

Audio transcripts and lesson notes

Hi and welcome back. This is your instructor Anup Narayanan and let us now move on to the second part of the PLAN phase, which is, “Defining the ISMS policy”.

Well, it my duty to remind you where we are in the whole ISMS P-D-C-A cycle. We are in the PLAN phase.

And, within the PLAN phase, we are in step 2, “Defining the ISMS policy”.

So, what is a policy?

A Policy is a plan of action to guide decisions and achieve targets

And...What is an Information Security Policy?

An Information Security policy is a document that states in writing “why” and “how” a company plans to protect the company's information and information assets

Now, there are some terms and definitions that you must learn because you will come across them often during an ISMS implementation. These terms are Policy, Procedure and Guideline.

Let us look at “Policy” first - An Information Security policy is a document that states in writing “why” and “how” a company plans to protect the company's information and information assets

A Procedure is a “step-by-step” instruction on how to implement the **policy**

A guideline is a User-friendly version of **procedure** that makes it easy for a layman to understand and implement the procedures

Sometimes, people use the term “Procedure & Guideline” interchangeably

So, when putting it all together, you will see that they all link together pretty nicely. A Policy essentially tells you what to do, for example - All sensitive systems shall have suitable access controls. The procedure tells you how to do it, for example - the default access control shall be passwords with minimum 8 alpha numeric characters. A guideline gives user friendly instructions to execute the procedure, for example - tips and tricks on choosing a strong password using 8 alpha numeric characters.

Next, we look at the importance of the ISMS policy.

The ISMS policy is the window through which the world sees your ISMS. The policy spells out your core business functions, why protecting these business functions are important and how you plan to protect it.

The ISMS policy demonstrates the vision and commitment of the organization towards protecting information and information assets. It demonstrates the willingness of the organization to undertake the challenge of protecting sensitive business information.

The ISMS policy sets the tone for the rest of the organization to follow for protecting business information and information assets. The ISMS policy is the principal document from which other functional policies and sub-policies are created.

Next, we will look into the steps that go into creating the information security policies, procedures and guidelines.

The ISMS policies, procedures and guidelines form a nice hierarchical structure as shown in this screen. At the top of the structure you have the “Primary Information Security Policy”, which is, sometimes called the “ISMS Manual”. You may also have a “policy statement”. Under the “Primary Policy”, you will have a set of policies that focus on specific targets such as “End-Users”, “Business Functions” or “Technical Processes”. For executing each of these policies you may choose to write procedures and guidelines.

Let us look at each one of them.

Please note something important. Since, it is very difficult to recreate the actual policy and procedure documents on the screen, please go through the sample documents that is provided in the iSQ World e-Learning portal.

Let us start with the “Primary Information Security Policy”

The contents of the “Primary Information Security Policy” looks like the list in this screen. It consists of, an,

1. An Introduction: That explains, why the organization is implementing an ISMS and the commitment towards the ISMS
2. Reason for adopting ISO 27001 as the ISMS standard
3. The Scope Statement
4. The Information Security Management Team (or Forum)
5. The ISMS implementation model (P-D-C-A approach)
6. The list of specific policies and procedures to support the ISMS
7. Frequency of reviewing the policy
8. Summary

Next, let us look at the “Policy Statement”

- A Policy statement is a brief summarized version of the Information security policy
- The Policy statement is usually used for publishing on the corporate website, displaying in strategic locations such as the visitors' lounge or company brochures
- The Policy Statement is usually signed by the CEO or the Managing Director of the company
- And, the Policy Statement is a good confidence-building as well as marketing tool

Next we shall look at specific policies such as end-user policies, function specific policies and technical policies.

- Specific policies are a sub-set of the Primary Policy
- They exist to support the Primary Policy
- For example
 - The Primary Policy specifies that all sensitive systems shall have access control enabled
 - To support this, we shall create an "Access Control Policy"
 - The Access Control Policy shall cover – "Password Management, Access Cards Management, Bio-Metrics, Physical Access Controls such as locks and keys etc."

Let us look at an example that explains the structure of an "Access Control" policy. The Section 1 of the policy specifies the objective of the policy which is "To ensure all sensitive systems are protected from unauthorized access". Section 2, explains the specific policies within the access control policy such as,

1. Password Policy – That explains the purpose of using and protecting the passwords for accessing computing systems
2. Access Cards Policy – That explains the purpose of using and protecting electronic access cards to enter the facility
3. Physical Access Controls – That explains the purpose of using and protecting locks and keys used to lock cabinets and rooms

Finally, we look at procedures & guidelines.

Procedures & guidelines, explains in a user-friendly manner on how to achieve the targets set by a certain policy

Examples are,

- Procedures & Guidelines for choosing strong passwords

- Procedures & Guidelines for protecting electronic access cards from misuse
- Procedures & guidelines for protecting mobile computing devices

Thank you and don't forget to go through the resources in the iSQ World ISO 27001 e-learning portal.