

# Audio transcripts and lesson notes

---

Hello and welcome back. This is Anup Narayanan, your instructor and in this chapter we shall go through the first step in the PLAN phase, Scope Definition.

To make sure, we are now in the PLAN phase.

And, within the PLAN phase we are at Step 1: Defining the scope of the ISMS

So, let us get started.

Scope Definition is the first “Big” decision in the ISMS implementation. This is because the scope determines exactly what is going to be protected and the scope statement is a public document. This means that the scope is visible to your customers, your partners, your employees, the Government and any other interested party. So, make sure that you define the scope with care.

What does the scope convey to someone who is reading it? The scope gives the following information,

- Which are the business functions that are important for your company
- Which are the information and information systems that are to be protected to execute these business functions
- The geographical locations where the scope is applied
- The exclusions (which are the information systems that are not protected)

So, as you can see, the scope gives a picture about your ISMS in a nutshell to the person who is reading it.

Also, there is something very important. The “scope” will be printed on your company’s ISO 27001 certificate. This means that the scope is visible wherever you may choose to display the ISO 27001 certificate, whether it is on the company’s website or physically displayed at the company headquarters or the branch offices.

The features of a good scope are,

- Considers the nature of the organization’s business
- Protects the most strategic business processes
- For example:
  - An advertising agency may choose to protect its creative designs and client data

- A BPO may choose to protect the IT and associated Information Systems

Let us continue looking at more features of a good scope. A good scope will specify the,

- The specific locations that are covered under the scope
- For example, if a company has 10 branch offices and a head office, the scope should clearly mention whether,
  - Only the head office is covered
  - Head office and all branch offices are covered
  - Head office and only a few branches are covered
  - Only a few branches are covered
  - Etc...

There are even more features to a good scope. A good scope will also explain,

- The business processes and associated information systems that are not covered
- The reason why they are excluded

You must also note that it is not mandatory to mention the exclusions in the actual scope statement that is printed on the certificate, but the exclusions must be documented to show to the auditors or interested parties.

You can choose what to include or exclude in the scope by using various criterion. In normal cases you will include all business functions that are very important for the business. You can exclude a business function if it is not important or if you have a valid reason such as lack of resources, time or if the business function is new and you feel that it needs time to settle down.

So, what does a scope statement look like? We shall look at a few examples. Let us first read the scope statement of a company that manufactures and sells televisions. The scope statement reads as follows – “The Information Security Management System is deployed for protecting the business information used for the manufacture and sales of Television sets. This information is used by the Finance, HR, Research & Development, Sales and Marketing divisions of ACME Inc., #1, North Block, Race Course Drive, New Delhi, India”

As you can see, the scope statement lays special importance on “manufacture and sales” of television sets. The scope statement also mentions all the other departments such as Finance, HR, Research & Development and Marketing that uses sensitive business information. So, a reader of the scope will understand that the principal focus of the company is television manufacturing and sales and the company is protecting all the relevant business functions that supports the principal business function.

Let us next read the scope statement of an IT Services company. The scope reads as follows – “For protecting the information and information systems used for data processing, data storage, network and system administration for delivering IT services of ProSolutions, Ho Chi Minh City, Vietnam”. As you can see the scope focuses exclusively on the Information Technology functions. So, the reader of this scope will infer that the core IT business function is suitably protected from information security threats. The company has chosen not to mention whether other business functions such as HR or Finance or Marketing is being covered under the scope or not. It could be that they are covering it or not covering it, but they have taken a decision to tell the reader of the scope that their core focus is on their principal business function, which is, IT services.

Let us next read the scope of an “Advertising Consulting” company. The scope reads as follows – “Creative media has deployed the Information Security Management System for protecting licensed and copyrighted information used by the “Designs & Products” department for creation of advertisements for our customers. The information security management system is applied at Creative Media, New Drive, Boston, USA”. By reading this scope it is clear that the company has understood that protecting “licensed and copyrighted information” is the most important aspect to be taken care of.

Let us now read the scope of a hospital that stores patient health records. The scope reads as follows – “City Hospital, London, UK has deployed the Information Security Management System for protecting the patient health records from unauthorized disclosure and modification.” As you can see, the scope is very simple and precise and conveys the fact that the patient health records are being protected. Again, this organization may be having other business functions also under the scope, but they have not mentioned it explicitly and have kept the scope short and sweet.

