

Audio transcripts and lesson notes

Hi, this is Anup Narayanan, your instructor and in this chapter we shall look at the structure of ISO 27001. I suggest that you purchase a copy of the ISO 27001 standard. Once you go through the standard, you will be able to appreciate this chapter and the rest of this course more. When you read through the actual ISO 27001 standard document, you may feel a little confused about what it is all about and how the different parts of the standard link with each other. For example you have parts 4, 5, 6, 7 and 8 of the standard that are mandatory requirements and then you have Annex A, that has 133 controls grouped into 11 domains. This chapter is an attempt to link the different parts of the standard together and explain it in simple terms.

For learning purpose let us divide ISO 27001 into 2 sections - *Section 1* and *Section 2*. Please note that I have used the terms Section 1 and Section 2 for learning purposes only. Section 1 consists of a set of mandatory requirements, that explains how to build the ISMS in the PDCA Model. In the ISO 27001 standard these are Parts 4,5,6,7 and 8 and you will see this when you read the ISO 27001 standard document. These mandatory requirements are nothing but the PDCA model in itself. When you implement ISO 27001, you are essentially building a PDCA model based management system and you must prove this to the auditor at the time of certification. Specifically you must prove that you have implemented the PDCA model and that you are continuously executing each component of the PDCA model. Section 2 consists of Control Objectives and Controls. In the ISO 27001 standard this is Annex A. “Controls” are essentially “information security safeguards”. For example, an “anti-virus” is a control, an “information Security training program” is a control, or a “change management process” is a control. “Control Objectives” specify the aim for using a control or a set of controls. ISO 27001 provides a set of 133 controls that you can use to build your ISMS. Now! this is what you must remember. There is a very simple relationship between Section 1 and Section 2. Section 1, tells you how to build the ISMS and Section 2 gives you a set of controls that you can use to build the ISMS.

Let us refresh once more. Section 1 consists of the mandatory requirements for building and managing the ISMS as per the PDCA model. In fact, if you wish to, please go through the video, “ISMS and ISO 27001” in the previous chapter to understand the P-D-C-A model once more.

And, section 2, provides a list of Controls and Control Objectives that can be used to build the ISMS as specified by Section 1.

Let us look at a few examples that explain the relationship between Section 1 and Section 2. If you read through the standard, you will see the “Part 4.2 - Define an ISMS policy in terms of the characteristics of the business,”.. Now, if you are looking at some more information on how to go about this, you can use the control in Section 2, which is “Annex A - A.5.1 Information Security policy document”.

Another example is the relationship between “Part 5.1” of the standard which specifies “Management commitment” and “Annex A - A.6.1.1”, that provides a control called “Management commitment to information security”. So, you will satisfy requirement specified by Section 5.1 of the standard by implementing the control A.6.1.1. Please remember that it may not be possible to draw an accurate link between Section 1 and Section 2 every time. So don’t expect an “apple-to-apple” comparison, but you will notice that the Section 2 is quite comprehensive and provides detailed controls for implementing the specifications set forth by Section 1.

It is also important to remember that adhering to Section 1 is mandatory, which is, you must prove that an ISMS exists and is working as per the PDCA model. To achieve this you may use controls from Section 2, but it is not mandatory to use all the controls or you can even use controls that are not listed in ISO 27001. It may be even impossible to use all controls as some of them may not fit your business. For example, if you are an advertising business, you may find that the controls pertaining to software development may not be valid for your business.

You can decide to avoid certain controls based on various reasons. The reasons could be Management of the company has decided to accept the risk and hence there is no need for implementing the control. It could be that there are alternative arrangements in place. It could even be that the “Time, Money and Resources” are not currently available for implementing certain controls. It could also be because of geographical factors or other valid or justifiable reasons. We will discuss this more in the later parts of this course when we cover the PLAN phase.

There are 133 controls in ISO 27001 and they are divided into 11 domains. We will learn more about controls in the Risk Analysis and Risk Treatment chapters

In the next chapter we shall quickly go through the steps in an ISO 27001 implementation project before we start with the real thing.

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