Ensuring Information Security in Sumitomo Chemical Group

Sumitomo Chemical Systems Service Co., Ltd.
Solution Department
Tatsuhiro SUZUKI

Sumitomo Chemical Group treats ensuring information security as one of its business issues, and has promoted information security management in the whole group. When managing information security in the group, points to ponder and approaches to take are different from when managing it in a single company. This article will discuss the approaches, issues, solutions for the issues and future efforts regarding ensuring security management in Sumitomo Chemical Group, by using some case examples in Sumitomo Chemical Group.

This paper is translated from R&D Report, "SUMITOMO KAGAKU", vol. 2009-Ⅱ.

Introduction

Sumitomo Chemical Group, in its efforts to grow as a global chemical company, is rapidly establishing an IT infrastructure to support global consolidated management and develop an environment in which group companies, including those overseas, can conduct business using the same network.

However, some group companies, including those overseas, have not yet implemented adequate information security measures. Therefore, in order to achieve global consolidated management, information security must be further strengthened.

Additionally, the social demands for information security are increasing. Examples of such social demands can be seen in the trend of companies' more serious considerations on compliance management, CSR (Corporate Social Responsibility) management and tightened internal control pressed by the Corporation Law and Financial Instruments and Exchange Act.

Under these circumstances, the information security management for the entire in the Sumitomo Chemical Group is proceeding, as ensuring information security is considered as one of the company's important management issues.

This article, by using internal case examples, will discuss the methods, issues, solutions and future initiatives regarding the assurance of information security in the Sumitomo Chemical Group.

Ensuring Information Security

1. Definition of Information Security

"Information" is the most important business resource after people, materials and money, and it may even affect the company's competitive power, so it is essential to use information effectively in company activities. However, as the more important the information is, the higher the risks will be, it is very necessary to safely protect the information from hazards and damage. Managing information in a safe condition is referred to as "information security."

The "ISO/IEC 27001:2005 Information-security Management System–Requirements" international information security standard [1] (hereinafter referred to as ISO/IEC 27001:2005) defines information security as "to maintain the confidentiality, integrity and availability of the information." **Table 1** shows the defini-

Table 1 Definition of 3 concepts of information security based on ISO/IEC 27001:2005

3 concepts of information security	Definition
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Integrity	The property of safeguarding the accuracy and completeness of assets.
Availability	The property of being accessible and usable demand by an authorized entity.

tions of "confidentiality," "integrity" and "availability" based on ISO/IEC 27001:2005 [1].

Confidentiality, integrity and availability are considered as three key concepts of information security and it is important to perform them in a good balance.

2. Basic Concepts of Information Security

Information, as described above, is an important factor which can affect a company's competitive power. Therefore, it is necessary to implement information security measures steadily and preferentially. However, it is important to carefully select suitable measures by taking cost-effectiveness into account and evaluating risks strictly from the management perspective, rather than implementing every single measure without considering the company's management environment.

In addition, as security risks change on a daily basis along with the progress of IT and changes in the forms of business, it is necessary to review information security measures according to the changes in risks in order to maintain information security in the best condition.

The implementation of information security is ultimately decided by company executives, by taking into account the cost-effectiveness and investment of management resources. Therefore, system departments and people in charge of IT at each company are required to present company executives with information on risk-analysis results and the effects of measures against the risks in a timely and easy-to-understand way, so that the executives are able to accurately evaluate the risks and make proper decisions.

3. Management Method for Ensuring Information Security (Information Security Management)

The framework of ISMS: Information-security Management System*1 stipulated by the international standard ISO/IEC 2700:2005 [1] is a de-facto standard management method for ensuring information security.

And, the measures stipulated by the "ISO/IEC 27002:2006 Rules for Implementation of Information-security Management" [2] (hereinafter referred to as ISO/IEC 27002:2006) are widely used as specific control measures for ensuring information security.

In ISO/IEC 27002:2006 [2] control measures for ensuring information security are classified into eleven categories, as shown in **Table 2**.

