

Audio transcripts and lesson notes

Hello and welcome back. This is your instructor Anup Narayanan. This is an important chapter where we focus on doing the risk analysis, which is central to the whole ISMS process.

Let us quickly remind ourselves about where we are. We are in the PLAN phase.

And, within the PLAN phase we are at step 4, which is “identifying the risks”

The first step in risk assessment is to get your tools ready.

In this case we shall use a simple and automated risk analysis spreadsheet that is provided along with this course. Please check the iSQ World e-Learning portal and download this tool. In fact, we will be using this tool a lot.

The spreadsheet provides a comprehensive view that links all components of the risk analysis which includes “asset”, “asset value”, “threat”, “vulnerability”, “impact”, “probability” and “risk”. We shall be learning this in-depth in this chapter.

Let us now get started with doing the risk assessment.

We have seen the 7 steps of risk assessment in the previous chapter “defining the risk assessment approach”. We will now start with step 1, that focuses on identifying the business functions within the scope.

Let us take a look at a sample scope which reads as follows – “The Information Security Management System is deployed for protecting the business information used for providing web hosting services of “We Host” Inc., Drive #1, North Heights, Illinois, USA. The business functions or “inclusions” within the scope are IT, HR and Admin. Let me give you a tip here. Please go through the chapter on “Scope Definition” to understand “inclusions” and “exclusions” if you would like to.

Next, in the spreadsheet we create a workbook for each business function. In this case, this is already created in the spreadsheet.

In step 2, we will list and identify the value of assets in each business function.

We have seen the definition of “asset” earlier. But, let us define an “asset” in the context of ISO 27001. An asset can be defined as,

- Something that stores Information (Hard disk/ Tape backup) or,
- Something that processes Information (Computer) or,
- Something that transmits information (Bandwidth) or,

- Something that displays/ outputs information (Monitor/ Printer)

For the sake of ease and simplicity you can use the following classification and arrangement of assets. There are various ways in which you can classify assets. These classifications are,

- “Hardware” – The assets that will come under this category are Servers, Laptops, Computers, Switches, Routers etc.
- “Software” or “Application” – The assets that will come under this category are Operating System, Email Client, Anti-virus software, firewall etc.
- “Paper” – The assets that will come under this category are Memos, Notes, Installation manuals, Legal agreements etc.
- Another category is “Electronic” – The assets that will come under this category are Fax, Telephone etc.
- The next category is “Service” – The assets that will come under this category are Internet bandwidth, Anti-virus update service, Web hosting service etc.
- Next category is “People” – The assets that come under this category are all employees and their roles such as CEO, IT Administrator, HR Manager etc.
- Next category is “Physical Assets” – The assets that come under this category are Information storage vaults, cabinets etc.

Please note that you can use your own logic for classifying and arranging assets

This is how the different assets will appear in the spreadsheet. If you notice, the red arrow shows the “Asset column” that lists all assets, whereas the green arrow shows the different asset categories such as “People”, “Hardware” assets etc. The different asset categories are listed together as indicated by the red dotted boxes that shows how “people” assets are listed together and also how “service” assets are listed together.

The next step in this phase is the identification of “asset” owners.

The owner is usually,

- The person directly responsible for the asset
- The person who uses the asset almost on a day-to-day basis

You can also use an additional term – “Custodian”, though this is not mandatory. There are some differences between “Owner” and “Custodian”. The owner is the sole responsible person for an asset. An example is an IT Manager. The owner assigns the asset to a custodian for usage and an example of this is when the IT Manager assigns a computer to a business executive.

Please note that when it comes to “human assets” or “employees”, the owner is usually the people they report to

This is how we list the owners in the spreadsheet. Please see the red dotted box that shows how the owners are listed against each asset.

The next step is to determine the value of the asset

An “Asset” is valued using 3 criterion. They are “Confidentiality”, “Integrity” and “Availability”.

Let us look at some definitions now.

- Confidentiality is defined as ensuring that the information is accessible only to those who have authorized access
- Integrity is defined as ensuring that the information is modified only by those who have authorized access, and,
- Availability is defined as ensuring that the information is accessible and usable for those who have authorized access

It is also important to learn the term “C-I-A” triad. Protection of information essentially means protecting the “Confidentiality, Integrity and Availability” of Information. This is called the “C-I-A triad”. Please note that a “Triad” is a three way relationship, in this case the relationship between C, I and A

Next, we calculate the value of the asset using the C-I-A triad.

