

Audio transcripts and lesson notes

Welcome back. I am your instructor Anup Narayanan and let us start with the ACT phase.

To recall – We are now in the ACT phase..

And within the ACT phase, we shall be completing all the 4 steps.

The aim of the act phase is,

- Check the whole ISMS
- Review the inputs from the “CHECK” phase
- Determine the corrective actions to be taken
- Assign the actions to the Owners and subsequently the Taskforce

There are two main activities in the ACT phase. They are,

1. Check the whole ISMS
2. Review the inputs (audit reports) from the CHECK phase and take appropriate actions

Let us start with “Task 1 – Check the whole ISMS”

This consists of, a set of activities

1. These activities are,
 - I. Review the scope
 - II. Review the Information Security Policies
 - III. Review the asset list
 - IV. Review the Risk Assessment
 - V. Review the Risk Treatment Plan
 - VI. Review the audit procedures
 - VII. *Review other relevant factors*

Activity 1 is, “review the scope”. The steps in this activity are,

- Check whether the scope needs to be modified
- Add more locations, departments or assets
- Get the new scope approved by the ISMF

Activity 2 consists of reviewing the information security policies. Information Security Policies are normally reviewed at least once a year. Check whether the policies must be updated to reflect ...

- New security threats
- New business functions/ processes
- New geographical locations

Activity 3, consists of reviewing the asset list. The steps are,

- Add/ Remove new assets if relevant. New assets could be,
 - I. New roles (people)
 - II. Computers, laptops etc.
 - III. Paper documents
- Re-rate the value of the assets based on current business value
- Identify the new asset owners

Activity 4 consists of reviewing the risk assessment. The steps are,

- Re-do the risk assessment on the latest assets
- The risks change over a period of time because
 - I. New risks emerge
 - II. Previous risks may increase
 - III. Previous risks may decrease

Activity 5 consists of reviewing the risk treatment plan. The steps are,

- Check the effectiveness of current controls
- Add or remove controls as required
- Review the “Degree of Assurance” and “Residual Risk”
- Check the performance of the “Owners” & “Task force”

Activity 6 is reviewing the audit procedures. The steps are,

- Check the audit plan
- Review the performance of the audit team
- Add new audit tasks based on the inputs from the Risk Treatment Plan

Activity 7 deals with other relevant tasks. These are based on business requirements. Examples are,

- Consider a new strategy for treating risk
- Consider a new risk treatment approach

Now let us move on to task 2 – “Act on the inputs from the “CHECK” phase”

The input for the “ACT” phase comes from the CHECK phase. The CHECK phase produces the audit reports. In the ACT phase, we shall

1. Review the audit reports
2. Decide on actions for correction
3. Assign action plan to owners

As a first step we shall prioritize what we must correct from the audit reports. You can see how this is highlighted on the screen.

In the next step, we assign the corrective actions with a target date for completion to various owners. As you can see in the sheet above, the corrective actions have been assigned to the IT Managers. You may want to press the pause button here and read the contents of this screen.

As we have seen in the DO phase, the owner can assign the corrective tasks to the “task force”. Please refer “Chapter 5, the DO Phase”.

The next step is set the dates for review. Once the corrective tasks are assigned, then the dates for review are set.

- The corrective actions are reviewed as per the fixed target dates
- This becomes a continuous process whereby the “CHECK and ACT” phase becomes mutually complementary

Thank you and we shall interact again in the next chapters.