Table 2 Category of controls to ensure information security (ISO/IEC 27002:2006)

Category of controls to ensure information security
1. Security Policy
2. Organization of information security
3. Asset Management
4. Human Resource Security
5. Physical and environmental security
6. Communications and operations management
7. Access Control
8. Information systems acquisition, development and maintenance
9. Information security incident management
10. Business continuity management
11. Compliance

Each company ensures information security by creating and implementing the most suitable control measures based on risk-analysis results, using these categories as reference.

Figure 1 depicts the relationship of the above de-facto standards and information security management in a company. As shown in **Figure 1**, ensuring information security can be achieved by establishing and operating a management system that is consistent with the business strategy following these information security de-facto standards.

In addition, ISO/IEC 27001:2005 [1] has adopted the "Plan–Do–Check–Act (PDCA)" model, so that information security management should be continuously improved in organizations is required.

4. Information Security Management for a Group

Because the framework for information security management defined in ISO/IEC 27001:2005 [1] does not specify the scale or business form of an organization, it can be applied not only to a single company but also to the entire group. However, even while belonging to the same group, each company has its own unique situation in terms of business form and scale, IT usage status and presence of dedicated IT staff. Consequently, it is unpractical to apply the same measures to all companies in the group, and it is neces-

*1 A management system is referred to as a framework by which to manage and continuously improve the organization's policy, methods and processes regarding information security.

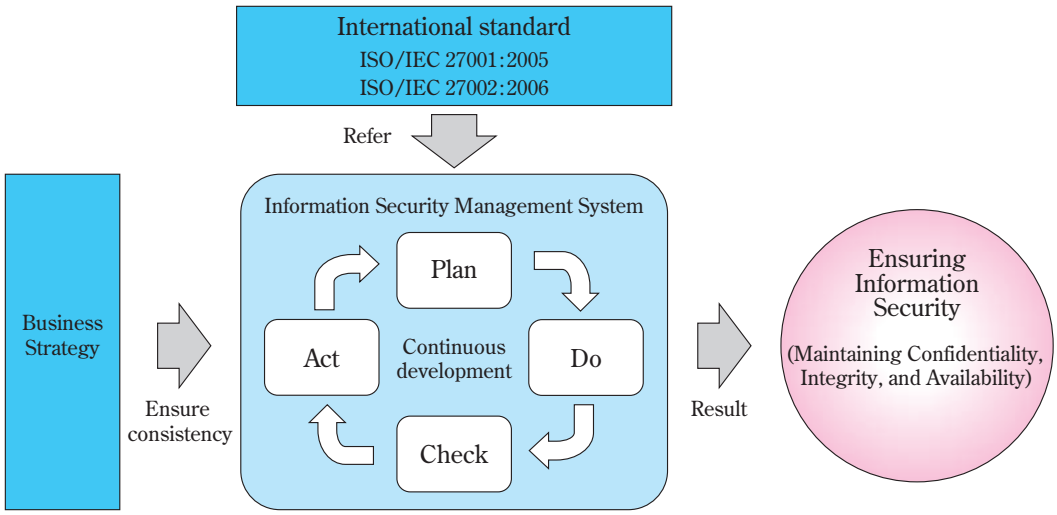


Fig. 1 Image of actions in companies for ensuring information security

sary for each company to find its own approach to information security management.

Several approaches for implementing group-wide information security management are introduced in the "Information Security Governance Implementation Guidance"[3] released by the Japanese Ministry of Economy, Trade and Industry in June 2009. An outline of them will be introduced below:

(1) Baseline Approach

In the "baseline approach," a common baseline for information security management (purposes, goals, control measures) is established, and all group companies are required to clear this baseline. In the baseline approach, it is important to set an appropriate and effective baseline that meets the group's basic policy.

(2) Group Company Mapping

The "group company mapping" refers to the approach that group companies are classified into several type by their industry type, scale and budget, and information security requirements are determined and applied to each company according to its type.

When using the group company mapping approach, it is essential to determine what factors should be used as criteria for classifying group companies.

(3) Sharing/Integration of IT Infrastructure and Organization

The term "Sharing/Integration of IT Infrastructure and Organization" refers to the approach for sharing and integrating the IT infrastructure and organization among the group companies from the perspectives of risk management and cost reduction.

Besides these, it is also effective to share the contents of user education.

