, or man-made act that could inflict harm or an act of God (such as a hurricane or tsunami)

A vulnerability is a source or situation with a potential for harm (for example, a broken window is a vulnerability; it might encourage harm, such as a break in).

A risk is a combination of the likelihood and severity or frequency that a specific threat will occur.

What you will need:

- The list of assets that you defined in the previous step
- The risk assessment methodology you defined in step 5

For each asset, you should identify vulnerabilities that might exist for that asset and threats that could result from those vulnerabilities. It is often helpful to think about threats and vulnerabilities in pairs—with at least one pair for each asset and possibly multiple pairs for each asset.

Results:

For each asset, you will have a threat and vulnerability description and, using your Risk Assessment methodology, you will assign levels of confidentiality, integrity, and availability to that asset.

If you used a table for step 6, you can add this information to that table, as shown in the following example.

Example:

Note: In the following example, the Risk Summary column describes the threat and vulnerability. The CIA profile classifies the asset's confidentiality, integrity, and availability.

Risk Assessment

Asset	Details	Owner	Location	CIA profile	Replacement value	Risk Summary	Risk Value	Control	Sufficient control?
Strategic Informa-tion	Medium and long term plans	CEO	CEO PC	C: High I: High A: Med	High	Disclosure (gives advantage to third party)			
Project plans	Short term plans.	CEO	CEO PC	C: High I: High A: Low	Medium	Disclosure (gives advantage to competitor); company might lose business			

Figure 7: Example of Risk Identification

8 Assess the risks

After you have identified the risks and the levels of confidentiality, integrity, and availability, you will need to assign values to the risks.

The values will help you determine if the risk is tolerable or not and whether you need to implement a control to either eliminate or reduce the risk.

To assign values to risks, you need to consider:

- The value of the asset being protected
- The frequency with which the threat or vulnerability might occur
- The damage that the risk might inflict on the company or its customers or partners

For example, you might assign values of Low, Medium, and High to your risks. To determine which value to assign, you might decide that if the value of an asset is high and the damage from a specified risk is high, the value of the risk should also be high, even though the potential frequency is low. Your Risk Assessment Methodology document should tell you what values to use and might also specify the circumstances under which specific values should be assigned.

Also, be sure to refer to your Risk Assessment Methodology document to determine the implication of a certain risk value. For example, to keep your ISMS manageable, your Risk Assessment Methodology might specify that only risks with a value of Medium or High will require a control in your ISMS. Based on your business needs and industry standards, risk will be assigned appropriate values.

What you will need:

- Lists of assets and their associated risks and CIA levels, which you created in the previous step.
- Possibly input from management as to what level of risk they are willing to accept for specific assets.

Results:

When you have completed your assessment, you will have identified which information assets have intolerable risk and therefore require controls. You should have a document (sometimes referred to as a Risk Assessment Report) that indicates the risk value for each asset.

In the next step you will identify which controls might be applicable for the assets that require control in order to reduce the risk to tolerable levels.

This document can either be standalone or it can be part of an overall Risk Assessment document that contains your risk assessment methodology and this risk assessment.

Examples:

If you used a table similar to the one in the preceding examples, your result after completing this step might look like the following example:

Risk Assessment

Asset	Details	Owner	Location	CIA profile	Replacement value	Risk Summary	Risk Value	Control	Sufficient control?
Strategic Informa-tion	Medium and long term plans	CEO	CEO PC	C: High I: High A: Med	High	Disclosure (gives advantage to third party)	High		
Project plans	Short term plans.	CEO	CEO PC	C: High I: High A: Low	Medium	Disclosure (gives advantage to competitor); company might lose business	Medium		
HR documents	Employee records	Company Board	HR Management Company	C: High I: High A: Low	Medium	Disclosure of personal information	Medium		

Figure 8: Example of Risk Assessment

9 Identify applicable objectives and controls

Next, for the risks that you've determined to be intolerable, you must take one of the following actions:

- decide to accept the risk, for example, actions are not possible because they are out of your control (such as natural disaster or political uprising) or are too expensive.
- transfer the risk, for example, purchase insurance against the risk, subcontract the activity so that the risk is passed on to the subcontractor, etc.
- reduce the risk to an acceptable level through the use of controls.

To reduce the risk, you should evaluate and identify appropriate controls. These controls might be controls that your organization already has in place or controls that are defined in the ISO/IEC 27002 (ISO/IEC 17799) standard.

