

Audio transcripts and lesson notes

Hi, this is Anup Narayanan, your instructor and in this chapter we shall look more in-depth at ISMS and ISO 27001. Meanwhile, I hope you have gone through the previous chapters, because it is essential that you do so in order to effectively understand the contents of this chapter.

Let us start with the term ISMS. There are many definitions of ISMS, but I prefer to stick to something very simple. An ISMS is a management framework for identifying important information, continuously evaluating security risks to this important information and taking reasonable steps to protect this important information. You will notice a cyclical structure in this screen depicting the model for an ISMS and the words, P-D-C-A around it. I will explain this as we move ahead in this chapter.

An ISMS is a continuous process and lasts throughout the life of the business. This is because a good management system always keeps on improving itself. As the famous saying goes, “The biggest room in the world is the room for improvement”. Improvement is a never ending process and an ISMS always tries to improve by reducing security risks to important business information.

Let me emphasize the word “Improvement” once more. This is because it is impossible to attain 100% security. What you must try to do is to continuously reduce the gap between 100% perfection or 100% security and the current level of security provided by the ISMS.

So, let us assume that if your ISMS is 99% perfect, you will strive to move to 99.9%, then to 99.99% and then to 99.999% and it goes on till you reduce the gap between “absolute perfection” and the current level you are at.

To pursue perfection, you will improve and repeat the ISMS cycle. This explains, the cyclical model of the ISMS.

Let us look more closely at the components of an ISMS. The ISMS consists of 4 steps, PLAN, DO, CHECK and ACT. This is usually referred to as the P-D-C-A model. The PLAN phase is where we Identify information to be protected, analyze risks to the information and define a risk treatment plan. In the DO phase, we shall implement the risk treatment plan. In the CHECK phase, we shall review and evaluate the performance of the ISMS by checking the effectiveness of the Risk Treatment plan. Finally in the ACT Phase, we shall make necessary corrections and improve the process.

Now you can see, the P-D-C-A model fits into a nice cyclical framework and each phase feeds from the other. This is what we had seen earlier in this chapter where I had shown the same diagram.

The P-D-C-A model is an internationally accepted model and followed by most well known standards and management systems. The P-D-C-A model is also called the Deming Cycle after the founder [Dr. W. Edwards Deming](#)

Now, what is ISO 27001? And, what is the relationship between an ISMS and ISO 27001? ISO 27001 is an international standard that provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an ISMS. To keep it simple, you will use ISO 27001 to create and manage your ISMS. It is a reference or a tool or a guideline for your ISMS. The full name of the standard is ISO/IEC 27001: 2005, but we will just use the term ISO 27001 in this course.

ISO 27001 adheres to the PDCA model and is in all probability the most widely used standard for ISMS implementation in the world.

Now, why is ISO 27001 popular? There are quite a few reasons. One of the main reasons is because it is a certifiable standard. An organization can implement an ISO 27001 compliant ISMS and get it certified through an “Accredited Certification Body”. ISO 27001 Certification enhances the profile and image of an organization. ISO 27001 certification gives confidence to customers. This is because customers feel more confident in doing business with an organization that protects valuable business information. We will cover more about this in the chapter focusing on “Certification”.

Let us take a brief look into how ISO 27001 evolved. In 1992 , the Department of Trade and Industry, UK, published the 'Code of Practice for Information Security Management'. In 1995, it was amended and re-published by the British Standards Institute as BS7799, where BS stands for British Standard. In 1999 , the 1st major revision of BS7799 was published. In 2000, BS7799 became ISO 17799, which is a code of practice. In 2002, BS7799-2 was published. It was a “Specification for Information Security Management System” and Certifiable. In 2005 , the new version of ISO 17799 was published and again in 2005, BS7799-2 became ISO 27001.

In fact there is a whole family of ISO 27000 standards. You have seen ISO/ IEC 27001: 2005 which is the Information Security Management System requirements standard or specification. [ISO/IEC 27002:2005](#) is the code of practice for information security management, formerly known as ISO 17799. [ISO/IEC 27003](#) will provide implementation guidance for ISO/IEC 27001. [ISO/IEC 27004](#) will be an information security management measurement standard. [ISO/IEC 27005:2008](#) is a new information security risk management standard. This information was accurate at the time of producing this chapter and we shall update it as and when we create a newer version.

The ISO 27001 Implementation process adheres to the ISMS implementation steps that we discussed earlier. There are well defined guidelines for each phase i.e. PLAN, DO, CHECK and ACT. This means that when you implement ISO 27001 you will be following a P-D-C-A approach. Let us look at the specific steps to be executed in each of the 4 phases.

In the PLAN phase, you will focus on establishing the ISMS. This consists of,

1. Defining the Scope of the ISMS
2. Defining the ISMS Policy
3. Defining the Risk Assessment Approach of the organization

4. Identifying the risks
5. Analyzing risk treatment options
6. Selecting control objectives and controls for treatment of risks
7. Obtaining Management approval and authorization for risk treatment and residual risks
8. Preparing "Statement of Applicability"

Now, don't worry about all these steps because we are going to learn each of them in detail during the rest of this training program.

In the DO phase, we will focus on implementing and operating the ISMS. This consists of,

1. Defining and implementing a Risk Treatment Plan
2. Selecting appropriate controls
3. Defining how to measure the effectiveness of the controls
4. Implementing training and awareness programs
5. Managing the operation of the ISMS
6. Managing the resources for operating the ISMS
7. Implementing security incident detection and response procedures

Again, let me remind you that we will learn all these steps in detail in the training program.

Next, we focus on the CHECK phase, which consists of,

1. Executing monitoring and reviewing procedures
2. Measuring the effectiveness of controls
3. Reviewing risk assessments and reviewing residual risks
4. Conducting internal ISMS audits
5. Undertaking management review of the ISMS
6. Updating security plans based on review and findings
7. Recording actions and events that may have an impact on the performance of the ISMS

And finally, we come to the ACT phase, which focuses on maintaining and improving the ISMS. The steps in this phase are,

1. Implement the identified improvements in the ISMS
2. Taking appropriate corrective and preventive actions
3. Communicate the actions and improvements to all relevant parties
4. Ensure that the improvements achieve their intended objectives

In the next chapter, you shall learn more about the structure of ISO 27001

Thank you and please make sure you go through all the resources available in the iSQ World ISO 27001 e-learning portal.