Initiatives for Information Security Management in Sumitomo Chemical Group

Sumitomo Chemical Co., Ltd. (hereinafter referred to as Sumitomo Chemical) established its own security regulations in 2000, and it has been engaged in the assurance of information security. Moreover, since 2006 it has been continuously improving and operating the group's information security management system based on the policy of ensuring information security for the entire Sumitomo Chemical Group.

In addition to the framework stipulated by ISO/IEC 27001:2005[1], approaches for group security management, such as baseline approach and group company mapping, have been adopted as the most optimal approaches for establishing information security management system for the entire Sumitomo Chemical Group.

In the following, after explaining Sumitomo Chemical Group's basic concepts on information security management, initiatives will be introduced by going with the flow of the PDCA model.

1. Concept of Information-Security Management

As shown in **Figure 2**, Sumitomo Chemical Group is proceeding with a group-wide information security management system by using a hierarchical structure, in which management systems for each company are included.

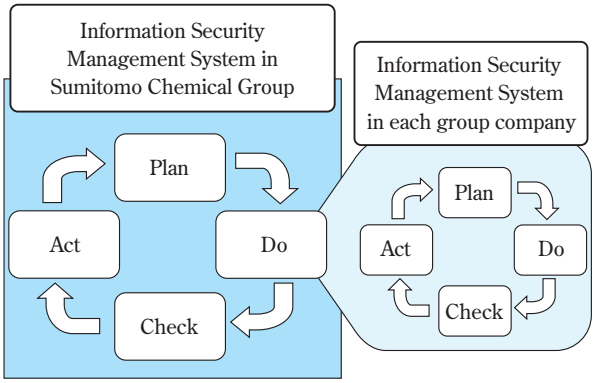


Fig. 2 Information security management structure in Sumitomo Chemical Group

Both the group-wide management system and each company's management system adopt the PDCA model, and the management system of each company is positioned in the "Do" phase of the group-wide management system.

2. (Plan) Establishing Information-Security Management

In the "Plan" phase, the basic policy is defined and the promotion structure is established. In detail, the activities will be conducted by taking the following three points into account:

- Defining a group-wide basic policy
- Classifying group companies and setting baselines by type
- Establishing communication routes and promotion structure

Following the above three points, the case example of Sumitomo Chemical Group will be introduced below.

(1) Defining Group-Wide Basic Policy

Upon establishing group-wide information security management, a basic policy of the group should be determined which defines what kind of attitude that the group should have for ensuring information security.

Sumitomo Chemical Group defines a basic policy that the entire group should strive to ensure security management, and each group company should be responsible for its own information security and implement security measures to address risks that it is faced with.*2

Sumitomo Chemical's information security related document structure is defined as shown in **Figure 3**. Group companies are also required to establish information security management by creating security regulations as part of the company rules.

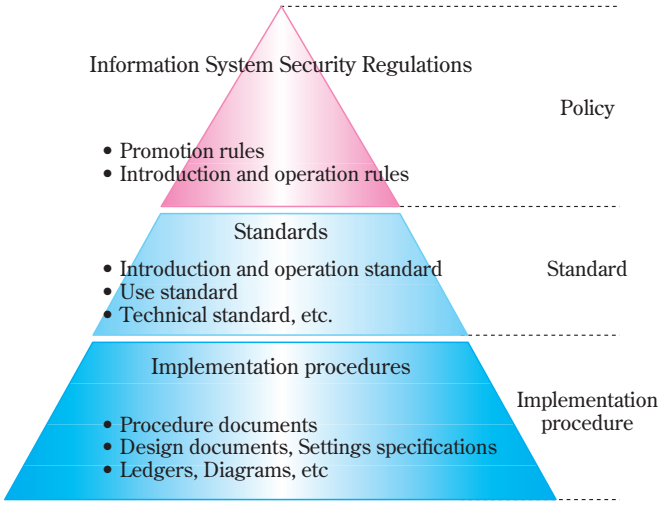


Fig. 3 Documents structure concerning information security in Sumitomo Chemical

(2) Classifying Group Companies and Setting Baselines by Type

The cost-effective information security measures should be conducted according to the risks each company is facing. Therefore, when implementing group-wide information security management, it is more effective to classify group companies into several types by business form and company scale, and then set the baseline for each type, instead of uniformly implementing the same measures for all group companies. The details of baseline setting by type are introduced in the Information Security Governance Implementation Guidance[3] of the Japanese Ministry of Economy, Trade and Industry. This security management approach can be seen as a combination of baseline approach and group company mapping.