(**Note:** An examination of the controls that you already have in place against the standard and then using the results to identify what controls are missing is commonly called a "gap analysis.")

What you will need:

- Annex A of ISO/IEC 27001. This appendix summarizes controls that you might want to choose from.
- ISO/IEC 27002 (ISO/IEC 17799), which provides greater detail about the controls summarized in ISO/IEC 27001.
- Procedures for existing corporate controls

Results:

You should end up with two documents by completing this step:

- A Risk Treatment Plan
- A Statement of Applicability

The *Risk Treatment Plan* documents the following:

- the method selected for treating each risk (accept, transfer, reduce)
- which controls are already in place
- what additional controls are proposed
- the time frame over which the proposed controls are to be implemented

The *Statement of Applicability* (SOA) documents the control objectives and controls selected from Annex A. The Statement of Applicability is usually a large table in which each control from Annex A of ISO/IEC 27001 is listed with its description and corresponding columns that indicate whether that control was adopted by the organization, the justification for adopting or not adopting the control, and a reference to the location where the organization's procedure for using that control is documented.

The SOA can be part of the Risk Assessment document; but usually it is a standalone document because it is lengthy and is listed as a required document in the standard.

For additional help with creating a Risk Treatment Plan and a Statement of Applicability, refer to the two sets of examples that follow.

Examples of Risk Treatment Plan:

If you used a table as described in the preceding steps, the control analysis portion of your Risk Treatment Plan could be covered by the Control column and the Sufficient Control column, as shown in the following

example. **Note:** Any risks that you transfer to others or that you choose to accept as they are should also be recorded in your treatment plan.

Risk Assessment

Asset	Details	Owner	Location	CIA profile	Replacement value	Risk Summary	Risk Value	Control	Sufficient control?
Strategic Informa-tion	Medium and long term plans	CEO	CEO PC	C: High I: High A: Med	High	Disclosure (gives advantage to third party)	High	15.1.1	Yes
Project plans	Short term plans.	CEO	CEO PC	C: High I: High A: Low	Medium	Disclosure (gives advantage to competitor); company might lose business	Medium	15.1.1	Yes
HR documents	Employee records	Company Board	HR Management Company	C: High I: High A: Low	Medium	Disclosure of personal information	Medium	None; HR activities and documentation management outsourced	Yes

Figure 9: Example of Risk Assessment with Control Analysis Included

The remaining Risk Treatment Plan requirements could be met by adding this table and by explaining the methods used for treating risk and the time frame in which the controls will be implemented to a Risk Assessment Methodology document, like the one you created in step 5.

Your revised document contents might look like the following example:

Table of Contents

Introduction

Preparation
- Scope and boundaries
- Security Objectives and Security Requirements
- Acceptable Risks
  - Description of Major Vulnerabilities
  - Description of Major Threats
  - Residual Risks

Uncertainty Analysis
- Assumptions
- External Dependencies

Planned Improvements
- Effectiveness of Controls
- Planned Controls
- Assessment of Residual Risk

Key and definitions
- Risk Value Color Scale
- Definitions of Confidentiality, Integrity, Availability, Accountability and the Consequences of Their Absence
- Definitions of key terms (such as asset, risk, threat vulnerability, information, data, control)

Asset Valuation Risk Identification, Control Analysis (the Risk Assessment table)

Statement of Applicability (could be a summary with pointer to detailed table in a separate document)
- Rational for Selecting Controls
- Rational for Excluding Controls

Figure 10: Example of Risk Assessment Document with Assessment Information and SOA Included

Example of Statement of Applicability:
The following is an excerpt of a Statement of Applicability document. The Reference column identifies the location where the statement of policy or detailed procedure related to the implementation of the control is documented.

Two items in the Reference column are incomplete in this example because at this step you might not have a complete set of policies and procedures for all controls. The next step addresses the creation of additional procedures so that you can complete the Statement of Applicability.

