

# Audio transcripts and lesson notes

---

Hi, this is Anup Narayanan and in this chapter we shall define the risk assessment approach using which we shall identify risks to information assets.

Before we proceed, let us note the following. We will use the terms “Risk Assessment” and “Risk Analysis” interchangeably. Both mean the same in the context of this course

It is my duty to remind you about where we are now in the whole course. We are now in the PLAN phase.

Within the PLAN phase we are now at the step of defining the Risk Assessment approach

Let us get started by understanding the different terms and definitions within risk assessment

The terms that you must know are,

1. **(Information) Asset:** Information of value which is owned and/or used by an organization ( Please note we shall use the term “Asset” for the sake of ease in the rest of this course)
2. **Vulnerability:** A weakness in the asset that can be exploited
3. **Threat:** An agent or an event that can exploit the vulnerability
4. **Impact:** The consequence (damage) if the threat exploits the vulnerability
5. **Probability of occurrence:** The possible number of times the threat can exploit the vulnerability in a given time period
6. **Risk:** The final impact. Expressed as a mathematical term that combines,
  - a) The value of the asset
  - b) The probability of occurrence (threat exploiting the vulnerability)
  - c) The impact of the threat exploiting the vulnerability
7. Let us look at these terms in a practical sense. A “car” is an example of an “asset”. A door lock that is not working properly and the fact that there is no burglar alarm is an example of “vulnerability”. A thief in the neighborhood is a “threat”. The “impact” of the “threat” exploiting the “vulnerability”, i.e. the car actually being stolen is financial loss, mental strain and loss of time. I have mentioned loss of time because in this case you will have to spend time on filling up insurance claims, filing a case with the police, the time to buy a new car and even the excess time that you spend on other modes of transport whereas earlier you could have just got

into your car and zipped away. The “probability of occurrence” of such a theft could be once in 5 years. The “risk” is now calculated by combining all these factors i.e. the value of the “asset”, “impact” and “probability of occurrence”. When we do the real risk analysis we assign a numerical value to the “asset”, “impact” and “probability of occurrence” to arrive at a numerical value for the “risk”. We shall see how this is done when we do the actual risk assessment.

Let us look at another example from an “information” perspective. In this example, the “asset” is a computer storing business information. The “vulnerability” is the fact that the anti-virus is not being constantly updated. “Threats” in this case are malware such as worms, viruses and Trojans. The “impact” of the “threat” exploiting the vulnerability, in this case a virus attack could be data loss, financial loss, mental strain and loss of time. The “probability of occurrence” could be once in 2 years. The risk is now calculated by assigning numerical values to the value of the “asset”, “impact” and probability of occurrence. Again, let me remind you that we will learn this in the risk assessment chapter.

Let us now define “Risk Assessment”. Risk assessment is the process of identifying risks using a pre-defined **“approach”**. In this case we shall use a pre-defined **“approach”** to identify information security risks

Now we will learn the risk assessment approach in-depth

The approach that we will use is an “Asset based risk assessment”. In this approach we shall assess the risks to information assets in each department or business function within the scope. For example, the business functions could be sales, HR, support or quality control. The assets in each of these business functions could be computers, paper, people etc. Using the asset based risk assessment approach we shall identify information security risks to each of these information assets.

There are certain advantages to the “asset-based” risk assessment approach.

Using this approach we get a specific understanding of the risks pertaining to each information asset. For example, risks could be data loss due to a hard disk crash or data theft from a computer.

So, how to do the “asset based” risk assessment?

The steps in the “asset-based” risk assessment are,

Step 1 - Identify business functions within the scope

Step 2 - List and identify the value of assets in each business function

Step 3 - Identify the threats that can affect the asset

Step 4 - Identify the vulnerabilities that can be exploited by the threats

Step 5 - Identify the impact

Step 6 - Identify the probability of occurrence

Step 7 - Calculate the risk

Now you are able to see how the different terminologies such as “asset”, “vulnerability”, “threat”, “probability of occurrence” and “risk” align together. In the next chapter we shall go through each of these steps thoroughly and we shall also see how to use the “risk analysis” tool provided along with this course.

Now, there is an important fact that you must note. Remember that we have done a gap analysis earlier. It is important that we use the results of gap analysis in coordination with the risk assessment reports to effectively mitigate the risks.

You have seen this screen earlier in the gap analysis chapter. It is important to note that in the final risk treatment plan we will consider the gap analysis findings along with the risk analysis report.

The reason is because the gap analysis report gives an overall view of risks either from a business perspective or a departmental perspective.

The risk assessment provides a specific understanding of risks at an individual asset level.

Combining the gap analysis report along with the risk analysis report gives a wholesome analysis of risks.

Hence the final risk treatment plan will consider both the gap as well as risk analysis reports. We shall see this in-depth during the risk assessment chapter.

Thank you and please go through the additional resources in the iSQ World ISO 27001 e-Learning portal.