In the Sumitomo Chemical Group, group companies are classified into three types based on sales, business

*2 In the Sumitomo Chemical Group, the activities designed to ensure information security have been undertaken with particular emphasis on digitized information and information systems. Therefore, in the Group the term "information system security" is used instead of the term "information security." However, in this article the term "information security" is used.

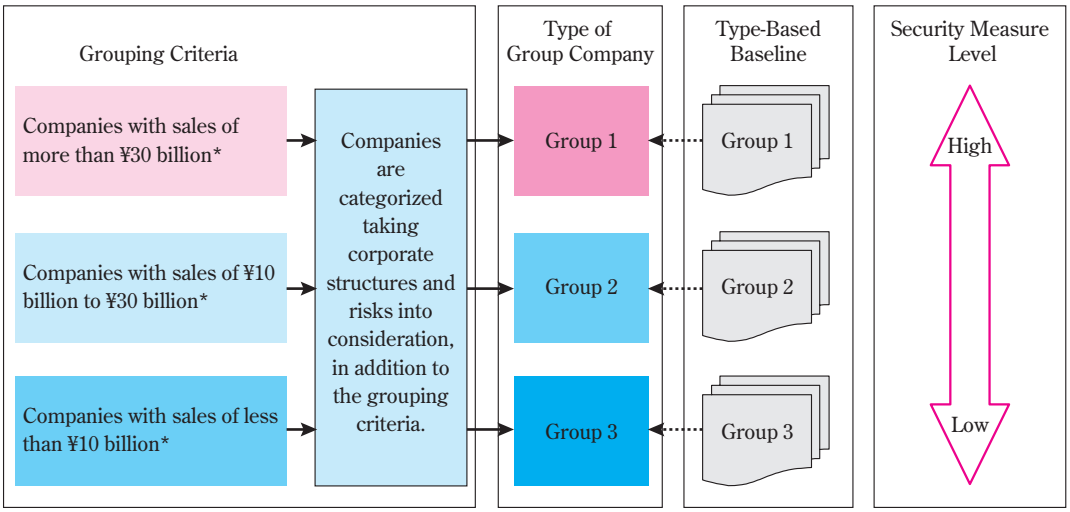
form and risk. In addition, by determining the baselines for the three types based on the security regulations and standards of Sumitomo Chemical, and presenting the baseline to each company as a template, each company can proceed with its own information security management smoothly. **Figure 4** shows the classifications and type-based baseline setting for group companies.

(3) Establishing Communication Routes and Promotion Structure

When establishing a group-wide information security management system, it is necessary to communicate sufficiently with group companies and have them well informed of group baselines and basic policy. In order to achieve this, it is effective to raise the awareness of the entire group on information security by holding meetings regularly to share information and exchange opinions. It is also important to establish a structure for promoting group-wide and single-company-wide information security management.