- First, we measure the “Confidentiality” of the information (asset)
- We rate the “Confidentiality” on a scale of 0-3, where
 - 0 means not valid or not confidential at all
 - 1 means “low” confidentiality or that the (Information) asset is accessible to most people
 - 2 means “medium” confidentiality or that the (Information) asset is accessible to a select group of people
 - 3 means “high” confidentiality or that the (Information) asset is accessible only to the owner or to a limited set of people

In order to measure “Confidentiality” let me give you some tips.

- Ask yourselves these questions,
 - How many people must be given access to this (Information) asset? (or)

- How many people must this (Information) asset reveal information to? (or)
- How secret is the information stored and processed by this asset?

Let us look at an example,

If you have an email server as an asset, you can ask the question “how many people must be given access to this server?”. If the answer is “all employees, but not anyone else as the email server stores sensitive business information”, you can rate the “Confidentiality” as “High”. If you are considering the asset, “company web-site”, you can ask the question “how secret is the information stored and processed by this asset?”. If the answer is that “information is accessible to all viewers”, you can rate the “Confidentiality” as “Low”. If you are considering a human asset such as an “HR Manager”, you will re-phrase the question slightly as “how many people must this asset reveal business information to?” or “how secret is the information stored and processed by this asset?”. If the answer is that the asset stores and processes employee records and salary (compensation information) that has some privacy concerns you may choose to rate the “Confidentiality” as “Medium”.

The “Confidentiality” value is captured in the Spreadsheet

- Second, we measure the “Integrity” of the information (asset)
- We rate the “Integrity” on a scale of 0-3
 - 0 means, not valid or information is changeable (modifiable) by all
 - 1 means, “low” integrity or that the information is to changeable (modifiable) by most people
 - 2 means, “medium” integrity or that the information is changeable (modifiable) by a select group of people
 - 3 means, “high” integrity or that the information is changeable (modifiable) only by the owner or a limited set of people

Let me share some tips that will help you to measure integrity with greater clarity.

- Ask yourselves these questions,
 - How many people can modify the (information) asset? (or)
 - How modifiable is the information used by this asset?
 - What is the level of “honesty” and diligence expected by this asset while modifying information?

Let us use the same set of assets that we used earlier and measure the “integrity value”. In the case of the email server we ask the question “How many people can modify the (information) asset?” and if the

answer is “No one, once and email is sent, the email should not be modified”, then you can rate the integrity value as “high”. In the case of the company web-site we can ask the question “How modifiable is the information used by this asset?” and if the answer is “Modifiable only by the administrator and no one else. Administrator can modify only after approval”, then we can rate the integrity as “high” again. In the case of HR manager we can ask the question “What is the level of “honesty” and “diligence” expected by this asset while modifying information?” and if the answer is “Very high since the HR Manager handles employees’ personal and salary information”, we can rate the integrity as “high” again.

The “Integrity” value is captured in the spreadsheet

- Third, we measure the “Availability” of the information (asset)
- We rate the “Availability” on a scale of 0-3
 - 0 means, no requirement for continuous availability
 - 1 means, low availability or long periods of unavailability is tolerable
 - 2 means, medium availability or short periods of unavailability is tolerable or the asset must be available most of the time
 - 3 means, high availability or information must be available to the maximum extent possible (close to 99.99%)

Let me give you some tips to measure availability.

- Ask yourselves these questions,
 - What is the % of time the (information) asset must be made available?
 - How tolerable is the downtime for this information asset?
 - Is an alternate asset required if this asset is not available?

Let us apply the principle of availability to the same set of examples seen earlier. In the case of the email server we ask the questions, “What is the % of time this (information) asset must be available?” and if the answer is “most of the time, since most business communication is done through email”, we can rate the availability as “high”. In the case of the asset, “company web-site” we can ask the question “How tolerable is the downtime for this information asset?”, and if the answer is “Slightly tolerable, since the corporate website is for information purposes only. But, a downtime still affects the image of the company”, we can rate the availability as “medium”. In the case of the asset, HR manager, we can ask the question “Is an alternate asset required if this asset is not available?”, and if the answer is “Yes, since the HR manager is the key to various employee recruitment and management processes”, we can rate the availability as “high”.

