

Audio transcripts and lesson notes

Hi and welcome. This is Anup Narayanan, your instructor. This chapter gives you a quick overview of the entire ISO 27001 ISMS implementation process. This chapter will be useful if you would like a short overview of the whole process before getting into the details. Before you go ahead, please remember that this course is presented from the perspective of the person who is responsible for implementing the ISO 27001 compliant ISMS in the organization. This chapter also follows the same perspective. It will help you to approach this chapter with the following thought in your mind – “OK!, so these are the steps that I have to follow to implement and certify an ISO 27001 compliant ISMS in my organization”. Please refer the relevant chapter in the “ISO 27001 Essentials” section in the iSQ World e-Learning portal where this approach is explained.

What I am aiming to do in this chapter is to give you a quick overview of the ISMS P-D-C-A implementation model in 8 steps

The steps in an ISMS implementation are,

1. Gap Assessment (this is an optional step)
2. Create the Information Security Management Forum
3. Define the Scope of the ISMS
4. Asset identification and classification
5. Risk Analysis
6. Risk Management
7. Internal Audits
8. Certification audit

The 7 steps link together as follows. You can kick start the ISO 27001 implementation project with a gap analysis. The gap analysis is not an absolute requirement, though it is very helpful to do one. Following this, we start with defining the scope of the ISMS, followed by identifying the important information assets and classifying them. Subsequent to this, a comprehensive risk analysis is executed followed by risk management strategies to mitigate the risks that were identified in the risk analysis stage. After we complete risk mitigation, the next step is to perform a series of internal audits that check whether the risks are mitigated properly or not. After we complete the audits, we do a reality check to see whether we are ready for the certification audit. If we are ready, there are a series of tasks to be executed in order to prepare for the certification audit.

Let us start with Step 1, which is an overview of Gap Assessment or Gap Analysis, whichever way you prefer to call it.

An ISO 27001 Gap Analysis is an examination of your organization's current information security management practices and a benchmarking against the ISO 27001 controls. What this means is that we compare the current information security practices or the current information security posture or the current information security level of the organization against the ISO 27001 standard. This helps us in getting a real picture of where the organization stands with respect to information security and what needs to be done in order to achieve compliance to ISO 27001.

So, what are the benefits of performing a gap analysis? The benefits are,

1. Clear idea of current information security level of the organization
2. List of poor or absent information security controls
3. The possible impact of these poor security controls
4. How much it will cost in terms of MONEY, TIME and PEOPLE to strengthen to implement an ISMS with the necessary controls

Once you get the results of the gap analysis, you can create an action plan. The action plan would include,

1. Prioritize the information security weaknesses to be corrected first
2. Use the "list of prioritization" as an input for the rest of the ISMS implementation

Let us now move to Step 2, "Create the Information Security Management Forum".

The Information Security Management Forum is a high level management team that looks after the implementation, maintenance and improvement of the ISMS. You can call this team using other names such as Information Security Review Committee or the Information Security Management Team etc. The forum looks after the various activities of the ISMS starting from the PLAN phase to the ACT phase. The forum is responsible for reviewing and approving the various activities of the ISMS. You will see more about the tasks of the forum when we learn the PLAN phase.

The forum consists of a chairman, which is usually the CEO or the CFO or someone from the company's top executive team. The forum has an Information Security Officer or a Chief Information Security Officer and representatives from various business functions. Apart from this the forum has a representative from the auditing team, who will report directly to the Chairman of the ISMF. This direct reporting structure is done to ensure that the audit team remains independent and unbiased. You will learn more about the ISMF in the PLAN phase and about Auditing in the "CHECK" phase.

Next, we will take a look at "Step 3 – Define the scope of the ISMS"

Scope definition is the step in which you will specify “exactly what is being protected by the ISMS?”. This usually includes, business functions, information assets in the business functions and the geographical locations that will come under the ISMS program. You have the freedom to define the scope that suits your business which means you can choose to include or exclude a business function. You shall normally include a business function if it is very important. You can exclude a business function if it is not important or if you have a valid reason (lack of resources etc.)

This is what a sample scope looks like. Let me read it out. “The Information Security Management System is deployed for protecting the business information used by the Finance, HR, Research & Development, Sales and Marketing business functions of ACME Inc., #1, North Block, Race Course Drive, New Delhi, India”. As you can see the scope specifies the business functions such as Finance, HR etc. The scope provides a reference to the “business information” used by the business functions and finally it specifies the Geographical location where the scope is implemented. Please note that a scope is always tied to a geographical location.

Step 4 focuses on Asset Identification and Classification. In this step, we shall identify all the information assets that come under the scope, list them and classify them based on their value.

An information asset can be defined as “information that has value to an organization”.

Some examples of information assets are, information (by itself) such as “source code”, components that input information such as “keyboard”, “scanners” etc., components that store information such as “hard disk”, “backup tapes”, “paper documents” etc., components that process information such as “computers”, “application software”, “firewalls” etc., components that transmit information such as “network cables”, “wireless medium”, “Bluetooth” and components that delivers or output information such as monitor, keyboard etc.

You will also notice that most information assets come under 3 categories. They are paper, people and electronic assets. You may be a bit surprised to see “People” being listed as an asset. Well, think of it. A human being takes information as an input by listening to it or reading it, processes it in their brains and then outputs it by talking about it or writing it on paper or typing it in a document or an email. So people are an information asset as well. As we go ahead you will learn more about “Information Assets” in the chapter focusing on the PLAN phase.

