

Audio transcripts and lesson notes

Hi and welcome back. This is your instructor Anup Narayanan and let us now move on to the DO phase, which focuses on implementing the “Risk Treatment Plan”.

Well, it is my duty to remind you where we are in the whole ISMS P-D-C-A cycle. We are in the DO phase.

And, we shall be covering the entire steps of the DO Phase in this video itself. I have consciously done this because based on my experience these 7 steps are linked together with a common logic and it makes sense to cover it in a single go.

Let us start with the risk treatment approach.

The approach is as follows. We now have a list of macro level risks, which we obtained from the “Gap analysis” phase and “Micro level risks” that we obtained from the Risk Analysis step in PLAN phase. These risks must be treated using controls. For ease of understanding, I have divided controls into “Essential controls”, “Common Controls” and “Function Specific Controls”. Each control shall have an owner. Under the owner there shall be an action plan consisting of a task force, resources to implement the controls and measurement metrics to measure the effectiveness of controls. Further, each control shall have time based milestones attached to it.

Let us now start implementing the risk treatment plan.

We will start with the macro level and micro level risks.

The first step is to prioritize the risks. The prioritization is done based on the value of the risks and we shall treat the highest valued risks first.

As you can see from this risk analysis report,

The top 5 risks are,

1. Underperformance of Mail Server due to technical malfunction
2. Underperformance of Bandwidth technical malfunction
3. Unavailability of bandwidth due to absence of backup
4. Unavailability of IT Administrator due to absence from work
5. Unavailability of CIO due to absence from work

Next, we select the controls for treating the risks.

As I have mentioned earlier, controls can be classified into 3 for ease of learning. They are,

1. Essential Controls
2. Common Controls
3. Function Specific Controls

Let us look at “Essential Controls” first.

The term “Essential” is used based on experience and industry best practices. It is not a requirement specified by ISO 27001. But, you can expect these controls to be “asked-for” and “audited” during an ISO 27001 certification audit

You can use the following criterion for selecting essential controls.

- Controls that help in satisfying the “Essential Clauses” of ISO 27001 i.e. Section 4, 5, 6, 7 and 8
- Controls that satisfy legal and privacy requirements
- Controls that satisfy Business Continuity Management
- Controls that satisfy Incident Management

Let us look at the controls that can satisfy Section 4, 5, 6, 7 and 8 of ISO 27001

- Information security policy document (A. 5.1.1)
- Review of Information Security Policy Document (A.5.1.2)
- Management commitment to information Security (A.6.1.1)
- Allocation of information security responsibilities (A. 6.1.3)
- Information security awareness, education and training (A.8.2.2)

Controls that satisfy legal and privacy requirements

- Intellectual property rights (A.15.1.2)
- Protection of organizational records (A..15.1.3)
- Data Protection and privacy of personal information(A.15.1.4)

Let us look at the controls that satisfy Business Continuity Management

- Including Information Security in Business Continuity Management Process (A.14.1.1)
- Business Continuity and Risk Assessment (A.14.1.2)

Let us look at the controls that satisfy Incident Management

- Reporting Information Security Events (A.13.1.1)
- Reporting security weaknesses (A.13.1.2)
- Responsibilities and procedures (A.13.2.1)

Next, we shall look at common controls

Common controls are, those controls that are uniformly implemented in all business functions of the organization

Examples of common controls are,

- Access Control Policy (A.11.1.1) - Is a common control that is applicable to all business functions
- Information Backup (A.10.5.1) - Is a common control applicable to all business functions as they all store, process and output information
- Protection against malicious code (A.10.4.1) - Is a common control applicable to all departments that use computing equipment that has to be protected through suitable anti-viruses etc.