The “Availability” value is captured in the Spreadsheet

Finally we calculate the “Net Value” of the asset by adding the individual values of “Confidentiality”, “Integrity” and “Availability”

Next, we move on to step 3 where we will identify threats that can affect the asset.

Let us refresh our memory. A threat is an agent or an event that can exploit the vulnerability

In chapter, “Defining the Risk Assessment Approach”, we have seen this example from real life. In this case, the threat is the thief in the neighborhood.

We have also seen this example where we identified threats to an “information asset”, in this case a computer. The threat in this case is a malware such as worm, virus or a Trojan.

Now, I want you to focus and listen very carefully. We will use a simplified approach for listing threats in order to make our risk assessment precise and clear.

The list of threats that we will use are,

- Destruction
- Corruption
- Underperformance
- Aging
- Unavailability

Now, you may ask, why such a simple list of threats. The reasons are,

- To keep the Risk Assessment sheet “NEAT” and “SIMPLE”
- To enable “CLARITY” of thinking
- To assess vulnerabilities more effectively, that we will see in the next step

So, let us look at an example of keeping threats simple. Look at the table in this screen. “Influenza outbreak” due to which employees may be unavailable to attend work is a threat. But here we focus on the key event, which is “Unavailability”. Similarly a “hard disk crash” on server due to which some data is lost and the server is unavailable is a threat, but the key event here is again “Unavailability”. Similarly “accidental deletion of data” by employees is a threat but the net effect is, “destruction”, specifically in this case “destruction of data”. Another threat is where “configuration management documents are not updated” and the result is “aging”, due to which the document may not be usable when it is really required. Another threat is “poor internet bandwidth”, the net effect of which is “Underperformance”.

Now, ask yourself one question. Which is easier? Listing all the threats in the world or bringing them under a simple list of threat categories? If you try to list all possible threats, the list could be endless and you could get confused.

Threat analysis will be all the more simple if you can consider 5 principal threat categories, which are, as mentioned before,

1. Destruction
2. Corruption
3. Underperformance
4. Aging
5. Unavailability

You will notice that almost all threats will fall under the above 5 categories.

How will you apply these threat categories to an information asset. It is very simple. Take the information asset and ask the 1st smart question. "Is there a "threat" of?"

1. Destruction
2. Corruption
3. Underperformance
4. Aging
5. Unavailability

This will make you explore all possible threats.

Now, ask the 2nd smart question - "What could be the reason.....?" Here you will see that you are able to list all possible reasons with clarity. For example, destruction could be due to physical accident, corruption could be due to hard disk crash, underperformance could be due to malfunction, aging could be due to poor maintenance and finally unavailability could be due to theft.

So, rather than filling the spreadsheet with too much information, you have now found a way to keep the list of threats simple.

So, it is a simple list of threats that we shall list in the Risk Analysis spreadsheet

But, how will you make people understand your logic? The answer is, use the "Comment" column to elaborate the reason for the threat. This way you satisfy your audience as well.

The next step is "Vulnerability" identification.

Let us recap. A vulnerability is a weakness in the asset that can be exploited by a threat.

In this example, as you have seen before, an example of a vulnerability is a door lock not working properly and that there is no burglar alarm.

An in this example that you have seen before, the vulnerability is an “anti-virus” is not being constantly updated.

Let us see how we can identify vulnerabilities?

Step 1 : Take the earlier list of “Assets” and “Threats”

Step 2: Ask yourself which are the “vulnerabilities” that can be exploited by the “threats”?

In this example, we are considering the assets “Sales Manager” and “Source code repository server”. The threats are “unavailability” due to “influenza outbreak” for the “Sales Manager” and “unavailability” and “corruption” due to “hard disk crash” for the “Source code repository server”. Now, take a look at the list of “vulnerabilities” that can be exploited by the “threats”. In the case of “unavailability” of Sales Manager, the “vulnerability” is, “Absence of sufficient backup personnel” and “Absence of cross-functional training”. In the case of the “Source code repository server” the vulnerability is “Improper backup procedure” and “poor access control” that can cause the “hard disk crash” and the “absence of restoration documents” that can cause “corruption of data” when the server is being restored.

To make identification of vulnerabilities easier, you can divide vulnerabilities into 4 categories.