Statement of Applicability

Control	Headline	App.	Compliance Statement	Reference
5	Security policy			
5.1	Information security policy		To provide management direction and support for information security	
5.1.1	Information security policy document	yes	The Information Security Policy is provided to New Employees on their first day of employment.	Company Security Manual
5.1.2	Review of the information security policy	yes	The Information Security Policy is reviewed by management on an ongoing basis as apart of management reviews	Roles and Responsibilities document
6	Organizing information security			
6.1	Internal organization			
6.1.1	Management commitment to information security	yes	Documented in the security policy	Company Security Policy I
6.1.2	Information security coordination	yes	Through a security forum, training sessions, and day-to-day work	<TBD—security procedures>
6.1.3	Allocation of information security responsibilities	yes	Allocation of information security responsibilities are documented	<TBD—security procedures> Company Security Manual

Figure 11: Example of Statement of Applicability

10 Set up policy and procedures to control risks

For each control that you define, you must have corresponding statements of policy or in some cases a detailed procedure. The procedure and policies are used by affected personnel so they understand their roles and so that the control can be implemented consistently.

The documentation of the policy and procedures is a requirement of ISO/IEC 27001.

What you will need:

To help you identify which procedures you might need to document, refer to your Statement of Applicability.

To help you write your procedures so that they are consistent in content and appearance, you might want to create some type of template for your procedure writers to use.

Results:

Additional policy and procedure documents. (The number of documents you produce will depend on the requirements of your organization.)

Some of these procedures might also generate records. For example, if you have a procedure that all visitors to your facility must sign a visitors log, the log itself becomes a record providing evidence that the procedure has been followed.

Sections 4.3.2 and 4.3.3 of ISO/IEC 27001 require that all documents and records that are part of your ISMS be properly controlled. Therefore, policy and procedure documents must also be created to address these controls.

Example:

The number of policies, procedures, and records that you will require as part of your ISMS will depend on a number of factors, including the number of assets you need to protect and the complexity of the controls you need to implement. The example that follows shows a partial list of one organization's set of documents:

Security Manual
Security Policy
Risk Assessment Methodology
Risk Assessment Report, Asset List, and Treatment Plan
Statement of Applicability
Roles and Responsibilities document
Procedure 1: Workplace Security
Procedure 2: Document and Record Control
Procedure 3: Training
Procedure 4: Server Backups
Procedure 5: Audit Procedure
Records:
- Audit Schedule
- Employee Training Records
- Employee Review/Evaluation Records
- Issues/Non-Conformances
- Server Maintenance Records

…..Management Review Records

Figure 12: Example of Some Documents in an ISMS

11 Allocate resources and train the staff

Adequate resources (people, time, money) should be allocated to the operation of the ISMS and all security controls. In addition, the staff who must work within the ISMS (maintaining it and its documentation and implementing its controls) must receive appropriate training.

The success of the training program should be monitored to ensure that it is effective. Therefore, in addition to the training program, you should also establish a plan for how you will determine the effectiveness of the training.

What you will need:

- A list of the employees who will work within the ISMS
- All of the ISMS procedures to use for identifying what type of training is needed and which members of the staff or interested parties will require training
- Management agreement to the resource allocation and the training plans.

Results:

Specific documentation is not required in the ISO/IEC standards. However, to provide evidence that resource planning and training has taken place, you should have some documentation that shows who has received training and what training they have received. In addition, you might want to include a section for each employee that lists what training they should be given.

Also, you will probably have some type of procedure for determining how many people, how much money, and how much time needs to be allocated to the implementation and maintenance of your ISMS. It's possible that this procedure already exists as part of your business operating procedures or that you will want to add an ISMS section to that existing documentation.

Example:

The following example shows a template for an employee training record:

Training Completed

Date Completed	Scope	Supervisor / Trainer	Overall Rating (S/U)	Type of Training / Comments

Training Planned

Target Completion	Scope	Type of Training / Comments

Figure 13: Example of Employee Training Record

12 Monitor the implementation of the ISMS

To ensure that the ISMS is effective and remains current, suitable, adequate, and effective, ISO/IEC 27001 requires:

- Management to review the ISMS at planned intervals. The review must include assessing opportunities for improvement, and the need for changes to the ISMS, including the security policy and security objectives, with specific attention to previous corrective or preventative actions and their effectiveness.
- Periodic internal audits

The results of the reviews and audits must be documented and records related to the reviews and audits must be maintained.

What you will need:

To perform management reviews, ISO/IEC 27001 requires the following input:

- results of ISMS internal and external audits and reviews
- feedback from interested parties
- techniques, products, or procedures which could be used in the organization to improve the effectiveness of the ISMS
- preventative and corrective actions (including those that might have been identified in previous reviews or audits)
- incident reports, for example, if there has been a security failure, a report that identifies what the failure was, when it occurred, and how it was handled and possibly corrected.
- vulnerabilities or threats not adequately addressed in the previous risk assessment
- follow-up actions from previous reviews
- any organizational changes that could affect the ISMS
- recommendations for improvement

To perform internal audits on a periodic basis, you need to define the scope, criteria, frequency, and methods. You also need the procedure (which should have been written as part of step 10) that identifies the responsibilities and requirements for planning and conducting the audits, and for reporting results and maintaining records.