Let us next look at “Writing the Scope”

First, start with a pictorial scope. The pictorial scope is a set of 3 concentric ovals. The oval at the center has the “name of the company”. The next oval focuses on the inclusions or rather, “what is part of the scope”. The 3<sup>rd</sup> oval focuses on the exclusion or rather, “what is not part of the scope”.

A pictorial scope has several advantages. It,

- Helps to visualize the scope before putting it into words
- Explains clearly the “Exclusions” and “Inclusions”
- Easy to explain to the Senior Managers, Customers and Auditors

Now, let us look at a case study for writing the ISMS scope for an IT services company.

In step 1, principal business functions are listed and a decision is taken on what to exclude or not to exclude. In this case the company has decided to include Data Center Services, Human Resources, Finance and Accounts, Administration and Sales because they are essential business services whereas they have decided to exclude Marketing because the marketing process is currently

outsourced to a 3<sup>rd</sup> party. But, still the company has decided that the Marketing function will be included in the next year.

In step 2, the pictorial scope is drawn and as you can see the inclusions are mentioned in the 2<sup>nd</sup> oval and the exclusions in the 3<sup>rd</sup> oval.

In step 3, the scope is written in words. The scope reads as follows – “ProSolutions IT Services has designed and implemented the Information Security Management System for protecting the information used for providing essential IT services. The ISMS is applicable at the ProSolutions IT Services head office at #1, South Drive, New Jersey, USA”. As you can see this is a clean and crisp scope and mentions that the ISMS “protects the information used for providing essential IT services”. So, if someone were to read it, they will understand that the company has protected the core business function, which is IT services.

In step 4, the reason for the exclusion is provided. This reads as follows – “The “Marketing” business functions has been outsourced to “M-outsourcing Inc.”. ProSolutions IT services is currently in the process of explaining and training “M-outsourcing Inc.” about the information security policies followed by ProSolutions. Once this is completed, “M-outsourcing Inc.” shall be given a 6 month time-frame to comply to the information security policies of ProSolutions. Subsequent to this, the “Marketing” business function shall be added to the ISMS Scope.”

Now, there is a very valuable lesson to be learned here. When you exclude something from the scope, you will not just forget about it, but rather do everything possible to still protect it as best as possible.

In the scope, though the “Marketing” business function is outsourced and not part of the scope, the company has not ignored it. In the previous screen, while explaining the exclusions, they have mentioned that they are taking all necessary steps to include this business function in the scope as soon as possible by providing necessary training to the outsourced company. Hence, you must realize that when you exclude something from the scope, you do not ignore it, but rather you will do everything within the powers of the organization to suitably protect the business function.

Please note that,

- It is not necessary that the “Exclusions” have to be published
- But it should be documented and explained in case of queries from the managers, customers, auditors and/or other interested parties

So, please document the reasons for exclusion and keep it safe.

Let us look at another case study, writing the ISMS scope for an e-Learning company

In step 1, we will list the inclusions and exclusions. As you can see, the principal business functions such as content development, quality control, finance and accounts and marketing is included. The

hosting of the e-learning content i.e. the server on which the e-learning content is hosted is excluded because the hosting is managed by a 3<sup>rd</sup> party company.

In step 2, we draw the pictorial scope that explains the inclusions as well as exclusions. You can see that the “E-learning content hosting” is excluded.

In step 3, we write the scope, which reads as follows – “For protecting the information and information assets that is used for creating, delivering and managing e-Learning services of Genesis e-Learning Inc., North-West Drive, Michigan, USA”. As you can see, the scope focuses on the principal business functions.

In step 4, the company has explained the reason for excluding the “content hosting” business function. This reads as follows – “The “Content Hosting” business function has been outsourced to “Excellent Hosting Services”. Genesis e-Learning Inc. has limited control over the information security infrastructure of “Excellent Hosting Services”. In spite of this, Genesis has taken the following measures in the servers that host the e-Learning content. These measures are, hardening the server, hosting an internal firewall in the server, conducting monthly penetration tests, regular patching and updates. Apart from this, Genesis has signed an NDA (Non-Disclosure Agreement) with “Excellent Hosting Services”.

Here we repeat the same valuable lesson that we learned from the previous scope. Though the content hosting function is excluded, the company has still taken all reasonable precautions to protect the content and the server through hardening, internal firewall, conducting penetration tests, regular patching and updates and an NDA. So, when you have an “exclusion” it does not mean that you just forget about it. You will still take all reasonable precautions to protect the excluded business function.

Thank you and we shall interact again soon in the next chapter.