1. Technical vulnerabilities
2. Procedural vulnerabilities
3. Human vulnerabilities
4. Physical vulnerabilities

An example of the 4 types of vulnerabilities is provided here. The asset is a “mail server”. The threats are “unavailability”, “ corruption” and “underperformance”. The vulnerabilities are divided into 4 categories.

- Hard Disk Failure, which is a technical vulnerability
- Accidental deletion by administrator, which is Human vulnerability
- Improper maintenance, which is a procedural vulnerability
- Absence of fire extinguisher, which is a physical vulnerability

There are no hard and fast rules regarding classification of vulnerabilities and you can create classification categories that suit your purpose.

Next, we capture the vulnerabilities in the risk analysis spreadsheet.

In case you would like to give more information regarding the threats and vulnerabilities, use the “comment” column.

The next step is determining the impact.

Let us remind ourselves as to where we are. We are now at “Step 5 – Identify the impact”

In this example from real life, we have seen that the impact is “financial loss”, “mental strain” and “loss of time”.

And, in this example, where we have considered an information asset, we have already seen that the impact is “data loss”, “financial loss”, “mental strain” and “loss of time”.

So, let us define impact. Impact is the severity of the damage caused when the threat exploits the vulnerability

Let us define an impact measurement scale as follows.

- 0 means, insignificant or no Impact
- 1 means minor impact or temporary shut-down of asset or “little extra effort” is required to restore the asset
- 2 means major impact, extended shut-down of asset or considerable effort and resources (time, money, people) is required to restore the asset
- 3 means severe impact, almost complete shutdown of asset or significant effort and resources (time, money, people) required to restore the asset

Next, you will determine the impact using your judgment. This is a pretty straightforward process because by now you have sufficient data. You have the value of the asset, the list of threats and the list of vulnerabilities. So you will now determine the impact using 3 simple steps.

Step 1 – Consider the value of the asset

Step 2 - Consider the severity of the “threat” and “vulnerability”

Step 3 – Use your judgment to rate the impact

Using this criterion we capture the impact in the spreadsheet.

The next step is determining the “probability of occurrence”.

Let us remind ourselves as to where we are. We are in “Step 6 - Identify the probability of occurrence”

Probability of occurrence is defined as “the number of times an **event** can occur in a fixed time interval”. In this case, event is the “threat” exploiting the “vulnerability”

We have a probability measurement scale where by,

- A probability of 0 means, the event is unlikely to occur

- A probability of 1 means, the event will occur 1 time in 2-3 years
- A probability of 2 means, the event will occur once in 1 year
- A probability of 3 means, the event will occur more than once in 1 year

Please note that the probability scale can be customized as per specific requirements of the organization

Capturing the probability of occurrence is a straightforward process. You will ask the question, “How frequently will the “threat” exploit the “vulnerability”? For example, “How frequently can the mail server hard disk crash due to poor maintenance?”

We capture the “probability of occurrence” in the spreadsheet.

Finally we come to risk calculation.

As part of constantly reminding ourselves about where we are, we are finally in “Step 7 - Calculate the risk”

We define risk as 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

In the real life example, that we have seen, we calculate risk by multiplying the values of the “asset”, “impact” and “probability of occurrence”.

In the example pertaining to information, we use exactly the same formula.

Finally we capture the risk in the spreadsheet. Please note that the “risk” column is automated and once the value of the “asset”, “impact” and “probability of occurrence” is fed into the spreadsheet, the risk will be calculated automatically.

I must also add here that there are numerous definitions of risk. To learn more, go to Google and search for “define: risk”.

For the our purpose, the current definition will suffice because,

1. We are considering the value of the asset
2. We are considering the threats and vulnerabilities and the subsequent impact
3. We are considering the probability of occurrence

4. The final risk analysis formula uses the data from points 1, 2 and 3 above

You can devise your own risk analysis formula. But, you must ensure that it satisfies a few basic logical requirements.

Let us pit our current formula against the basic requirements. Our formula is ***Risk = Asset Value * Probability of occurrence* Impact***

The basic logical requirements are,

- 1) If the value of the asset increases, the risk must increase consequently
- 2) If the probability of occurrence increases, the risk must increase consequently
- 3) If the impact of the threat exploiting the vulnerability increases, the risk must increase consequently

You will see that the risk analysis formula satisfies these logical requirements. So, check your formula with the above criterion before usage Thank you and I hope you have understood this chapter on risk assessment well. There are more resources in the e-learning portal and please make sure that you go through them.