Results:

The results of a management review should include decisions and actions related to:

- Improvements to the ISMS
- Modification of procedures that effect information security at all levels within the organization
- Resource needs

The results of an internal audit should result in identification of nonconformities and their related corrective actions or preventative actions. ISO/IEC 27001 lists the activity and record requirements related to corrective and preventative actions.

Example:

The following example shows the outline of a preventative action plan. Such a plan might be the result of an internal audit or a management review of the ISMS. You could use a similar outline to prepare a corrective action plan.

Preventative Action Plan:

Description

This section should identify the similar or related occurrences of nonconformances in question. In addition, this section should also identify the corrective actions that were taken for each nonconformance.

This section should then also provide reasoning for needing a preventive action to be taken.

1 Action Plan

This section shall outline the action plan selected for implementing the preventive action in such that it is clear how the preventive action is to be implemented and what is expected as a result.

1.1 Goal

This section shall identify the goal of the action plan. The goal, in most cases, is to prevent future occurrences of the non-conformances identified from reoccurring.

1.2 Method

This section shall describe the approach taken to prevent future occurrences of the nonconformances identified from reoccurring.

1.3 Expected Results

This section shall identify what is expected as a result of implementing the preventive action. The expected result shall in some way be consistent with the goal described above.

2 Results

This section shall identify the results of the preventive action. It may be necessary to list more than one set of results, in cases where you may audit the area of nonconformance more than once after implementing the preventive action. This allows the auditor to examine the consistency between the results.

3 Effectiveness

This section identifies the effectiveness in the preventive action selected. The effectiveness may be measured based on the consistency or comparison of the expected results and the actual results. If the results are very similar to each other then the preventive action was very effective.

Figure 14: Example of Preventative Action Plan

13 Prepare for certification audit

If you plan to have your ISMS certified, you will need to conduct a full cycle of internal audits, management review, and activities in the PDCA process.

The external auditor will first examine your ISMS documents to determine the scope and content of your ISMS. Then the auditor will examine the necessary records and evidence that you implement and practice what is stated in your ISMS.

What you will need:

- All of the documents that you created in the preceding steps.
- Records from at least one full cycle of management reviews, internal audits, and PDCA activities, and evidence of responses taken as the result of those reviews and audits.

Results:

The results of this preparation should be a set of documents that you can send to an auditor for review and a set of records and evidence that will demonstrate how efficiently and completely you have implemented your ISMS.

14 Ask for help

As you can see in this guide, establishing, implementing, and maintaining an ISMS can require a lot of work—especially in its formative stages. If you are new to management systems or specifically to information security management systems, consider hiring a professional ISMS consultant to guide you through the process. A consultant's familiarity with the requirements of an ISMS and the suggested controls in the IEO/IEC standards can save you time and money, and will ensure that you will achieve effective security practices and possibly a successful ISMS certification.

Appendix A Documents and Records

As described throughout this guide, your ISMS will depend on many documents and records.

Certain documents are required by ISO/IEC 27001 and records are required to provide evidence of the implementation of the ISMS.

The following lists provide a summary of the documents and records discussed in previous sections of this guide.

Documents

- Documented statements of the ISMS policy and objectives
- The scope of the ISMS
- Procedures and controls in support of the ISMS
- Description of the risk assessment methodology
- Risk assessment report
- Risk treatment plan
- Documented procedures needed by the organization to ensure the effective planning, operation, and control of its information security processes and describe how to measure the effectiveness of controls
- Records required by ISO/IEC 27001
- Statement of Applicability

The documents listed here can be separate documents or presented together in one or more sets of documents.

Records

The records required for your ISMS will depend on the requirements of your business. ISO/IEC 27001:2005(E) states that records shall be established and maintained to provide evidence of conformity to requirements and the effective operation of the ISMS. It further states that the ISMS shall take account of any relevant legal or regulatory requirements and contractual obligations. They should be controlled and maintained according to the organization's document control and retention policies and procedures.

Some examples of records are:

- Internal audit records
- Employee training records
- Management review minutes
- Preventative and corrective action records
- Incident reports