Asset identification involves listing all the important information assets in the organization as per the scope. Asset classification is process of classifying the assets in terms of ,

1. Confidentiality
2. Integrity
3. Availability

Let us take a quick example of asset classification by considering a laptop computer. We classify the “Confidentiality” factor of an asset by answering the question, “How sensitive/ secret is the information

in this laptop or how many people are authorized to SEE this information?” The “Integrity” factor is classified by answering the question, “How many people are authorized to CHANGE this information?” and finally the “Availability” factor is classified by answering the question, “What is the duration of TIME, the laptop must be available for access by authorized people?”. More about this, when we learn the PLAN phase.

Next is Step 5, Risk Analysis.

Information security risk analysis is the process of determining the probability of an information asset being compromised (stolen, destroyed, corrupted etc.). This means that you will identify the various possibilities due to which the information assets could be compromised, what would cause these compromises etc. In fact risk analysis is one of the most significant steps in the ISMS implementation as you will see as we move ahead in this training program.

There are a few terminologies that you must keep in mind while performing a risk analysis. These terminologies are,

1 – Information Asset: Which, as you have already seen is an information component of value. An example is a computer used to store business information

2 – Threat: Which is something that can compromise the information asset. An example is a virus

3 – Vulnerability: Which is a weakness that can be exploited by the threat. An example is an “absence of proper signature update of anti-virus”

4 – Probability: Which is the likelihood of the “Threat” exploiting the “Vulnerability”. An example of probability is “Once in 2 years”, which means that there is a likelihood of a virus attack once in 2 years due to the absence of proper update of Anti-virus.

The risk is measured by assigning a qualitative numerical value to all these 4 components. We will learn more about how this is done in the PLAN phase.

Step 6, is Risk Management.

Information security risk management is the process of deploying suitable countermeasures (controls) to reduce the information security risks and protect the information assets.

The information security controls can be broadly classified into 4. They are technical controls such as firewalls, encryption, passwords etc. Physical controls such as lock and key, fire-exits etc. Procedural and legal controls such as laws, rules, policies, guideline etc. And, awareness is also a type of control that deals with human beings who handle information. This involves training human beings or employees on how to handle sensitive information with diligence and care.

One of the biggest advantages of ISO 27001 is that it gives you a comprehensive list of 133 “controls” to mitigate information security risks. These controls cover technical, physical and procedural/ legal as well as awareness.

Step 7 focuses on internal audits.

The internal audit is a pre-certification inspection of the ISMS done by the organization by itself. This is essentially a series of audits undertaken by the organization before the final certification audit.

The purpose of the internal audit is to check the entire ISMS implementation and the effectiveness of the same. Well, you have seen this diagram at the beginning of this chapter.

You must treat the internal audit just like it is a certification audit to derive maximum benefit from it. So, you will have to get the following things ready such as the gap analysis reports, the scope statement, the asset list with the classification, the risk analysis reports, the proof of risk management such as list of controls that are implemented, policies, evidence of physical controls, proof that the ISMS is being reviewed frequently through “minutes of meetings” etc.

The benefits of conducting the internal audits are,

1. You know whether you are ready for certification or not
2. You know how much the ISMS has improved
3. You know the last minute changes to be made
4. You are more confident

The last and the final step is step 8, the “Certification Audit”.

Certification audit is the process whereby an external independent certification body checks the ISMS for compatibility with ISO 27001. If the ISMS is found compatible, the certification body recommends to the accreditation body to issue the ISO 27001 certificate to the organization. For this purpose you will approach a certification body, pay their fees and ask them to audit the ISMS.

There are a few terminologies that may be useful when you approach the certification. A “Certification body” is the organization that performs the certification audit and an “Accreditation body” is the organization that issues the ISO 27001 certificate based on the recommendation by the Certification body. This means that the “Certification Body” after auditing your ISMS will recommend your organization for the ISO 27001 certificate to the “Accreditation Body”.

The certification audit consists of 2 steps. The first step is commonly known as Stage 1 which consists of a review of all reports, policies, scope etc. and an initial audit of the ISMS. An initial list of findings is submitted and corrections recommended. A gap of 1-2 months is provided to the organization to implement the corrections. After this, the Stage 2 audit is conducted which consists of verifying corrections of findings in Stage 1, a second round of ISMS audits and if valid, the organization is recommended for certification.

The documents to be kept ready for the certification audit is similar to the documents to be kept ready for the internal audit. Additionally you are also required to keep the “Statement of Applicability” ready.

Nevertheless, nothing stops you from keeping the “Statement of Applicability” ready for the internal audits as well.

The “Statement of Applicability” is referred to as the SOA. The SOA is a list of all 133 controls and contains an indicator whether you have used a control or not along with the reason for usage or non-usage. For example, if you have used the control “A.5.1.1 – Information Security Policy Document “, then you will mention it in the SOA and assign a justification as to why you have used it along with an indication to the evidence. If you have not used a control, for example the control “A.10.9.1 – Electronic commerce”, then you will mention that in the SOA and justify the reason for not using it. We will focus more on SOA in the PLAN phase.

On successfully completing the audit and after being recommended by the certification body, the organization is issued an ISO 27001 Certificate. Since an ISMS is a continuous process, the ISO 27001 Certification too is a continuous process and the organization must undergo 2 or more audits in the next 3 years. After 3 years, the organization must undergo a “re-certification” process

Thank you and now you have learned in brief the entire ISO 27001 implementation process. In the subsequent chapters, you will learn more about each step of the implementation in depth.