<A series of articles about ISMS>
Shift of Focus from “Conformity” to “Effectiveness” in ISMS Auditing

2. We Cannot Respond to Invisible Issues – Visualization of Information Security Risks

2.1. Identification of Information Security Risks

For visible risks, we can plan and implement appropriate measures in consideration of their specific features, but for invisible risks, the features of which we do not know, simply implementing measures that are suitable for visible risks might not be appropriate.

In risk assessment, a range of information asset-related risks are analyzed. How should internal auditors make judgments about the materiality, threats and vulnerabilities of the analyzed risks and the appropriateness of the measures taken against those risks?

The answer to this question is shown in the following, which employs drawings of a new product as an example of an information asset.

-Materiality

If the new product is an important product on which the future of the company might depend, the level of materiality of the drawings will be judged to be very high.

-Threats and vulnerability

For drawings in electronic format, the data may be leaked or falsified, while paper drawings may be stolen, lost or damaged. These incidents must be avoided.

-Measures taken against risks

As preventive measures to be taken against these risks, access right control and regular data backup might be carried out in the case of electronic data, while paper drawings can be kept in a lockable fireproof book storage room.

However, these represent general measures to be taken against visible risks. Such measures would not be applicable to possible invisible risks.

For example, the drawings may be associated with the following invisible risks:

-Integrity

Not all changes made to the drawings may be correctly communicated to the related departments or subcontractors.

-Confidentiality

Are the drawings shared with the companies engaged in the manufacture of parts for the new product, and stored and treated in a manner that ensures confidentiality? Do the companies to which the subcontractors entrust a portion of the work also keep the drawings confidential?

Are confidentiality clauses included in the relevant contracts and memorandums, and is compliance with the provisions checked on a regular basis?

-Lifecycle

Is the lifecycle of each drawing clearly defined from creation through to disposal, and is each recorded properly? In particular, are the drawings presented to the subcontractors returned or appropriately disposed of upon completion of the contracted work?

-Transportation

In transporting the drawings, including transmission by email, are measures against risks such as erroneous transmissions and loss of data examined and implemented?

In order to identify these risks, it appears necessary to go beyond simply analyzing the confidentially, integrity and availability of the information assets themselves. The targets of risk analysis include not only information assets but also the following: physical facilities that may impact the security of information assets; lifecycle of the information assets; and compliance with laws, regulations, and provisions set forth in the related agreements.

2.2.Visualization of Invisible Risks

Visualization of all issues related to your organization helps to identify risks and to implement appropriate measures against them.
After visualizing all the issues, you may find that there are a great number of items that you were unaware of or that you misunderstood about your organization and its features.

Then, what issues need to be visualized?
-Actual status and features of the organization
-Environment surrounding the organization
-Potential risks (threats)
-Vulnerabilities
-Anti-risk measures

Internal auditors must visualize the features of the departments they will audit so that they can understand them, which will allow them to identify important points to be focused on in the auditing process. To carry out internal audits effectively within a limited timeframe, auditors must keep focused on the truly important points.

Then, how should the issues be visualized? They can be visualized in various forms as follows:
-Job charts created for the establishment and maintenance of the ISMS
-Workflow diagrams created to identify informa -tion assets
-Information concerning the results of interviews with the ISMS promotion departments and the organizations to be audited
-Reports about surveys of internal materials

There are also various other visualization methods. As an example of a visualization tool, modeling by mind mapping is introduced as follows.

Figure 2-1 Example of mind mapping used as a visualization method (reference): modeling to understand the condition of the organization to be audited
Provided by Takuro Haneda, Information Security Consulting Group, Consulting Promotion Office, Solution Marketing Division, Ricoh Japan Corporation

Mind mapping, which was invented by Tony Buzan, is based on chained descriptions of keywords. The human brain can store a massive amount of memories, and these memories can be recalled with the use of keywords. Without itemization or the use of documents, it is possible to recalled a vast amount of memories based on these keywords. If an analyzer visualizes the process of his/her thinking using a chained description of keywords, all those concerned are able to share and review the process together.
ThinkBuzan of the United Kingdom possesses all rights related to mind mapping.

Internal auditors can understand how visible risks are associated with invisible risks by visualizing the organizations that they are auditing, thus becoming aware of risks that were previously unknown.

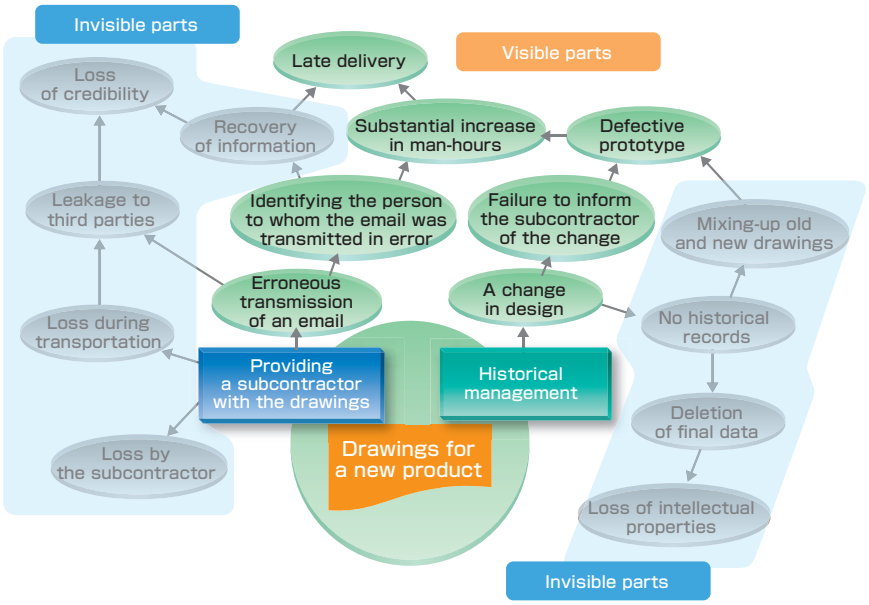

Figure 2-2 Visualization of risks related to drawings of a new product

Internal auditors and departments to be audited are both required to share the same information. If the quality of the information possessed by both parties differs, the quality of the organization's ISMS will be badly affected. Both parties can further improve the management system by sharing the organizational profile and by recognizing risks.

2.3.Structure of Risk Analysis Targets

Risk assessments are generally carried out primarily targeting information assets.
Under the ISMS, however, it is also necessary to assess risks regarding specific business requirements as well as those that concern legal and regulatory requirements.
Threats to information assets are related to their life-cycle management and environment (facilities), as well as to compliance with related laws, regulations and agreements. Risk assessments must therefore be conducted targeting all these elements.

For the protection of information assets, it is necessary to understand the structure of the risk analysis targets as shown below.
-Information
-Information storage media
-Information storage facilities
-Environment for the facilities (rooms, build -ings, premises)
-IT devices and software used for the manipu -lation of electronic information
-Services for IT devices, such as power supply and communication services
-People who manage the above

Risk analysis targets are classified into the following:
(1) Information
(2) Physical assets
(3) Service assets
(4) Software assets
(5) Intangible assets
(6) Human resources

In risk assessment, it is necessary to check whether these information assets are within the application range of the organization's ISMS, create a ledger of all relevant information assets, identify the threats to and vulnerability of the assets, and examine countermeasures to be taken.

Internal auditors are required to check whether risk analysis targets are identified and assessed appropriately within the organization.

In the next article, we will cover the following topic: "Auditing for the Maintenance and Development of Business: Actual Audits on Effectiveness"