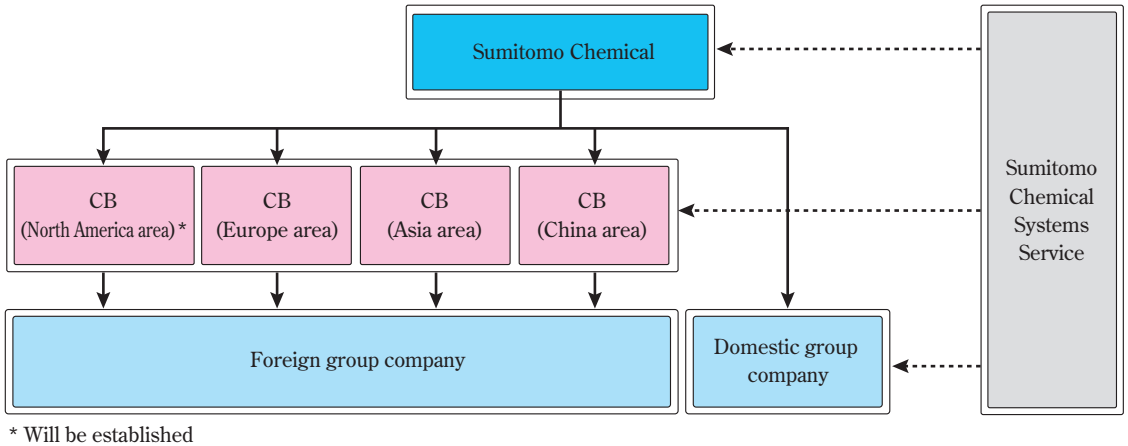
In the Sumitomo Chemical Group in 2006, Sumitomo Chemical Co., Ltd. and Sumitomo Chemical System Services Co., Ltd. (hereinafter referred to as "our company") jointly attempted to thoroughly disseminate information security management by explaining the group basic policy and type-based baseline to all domestic and overseas group companies. Meetings have also been holding periodically for information and opinion exchange among the group companies.

Furthermore, as part of the information security management promotion structure, IT support bases (Corporate Branch: CB) have been established in China and other countries in Asia and Europe in order



* calculated before consolidated accounting

Fig. 4 Category of group companies and type-based baseline setting



* Will be established

Fig. 5 Information security management promotion structure in Sumitomo Chemical Group

to provide support to neighboring group companies. In the future, IT support bases will be expanded to North America as well.

Figure 5 shows the information security management promotion structure in the Sumitomo Chemical Group.

2. (Do) Introduction/Operation of Information-Security Management

As previously introduced, the activities taken by each company are the main part of the "Do" phase. Thus the introduction and operation of group-wide information security management are conducted by taking the following two points into account:

- Supporting group companies for introducing information security management
- Understanding the Group's progress status

Following the above points, the case examples of Sumitomo Chemical Group will be introduced below:

(1) Supporting Group Companies for Introducing Information Security Management

Group companies range in scale from small to large, and there are many companies without dedicated IT staff. Because specialized knowledge is required for introducing information security management, it is necessary to provide support to these companies for introducing security management, such as establishing security regulations and analyzing risks.

Our company, as the only information system company in the Sumitomo Chemical Group, provides support to group companies for introducing information security management as a service, with the aim of helping each company to smoothly conduct their information security management activities. These services include support for establishing security regulations, support for risk analysis and measure discussion, and support for security education.

(2) Understanding the Group's Progress Status

To ensure group-wide information security management, it is necessary to be aware of the implementation status in each group company, and to take appropriate measures if any problems happen.

As a means to promote introductions of information security management in each group company in the Sumitomo Chemical Group, the status of the security regulation establishment in each group company is observed, and its progress is checked at the periodic meetings.

3. (Check) Monitoring/Reviewing Information Security Management

The "Check" phase is the one in which we check if the information security management is effectively functioning and if information security is being ensured. The appropriateness of the baseline set during the "Plan" phase is also checked.

As a method of checking these points, it is effective to monitor information security by using a group internal audit system. The "Information Security Audit Standards"[4] released by the Ministry of Economy, Trade and Industry in April 2005 and various guidelines attached to those standards are widely used as de-facto standards for information security audit methodology.

Information security audits have been implemented in the Sumitomo Chemical Group since 2008 as part of the internal audits conducted by Sumitomo Chemical Co., Ltd. Within the group internal audit activity, each group company, whether domestic or overseas, is cyclically audited every three years. Internal security audits are used not only for the purpose of inspection but also as an opportunity to provide advice and education, which can facilitate the effective operation of group-wide information security management.

Additionally, the audit procedures for the Sumitomo Chemical Group have been established based on the Information Security Audit Standards[4] of the Ministry of Economy, Trade and Industry and various guidelines attached to those standards.

4. (Act) Maintaining/Improving Information Security Management

The "Act" phase is the one in which group-wide information security management is continuously developed by improving the baselines and operation method if necessary based on the facts discovered through security audits.

In the Sumitomo Chemical Group, the issues discovered during security audits are shared among the parties involved and the group-wide information security management procedures and type-based baselines are reviewed if necessary.