Next, let us take a look at function-specific controls

Function specific controls are those controls that are implemented in a specific business function or a group of business functions, but not uniformly across the organization

Examples of function specific controls are,

- Outsourced Software Development (A.12.5.5) - Is a function-specific control applicable only to a specific department (function) that has outsourced the software development
- Electronic Commerce (A.10.9.1) - Is a function-specific control applicable to those departments that deal with electronic financial transaction

The next step is assignment of ownership of controls

Let us now understand how to identify owners for each control

Let us define the word "owner" first. An owner is a "role" that is responsible for ensuring that the controls are properly implemented, monitored and reviewed to treat the appropriate risk

Let us look at an example of "owner". Owner is a "role" undertaken by an individual. "HR manager" is responsible for ensuring privacy of employee records. In this case any individual who occupies the role of the HR Manager is responsible for ensuring privacy of employee records

Please note that it is not necessary that the “Owner” has to treat the risk. The owner delegates this task to a suitable individual or team

So, what are the responsibilities of the owner. The owner has to ,

- Ensure that the appropriate control is implemented to treat the risk
- The owner shall formulate an action plan to,
 - Allocate the risk treatment to an appropriate individual or team
 - Define milestones and dates of review
 - Ensure that necessary resources are provided

Let us take a look at how ownership is assigned.

The ISMF (Information Security Management Forum) is responsible for identifying an owner. The owner is responsible for treating the risks using controls. The owner can assign the controls to a Task Force that executes the controls.

So, Which are the roles that are generally assigned the role of “Owners”?

Let us take a look at some Industry best practices

- Essential Controls are usually owned by the CISO or members of the ISMF
- Common Controls are assigned ownership depending on the nature of the control
- Function-Specific Controls are assigned to the owner of the specific Business-Function

Let us look at some practical examples. Essential Controls such as Information Security Policy Document is assigned to CISO and the ISMF. Common controls such as physical access controls to the office are assigned to facilities and physical security manager. A function specific control such as background verification of employees is assigned to HR Manager.

Let us next take a look at the action plan

So, we are the last stage i.e. the action plan

Action Plan consists of 4 components

1. The Task force: An Individual or Team that will implement the controls
2. Resources: Authorization, Money, Tools, Systems, Equipments etc.
3. Measurement & Metrics: Criterion for measuring the effectiveness of implementation
4. Time & Milestones: Periodicity of review and goals to be attained

Let us look at the functions of the “Task Force”

- The Task Force will work as per the owners’ instructions

- They will report to the owner

Example of Owners & Task Force are,

- The HR Manager (Owner) instructs the Task force (HR Executives) to ensure security of employee records
- The Task Force implements the following controls
 - Store all employee records in a locked cabinet
 - The keys to the cabinet will be with a designated HR executive

Now we move onto resources for executing the action plan

Now, what are the resources for the task force? Resources are generally Money, People, Equipment and tools .

Some examples of resources for the task force are,

- For implementing controls against malicious code, the task force requires
 - A suitable anti-virus
 - Authorization to access systems and implement the anti-virus
 - A test system to test the installation before deploying on all systems

Let us move on to measurement metrics

Next, we will take a look at measurement metrics. Measurement criterion & metrics are defined to check the effectiveness of implementation of the risk treatment plan.

Let us look at Linking Measurement Criterion & Metrics .Measurement criterion specifies the controls that must be measured and the frequency. Metrics specify quantitative measure of the performance of the control.

An example is,

Measurement criterion specifies to measure the effectiveness of “malicious code” controls every quarter

The metrics for satisfying the measurement criterion are,

- Total No: of systems in the organization
- No: of systems that have Anti-Virus installed
- Frequency of anti-virus signature updating

An in actual practice it looks like this. Take a look at the columns on the right side with the readings for the 1st month, 4th month and 7th month.

Also, keep in mind that, metrics are a “thinking” tool or thinking “aid”.

- For example, from the previous slide, an intelligent manager can infer
 - Installation of anti-virus is not catching-up with the speed at which systems are deployed (*or*) *it can be interpreted as*
 - Systems are being deployed before anti-viruses are installed

So, what is the benefit of measurement? The benefits are,

- Helps keep track of the effectiveness of controls
- Make corrective decisions
- Ensure that resources are not being wasted
- Review and improve the controls

Let us now move onto “time & milestones”

It is important to fix target dates to implement the controls and time-intervals to review the controls .

The importances of Time & Milestones are,

- Fixing milestones and time-period of review is very important for the success of the ISMS
- Only when controls are reviewed periodically, improvements are made
- Also, when controls are reviewed frequently, the task force are on their toes

In actual practice it looks like this. See the target date set for completion of the control as well as the frequency of review.

Please note that a detailed action plan template is given along with this chapter. Please ensure that you read and go through it and preferably use it for your implementation purposes

Thank you and we shall interact soon in the next chapter.