

Audio transcripts and lesson notes

Hi and welcome back. This is Anup Narayanan, your instructor and in this chapter we are going to go through the importance and creation of an Information Security Management Forum. You can call it a forum or a committee, but we will use the name information security management forum or ISMF for short in this course. It is important to create the information security management forum before you actually start the ISMS implementation because the forum has to approve and review the various activities of the ISMS throughout the lifecycle of the ISMS.

The information security management forum is a high level management team that looks after the implementation, maintenance and improvement of the ISMS

Let us look at the structure of the ISMF

The ISMF consists of a chairman, an information security officer or a chief information security officer and then representatives from various business functions. Please note that this diagram is only a basic representation and you may create a more elaborate forum based on your business requirements. But, please remember that the forum must have a chairman, an information security officer elected by the forum, adequate representation of business functions and a representative from the audit team. Please note that I have highlighted the audit team as reporting directly to the chairman of the forum without linking to any other business function or the information security officer. This is because auditing must be an independent function and I shall explain this shortly.

Let us look at each component of the ISMF structure.

1. The chairman of the ISMF is usually a Top Management executive like the CEO
2. The (C)ISO is usually someone who understands information security risks well or could even be a person with similar risk management experience
3. The business functions will have a representative each. It is also possible that different business functions may be grouped under one representative
4. The auditing team will be independent and will report directly to the Chairman of the ISMF

The independence of the audit team is very important. This is because most of the ISMF team will be responsible for implementing the ISMS. As per industry standards, the “implementer” should not be the “auditor” to ensure absence of prejudice and for truth and honesty in reporting the status of the ISMS. This gives confidence to interested parties such as customer. For an ISMS to be effective, the review must be fair and state the actual facts. Else the ISMS will stagnate and fall into disrepair, hampering the very purpose of the ISMS.

Let us take a look at the various tasks performed by the ISMF

The ISMF must meet at pre-defined intervals. Ideally, once every 3 months or once every 6 months.

Some of the typical activities undertaken by the ISMF members during an ISMF meeting are,

1. Reviewing the current status of the ISMS, information security risks etc.
2. Approving new ISMS policies, initiatives, activities
3. Reviewing audit reports
4. Recommending corrective actions for information security violations
5. Considering new information security threats & more....

The task of the ISMF chairman normally are,

1. Chair the ISMF meetings and reviews
2. Final authority for approving or not approving decisions
3. Take balanced decisions about Information Security
4. Bring a sense of "Business" to Information Security

The last point, i.e., bringing a business sense to information security is very important. Since I have already mentioned that it is normally a top management executive who takes the role of the chairman, they will be able to balance information security challenges from a business perspective. For example, the chairman will be able to appreciate an ISMS as a confidence building measure for customers. Similarly if a new ISMS initiative costs a lot of money, the chairman may be able to bring a budgetary or financial perspective to it and decide to approve it or not approve it.

The (C)ISO's role is extremely important in the ISMS. This includes,

1. Undertaking the responsibility of implementing the ISMS in the organization
2. Initiating new ISMS activities
3. Collecting feedback from the different department representatives as well as customers and regulatory bodies
4. Informing the Chairman about the status of the ISMS

In fact it is the (C)ISO that leads the ISMS forward by constantly appraising the ISMF about the information security initiatives, their current status etc.

The (C)ISO adds tremendous value to the ISMF by communicating effectively about various aspects of information security management. This includes,

1. Informing the ISMF about what the rest of the industry is doing in the domain of information security
2. What are the new information security challenges?
3. What could be the future information security challenges?
4. Sharing experiences and learning
5. Presenting new ISMS strategies & more....

The business Function representative's role and responsibilities include,

1. Ownership of ISMS implementation in their respective business function
2. Providing feedback to the (C)ISO
3. Providing information about new business requirements that may need information security support

Finally the audit team representative's role and responsibilities include,

1. Submitting the audit reports to the Chairman of the ISMF
2. Providing a balanced view of the quality of the ISMS implementation
3. Maintaining the independence at all times

As I have mentioned before, the independence of the audit team is very important for the functioning of the ISMS.

Thank you and please don't forget to go through the resources in the iSQ World ISO 27001 e-learning portal.