Detailed case examples of the issues and measures will be explained in the next chapter.

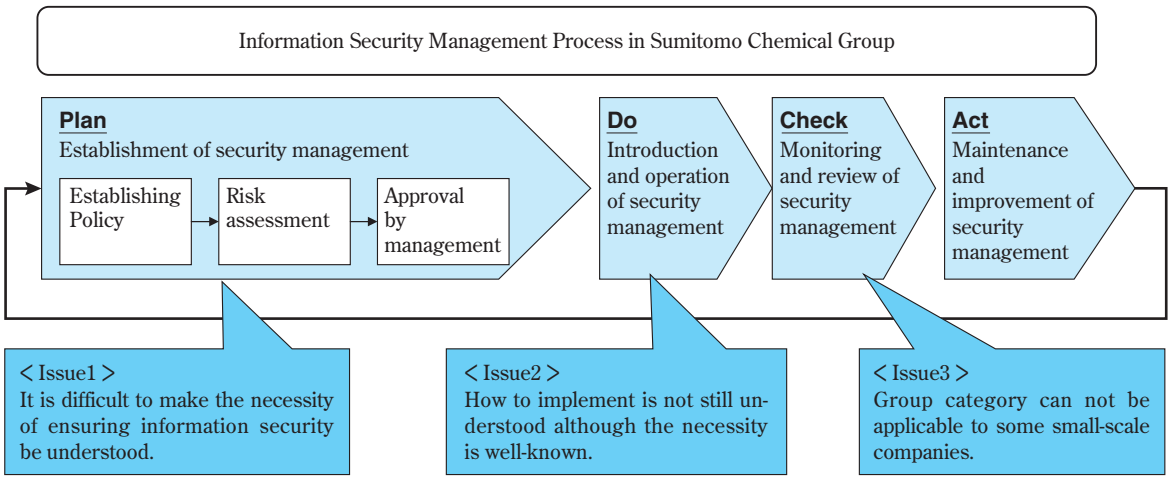


Fig. 6 Issues of information security management in Sumitomo Chemical Group

Issues and Measures in Information Security Management of Sumitomo Chemical Group

Information security management in the Sumitomo Chemical Group handles various issues and makes appropriate improvements. **Figure 6** shows the issues during establishment and operation of information security management in the Sumitomo Chemical Group.

The three typical issues listed in **Figure 6** and the measures taken for dealing with these issues will be explained below.

1. <Issue 1> It is difficult to convey the importance of ensuring information security.

Each company in the Sumitomo Chemical Group should assume responsibility for its own information security and implement security measures in accordance with the risks it is facing. However, in 2006, when the Group's basic policy was presented, the security regulations establishment at each company in the group did not initially go smoothly.

The reason for this was because the need for ensuring information security had not been adequately understood by group companies. Therefore, data on information security such as trends in security incidents and damage was shared at the periodic meetings. As a result, group companies' awareness has been raised, and this has accelerated the establishment of security regulations in each group company.

In order to enable each company to be well informed of the necessity for assurance of information security, it is important to repeatedly introduce cases on familiar topics and to emphasize the fact that every company has similar issues to be understood.

2. <Issue 2> Method of implementation is not still understood, although the need is well known.

Many group companies are small-scale and without dedicated IT staff. When there is no dedicated IT staff, although the need to ensure information security ("why") can be understood, what kind of measures should be taken ("what") and how to do them ("how") have not been identified, which hinders the implementation of information security management in group companies.

Consequently, to deal with this issue, our company has reviewed the information security management introduction services provided as a support for group companies, to enable the people in charge of IT to understand the significance of the security measures. As shown in more detail in **Figure 7**, in addition to the security measures, the significance of the security measures and the key points in implementation are also explained which improves the awareness of the people in charge of IT. Understanding the significance of the security measures enables the people in charge of IT to check the appropriateness of outsourced work.

