

Audio transcripts and lesson notes

Hi, this is Anup Narayanan and let us get started with the chapter on gap analysis. It is a great idea to do a gap analysis so that you know where you stand before actually getting into the ISMS implementation. But, it is not mandatory to do a gap analysis if you already have an idea about what you are trying to protect by implementing an ISMS. So it is up to you to decide whether you want to do a gap analysis or not. I will present the benefits of a gap analysis in this chapter so that you can take this decision yourself.

Let us define gap analysis. Gap analysis is the identification of the difference between the current level of information security your organization has and the information security that the organization wants to have (or the level of information security normally practiced by the industry)

Let us look at an example of an “Information Security Gap”.

- Industry best practice for passwords are – Minimum 8 characters with a mix of alphanumeric characters and symbols
- Whereas, your organization is only following minimum 6 characters without stress on alphanumeric characters

So, here you have a gap because you are not following the industry best practices.

Let us look at the importance of a gap analysis.

1. A gap analysis is often the first “Reality Check” of your organization’s information security management
2. The analysis shows where you stand in comparison to “more secure” organizations
3. The gap analysis report can be used to push or promote the ISO 27001 compliant ISMS to your top management
4. The gap analysis report can provide strong reasons to justify an ISMS
5. The gap Analysis findings can provide an approximate cost and effort estimate for implementing an ISO 27001 compliant ISMS

As you can see, the gap analysis is a strong starting point for getting sanction and approval for your ISMS.

Let us now look at the various steps of performing the gap analysis.

There are two approaches for performing the gap analysis depending on the time and resources that you have. In approach 1, you can do a gap analysis covering the whole organization or in approach 2, you can do the gap analysis covering only one business function. You can also combine both approaches whereby you do a gap analysis of the whole organization and you do a more in-depth gap analysis of a very critical business function.

Let us start with approach 1, where we do a gap analysis covering the whole organization.

In both our approaches we will adhere to the following steps,

1. We will use the ISO 27001 controls as the benchmark
2. We will do a survey of the organization using the ISO 27001 controls as the benchmark
3. We will do this using the spreadsheet tool that is provided along with this chapter
4. We also have a video that explains how this is done

Please make sure that you go through the video that explains how the gap analysis is done covering the whole organization.

I have a few screenshots here from the video that shows the gap analysis spreadsheet

A few more screenshots here...

In approach 2, we shall do a gap analysis of a specific business function.

The steps in approach 2 are similar to the steps in approach 1, except that we focus on a specific business function rather than the whole organization. Also, as explained earlier you can combine both approaches for a very effective gap analysis. We have a separate video for approach 2, in the e-learning portal and I request you to go through the same.

Here, you can see a screenshot that shows approach 2 and you will learn more in the video.

Before I end this chapter, I want you to know that you can use Gap Analysis reports while defining the Risk Treatment plan.

There are two inputs to the risk treatment plan. They are gap analysis report and risk analysis report. You will learn more about risk treatment plan in the PLAN phase.

Thank you and don't forget to go through videos that demonstrate the performance of gap analysis in the iSQ World ISO 27001 e-learning portal.