Internal audits must assess whether or not:
- rules are established,
- necessary measures are implemented, and
- regular monitoring of the situation is in place; and if there is a
- mechanism to ensure the aforementioned three conformity components are put in place.

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

3. Auditing for Maintenance and Development of Business
   – Actual Audits on Effectiveness

3.1. Three conformity components and a mechanism for ensuring conformity
Conformity with ISMS standards is the prerequisite for an effective management system. What then, constitutes a system such as this, which complies with the standards and delivers effective results?

The chart below illustrates the components and mechanism of the system:

![Figure 3-1 Three conformity components and a supporting mechanism to ensure conformity](image)

**1. Rules are established.**
If rules are established but no measures are implemented, the system is considered noncompliant with the standards.

**2. Measures are implemented.**
A situation where measures are implemented but no rules are established provides the organization with an opportunity for improvement.

**3. The performance of the system is monitored.**
Whether or not rules are established and/or measures are implemented is unknown, regardless of the actual status, unless the situation is regularly monitored and reviewed. Without regular monitoring, there are no tools to detect any discontinuation of necessary activities should such an event occur sometime in the future.

**4. A mechanism is in place to ensure conformity.**
When rules are established, measures are implemented, and the situation is regularly monitored, the system can be considered to be compliant with the standards. Such compliance can be ensured by a relevant mechanism put into place. Internal audits assess whether or not compliance is achieved and in what way, and there is a mechanism in place to ensure consistent compliance.

Internal audits must assess whether or not: rules are established, necessary measures are implemented, and regular monitoring of the situation is in place; and if there is a mechanism to ensure the aforementioned three conformity components are put in place.
3.2. Assessing effectiveness through audits

Another important role of internal audits is to assess whether or not the objectives of the management system are fulfilled on an ongoing basis—in other words, whether or not the management system is effective.

- Evaluation criteria are unclear.
  Management indicators, quantitative targets, evaluation methods, and other yardsticks of effectiveness are not specific enough.
- Delivered results are not effective.
  No or little improvement has been made or no root causes have been addressed.

The applicability of this analysis is not limited to management systems. For instance, if you cannot obtain expected results from day-to-day operations or from a project, it means that the operation or the project in question is not effective. Without taking corrective actions, you will not be able to maintain, let alone grow, your business.

3.3. Effectiveness of ISMS

Now let us take another look at the effectiveness of an ISM from the perspective of a process-based approach.

1. “Planned activities”
   “Planned activities” refers to the control measures employed based on risk assessment results being taken as specific risk treatment measures. Therefore, in the planning stage, it is expected that control measures, once implemented, will reduce target risks. In this sense, developing an appropriate plan is the key.

2. “Implemented”
   Here, “implemented” means that control measures are implemented as employed risk treatment measures. Implementation should be conducted within a planned budget and a planned schedule.

3. “Planned results are achieved.”
   The purpose of control measures is to reduce risks. Reducing risks means preventing the occurrence of incidents. Achievement is measured by using a planned evaluation method.

The effectiveness of the ISMS and control measures of an organization can be assessed when the achievement levels of ISMS objectives and goals and the number of incident occurrences fall within acceptable levels.
4. Conclusions
As they are conducted within a limited period of time, internal audits are unable to assess all information assets in all departments to verify compliance with applicable standards. Internal auditing always involves uncertainties. To assess if an organization’s management system is effective, auditors examine the conformity levels of some of the organization’s information assets and mechanisms for ensuring the conformity. If the organization’s management system (i.e., the PCDA cycle) is operated appropriately and the system delivers effective results, it can be assumed that the organization’s ISMS objectives and goals have been achieved and that an unacceptable level of incidents is not likely to occur.

Whether or not selected control measures are appropriate as outputs cannot be judged by assessing the control measures themselves. Rather, the appropriateness can be evaluated indirectly by checking corresponding inputs and process to see if:

1. As inputs, the risk assessment standards and procedures are logical and acceptable; and
2. As processes, risk assessment was performed and control measures were selected by following the standards and procedures.

The evaluation of one of the three process-based approach elements (inputs, processes, and outputs) can be conducted by review of the other two.

Audits for the maintenance and development of business are required to assess whether events that threaten business security (in the three areas of confidentiality, integrity, and availability) are appropriately controlled. This means that auditors without knowledge of what an “appropriately controlled” state is cannot assess effectiveness through an audit.

![Diagram of ISMS Assessment](image-url)