The people in charge of IT play an important role in promoting information security management in group companies and should be responsible for accurately providing information to management, to help them make appropriate decisions about the pros and cons of security measure implementation. Thus the success or failure of information security management in the group can be greatly affected by the degree of

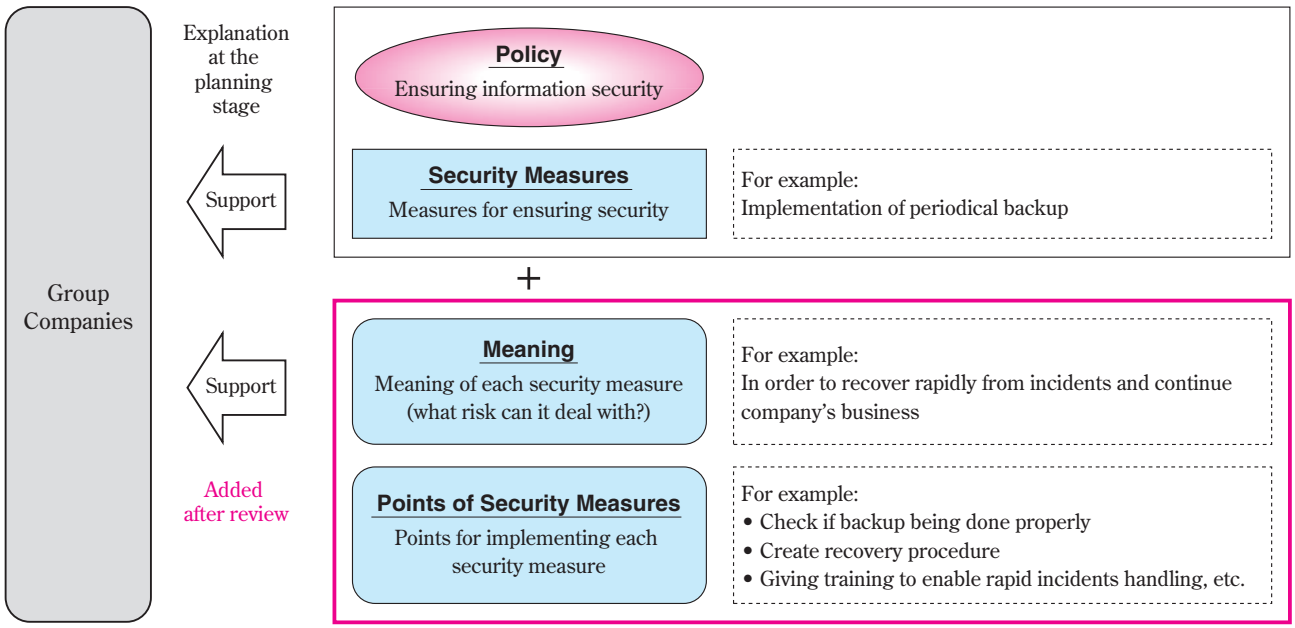


Fig. 7 Review of support for group companies to implement security measures

understanding of the people in charge of IT in each company. Accordingly, raising the awareness of the people in charge of IT is an important issue.

3. <Issue 3> Group categories may not be applicable to some small-scale companies.

Group companies are classified into three types based on several factors, such as sales and business form. The baseline is then determined for each type and presented to group companies as a template. However, when templates were applied to group companies (including those overseas), some small-scale companies which have a low IT dependency or own few IT assets were found.

As a result, the type-based baselines determined during the "Plan" phase were revised, and a new baseline was created which can be applied to companies with low IT risk. Upon revising the baseline, the categories of measures stipulated by ISO/IEC 27002:2006 [2)] were strictly considered to ensure all requirements would be met.

It is essential to take cost-effective security measures in accordance with the specific risks a company is facing. Therefore, it is important to create a practical but effective baseline based on the understanding of the situations in group companies.

The issues and measures have been explained in this chapter based on three case examples. The common point in these examples is that it is essential to properly understand the facts and implement measures. Especially, when implementing group-wide information security management, it is difficult to master the facts precisely so it is necessary to keep adequate daily communication with all group companies.

Future Efforts for Security Enhancement within the Sumitomo Chemical Group

The Sumitomo Chemical Group takes security measures to prevent serious damage by establishing/operating a group-wide management system and implementing technical measures. However, to achieve further progress in global consolidated management, it is necessary to strengthen information security in each group company.

