Internal auditors for an ISMS tend to be very precise because of their strong commitment to ensuring conformity to ISMS standards. It is of course essential for us to ensure conformity to the standards through internal auditing, but in order to identify any unrecognized risks, we must take one extra step forward, shifting the focus of the internal audit from “conformity” to “effectiveness.”

Threats to information assets can be recognized in the management of the assets (throughout their lifecycles), in the environment (facilities) where the assets are kept, and also in relation to compliance with information assets-related laws, regulations and agreements. We must carry out risk assessments and internal audits in consideration of all these factors.

It will help us to further maintain and develop our business if we are able to ensure through internal auditing that the purpose of introducing an ISMS is being achieved continuously so the system remains effective.

Here, to be effective means that planned activities have been conducted and expected results have been achieved. Appropriate planning and reasonable implementation will lead to achieving effective results. That is “integration of the ISMS and core business operations”.

To explore this issue, we will launch a series of the articles under the general title, “Shift of Focus from ‘Conformity’ to ‘Effectiveness’ in ISMS Auditing.” This first article will discuss the basic problems related to the ISMS Internal Audit.

1. Problems Related to the ISMS Internal Audit
   – What caused the internal auditors to become so fussy?

1.1. Standards vs. Facts
For ISMS internal auditing, auditors check whether the organizations being audited are conducting their daily operations in conformity with information security-related standards and in-house rules in an effective manner.

However, auditors often cannot decide whether their findings imply conformity or nonconformity to the standards, because they:
- Overlook the facts at hand
- Do not know how to identify the facts
- Cannot decide whether the findings are important or not
- Do not know which of the audit criteria should be applied to specific findings
- Do not understand the purpose of the audit criteria
- Inflexibly apply audit criteria to all items
- Interpret audit criteria as they wish, often incorrectly

Such auditors may not identify any risks, and even if some risks are identified, if they have no knowledge of the business operations of the organizations being audited and do not know the significance of their findings, they might hesitate to point them out to the organizations for correction.

It is true that the purpose of the auditing is to decide based on the findings whether the audited organizations meet the audit criteria; however, if the auditors cannot identify the facts or cannot correctly understand the purpose of the audit criteria, they will be unable to point out the issues that need to be corrected in a manner effective enough to attain the true goal of the auditing.
1.2. Understanding the Essentials
An auditor might decide that the audited organization does not meet the criteria based on their findings, and he/she demands that the organization take corrective action by saying, “This fact implies nonconformity to this criterion. Please make corrections.”

In this case, however, the audited organization tends to resolve the problem without really recognizing what the essential cause(s) were. As a result, similar issues arise again, and again and the auditor is forced to repeatedly point out the same issues to the organization.

For example, an organization not keeping some necessary records might be due to a lack of recording procedures, a failure in clarifying roles, or the lack of education necessary to make employees aware of the importance of keeping records.

Both the auditor and the audited organization should recognize the primary causes of the problem so that necessary corrections will be made.

As implementation of the ISMS is encouraged and relevant rules are applied towards the more appropriate management of information assets, the number of visible or easily detected problems identified in audits will gradually decrease as more audits are performed and necessary counter measures are implemented by the audited organizations. This results in auditors becoming too fussy and reporting on any issues they can identify.

What are essential causes of the following findings:
- Some records were not signed by the manager.
- Due to revision of the rules, some inconsistent terminologies were found in some sections of other related rules.
- Follow-up has not been completed for employees who have yet to receive required education and training.
- Some documents were left on the printer and fax machine.
- Some information assets that should have been disposed of, remained.
- Documents were piled up on the desk of an employee who was absent.
- Among the items to be input for management review, one had been left unreported for over one year.

Auditors cannot help but become over precise if they only focus on “conformity” in the audit. Does a decrease in the number of issues pointed out in the audit really imply that the information security level of the audited organization has improved?

1.3. Questions Raised by the Management Team
For information security, the return on investment is not easy to calculate, as much cost is necessary for personnel expenses for the development of internal auditors, implementation of risk assessments and internal audits and management reviews.

It is therefore natural for a management team to have questions concerning information security in their company, including questions on the effectiveness of information security management. Specifically, the following questions may be raised.

- If no problems are pointed out in the internal audit, does it mean that our information security system is perfect?
- Have the auditors improved their abilities by carrying out yearly audits?
- The management review process reported that no incidents or accidents took place at our company, but there might be some accidents that were not reported, either intentionally or unintentionally.
- Cost of information security is are indeed expensive. Is our ISMS really effective?

The cost effectiveness of information security is not easily demonstrated.
1.4. Shift of Focus from “Conformity” to “Effectiveness”

Assuming that the acceptable risk level is fixed, the number of noncompliance issues identified in the internal audit will decrease over time and conformity-related risks will no longer exceed the acceptable level. The internal auditors, however, will become more precise. On the other hand, if anti-risk measures are left as they are without being updated in response to changes in the environment, risks will increase and approach the limits of what is acceptable, making it impossible to ensure appropriateness of the management. To ensure that risk-measures lead to an acceptable level of risk, one needs to shift focus from “conformity” to “effectiveness.” The following figure illustrates the shift of focus from “conformity” to “effectiveness.”

With ineffective internal auditing, invisible risks will be overlooked and no measures will be taken until such risks cause actual incidents.

1.5. Importance of the Findings

Auditors may not understand the business operations of the departments they audit. It is indeed desirable for each auditor to examine the business operations of the audited department and make an auditing plan by focusing on the department’s key operations and the security of related information assets.

In reality, however, auditors tend to perform audits in haste in their bid to avoid interfering with business operations so the audits tend to be superficial, without details being fully examined.

The audited departments, however, deepen their understanding of internal audits as a result of repeated executions of the PDCA cycle* for the ISMS, and will no longer be satisfied with superficial audits or superficial identification of problems. If there is no clear understanding of why issues are being pointed out, to what extent corrections are needed, or whether it is necessary to consider cost effectiveness, departments may feel that auditors are just disturbing their business operations with ineffective and inappropriate auditing.

*PDCA cycle is a management cycle in which the process of planning (Plan), doing (Do), checking (Check) and acting (Act) is implemented in an ordered sequence.

In pointing out any problems, auditors therefore need to clearly show the potential risks associated with the business operations of the audited departments and explain what incidents might take place if problems are left unresolved. If this process is appropriately conducted, the audited departments will believe that the auditors have effectively identified issues to the extent anti-risk measures are now feasible.

In-house rules should of course be obeyed, and even minor violations should not be ignored. Auditors must therefore point out all issues needing improvement even if they do not pose great risks rather than leaving them unresolved.

Auditors who do not understand the actual business operations of the audited organizations tend to make decisions on the findings by lumping them all together as equally important; however, if auditors understand the features of the organizations they audit, they can discern differences in the importance of the findings.

In the next article, we will discuss the theme: “We Cannot Deal with Invisible Issues: Visualization of Information Security Risks.”