Moreover, measures for quality improvement and cost reduction, such as sharing and integration of infrastructure, should be implemented.

Some initiatives to enhance information security management for the Sumitomo Chemical Group are introduced below:

1. Further Improvement of Security Awareness

Although information security incidents are reported with great frequency, information leaks and system failures are occurring again and again in today's society. Security incidents can be linked to credit rating falls and huge damage, and once they happen, they can subject the company to serious, unrecoverable damage.

In addition to continuing the activities that have been carried out by far with regard to Sumitomo Chemical Group information security management, strengthening our actions on further raising security awareness is considered to be an important issue.

Accordingly, besides the information security audits which are conducted as part of internal audits, self-checking is also being focused on as a method for raising awareness.

Self-checking is an action where the person in charge of IT in each group company checks the progress status of the company's security measures based on the Evaluation Sheet.*3 This is considered an effective means for maintaining and improving security awareness. Additionally, self-checking can be used to check if anything is missing in the work that was determined on during the "Plan" phase, as well as to check the effectiveness of that work.

2. Sharing and Integration of IT Infrastructure

Common IT standards have been established in the Sumitomo Chemical Group in order to achieve sharing and integration of IT infrastructure. Currently, we are proceeding with the application of these standards to each group company. Several companies have already achieved sharing and integration of mission-critical system and network environments, and these group companies purchase and use these IT resources as a service, instead of owning the IT infrastructure individually.

Sumitomo Chemical is endeavoring to achieve further cost reductions and rationalizations for total optimization by expanding sharing and integration of IT infrastructure to PC management and anti-virus software operation.

3. Achieving Efficient Management by Effective Data Usage

In the Sumitomo Chemical Group, information security auditing is conducted on domestic and overseas group companies, so the details on the status of information security management implementation in each group company can be well understood. Since security audit is conducted at a three-year-one-cycle pace, the implementation status of the entire Group will be understood in detail by the time one cycle is over (in 2011 as planned).

Because more practical measures can be taken by effectively using the accumulated data, various tasks such as the aforementioned sharing and integration of IT infrastructure can be carried out in a more effective manner. For example, implementing sharing of IT infrastructure in a high security risk area can better ensure information security and prevent the occurrence of damage before it happens.

In addition to the data from audit, the results of periodic meetings and self-checking should be collected as a means of shortening the data renewal cycle. This can result in an improvement in management accuracy.

Conclusion

The initiatives for ensuring group-wide information security have been explained in this article by using case examples from the Sumitomo Chemical Group from the management perspective. It is important to note that group-wide information security management cannot be achieved in one day, and a step-by-step implementation not only allows us to ensure information security but also can help us achieve speedy management by enhanced collaboration among group companies, which will lift the activity to a higher rank.

With the increasing IT dependency of companies, security risks are becoming larger. Additionally, there is a trend toward demanding the reinforcement of information security governance in Japanese policy from the accountability perspective (e.g., disclosure of the status of information security management at a company to both internal and external stakeholders in a report).

Sumitomo Chemical Group information security management must be able to quickly and flexibly respond to changes in business environment as well as in laws and regulations. It must also be effective as the IT infrastructure which can support our global consolidated management in the future.

To achieve these goals, it is important to develop a management system aiming at total optimization, by which communication among group companies can be

*3 The Evaluation Sheet contains the end points such as, "Is the security-awareness education implemented once a year?" according to the Group's policy. The person in charge of IT at each group company enters the evaluation results on the sheet. This allows the person in charge of IT to check the security management status of his/her own company.

strengthened, activities for mutual awareness improvement can be continued, and all group companies can function with a sense of oneness.

References

1) ISO/IEC 27001:2005 Information security management systems -- Requirements
2) ISO/IEC 27002:2006 Code of practices for the management of IT security and information security
3) Ministry of Economy, Trade and Industry: June Heisei 21, Information Security Governance Implementation Guidance
4) Ministry of Economy, Trade and Industry: April Heisei 15, Information Security Audit Standards

PROFILE

Tatsuhiro SUZUKI

Sumitomo Chemical Systems Service Co., Ltd.
Solution Department