

Think Beyond “Controls”: A “process” based approach for Information Security Management using ISM3

Anup Narayanan, CISA, CISSP

Founder & Sr. Consultant, First Legion Consulting
2nd Floor, MELKA Tower, Cheruparampath Road, Kadavantra, Kochi, Kerala, India Pin
682020

Anup@anupnarayanan.org

ISM3 (Information Security Management Maturity Model) uses a process based approach for deploying or enhancing an ISMS (Information Security Management System). ISM3 defines information security as a result of a process. The better the process, the better the protection achieved from the resources available. In a "controls" oriented approach there is no expected result because the focus is on protection of an asset. Results are obtainable from a process and these results can be measured to improve the process. ISM3 focuses not on "what approach can do it" but "what approach helps me make the right decisions". Moreover ISM3 does not perceive Information Security as "avoidance of incidents" but "achieving business goals inspite of incidents".

Introduction

A “Controls-Oriented” approach is preferred by many organizations for deploying an ISMS. Controls are associated with an objective. For example, the question “What is the objective of a Firewall?” has an answer - “To protect the perimeter of the network”. The next logical question in sequence is to check whether the objective is fulfilled, - “What is the result of using a firewall?” This can be answered only by measuring the result of a process which uses the firewall. By implementing processes, information security becomes more wholesome and holistic. The focus shifts from the “control” to the whole “environment”

ISM3 uses a process oriented approach towards Information Security Management. ISM3 defines Information Security as the result of a process. The better the process, the better the security achieved using the available resources. Definition of a process includes various components such as the person entrusted with ownership of the control, the scope of protection, the updates on the control, the availability of systems protected by the control etc.

The fundamental improvement here is that the information security processes are measurable using metrics. Considering the above example of a firewall, the metrics here could be updates (the number of times the firewall rules are updated), availability (the availability of the firewall as well as systems protected by the firewall). ISM3, thus compared to other standards brings a paradigm shift in approach by focusing on the processes centered around a control and measuring the results of the process and constantly improving them.

Overview of ISM3

The features of ISM3 can be characterized by explaining the following aspects.

Metrics - ISM3 makes information security a "measurable" process by using metrics for every process. The principle followed is - "What you can't measure, you can't manage, and what you can't manage, you can't improve". This allows for a continuous improvement of the processes, as there are criterion to measure the efficiency and performance of the information security management system.

Maturity Levels - ISM3 has 5 maturity levels, each level tailored to the security objectives of the organization and available resources. This makes ISM3 adaptable to organizations with varying resources for Information Security.

Process Based - ISM3 is process based, which aligns it with ISO9001 or those that use ITIL for as the IT management model. This makes ISM3 friendly for organizations already using ISO 9001 and ITIL.

Adopts best practices - ISM3 uses extensive reference to established standards for every process, and the explicit distribution of responsibilities in the organization between leaders, managers and technical personnel using the concept of "Strategic, Tactical and Operational Management" for Information Security.

Accreditation - ISMS based in ISM3 are Accreditable under ISO9001 or ISO27001 schemes, which means that you can use ISM3 to implement an ISO 27001 based ISMS.

Business Friendly – A key advantage of using ISM3 for ISMS is that Senior Managers and Stake Holders are able to clearly see Information Security as a business investment and measure ROSI (Return on Security Investment).

Applying ISM3 for Information Security Management

ISM3 uses four models for designing an ISMS.

1. **ISM (Information Security Management) Process Model** - For identifying key ISM processes.
2. **Responsibilities Model** – For providing a responsibilities-based view of an organization.
3. **Security in Context Model** – Aligns Information Security Objectives to business objectives.
4. **Information System Model** – For identifying and describing critical Information Systems in an organization

The ISM process model

The ISM process model stresses on the value of Information Security Processes rather than controls. The principal difference between a control and process can be explained by elaborating an example of testing a control as well as a process. For example, a control “passwords should be minimum 8 characters long” can be audited by trying to create a password 6 characters long and observing whether the system accepts or rejects the password.

In a process oriented approach, this works more elaborately. For the purpose of discussion let us term the process for password management as “User Registration Process”. For testing a process a result of the process is defined beforehand, termed in ISM3 parlance as “Work Products”. In case of the “User Registration Process” the expected work products of the system could be defined as,

- Grant of Access to Authorized Users
- Denial of Access to Unauthorized users
- Logs of password changes
- Logs of Authorized access to Information Repositories
- Unauthorized Access Attempt Reports

Once the work products are defined, metrics are used to measure the process. The metrics are

- **Activity** – Description of the volume of work products produced
- **Scope** – The environment covered by the scope
- **Update** – Frequency of update of the process and the frequency of updates on the system covered by the process.
- **Availability** – The period of time the process has performed as expected upon demand and the frequency and duration of interruptions.

There are two ways in which the process could be tested, the first method is similar to testing the control (mentioned in the previous page), but this would reflect only the current state of the system A more comprehensive way to test process would be to measure the results of the process by using the metrics. Using the above example, it could proceed as shown below,

- **Activity** – The following values could be checked
 - Number of access rights granted
 - Number of access rights revoked
 - Number of user accounts expired
 - Number of user accounts “active” beyond expiry
- **Scope** – The following values could be checked
 - Percentage of “Access Control Databases” in which unused user accounts should expire
 - Percentage of “Access Control Databases” in which passwords must follow minimum guidelines.
- **Update** – The following values could be checked
 - Mean time between access rights granted
 - Mean time between access rights revoked
- **Availability** – The following values could be checked
 - Percentage of time the user registration system is available

From the above metrics, the values obtained under “Scope” and “Availability” would be used to improve security directly. The metrics “Activity” and “Update” would be used to improve security in-directly by increasing the efficiency of the processes. The benefits could be explained by the following examples.

- If 100 access rights are normally granted every month, but one month it was noticed that only 10 access rights were granted, it would call for an investigation of the process. This could indicate different scenarios, for example, people are not asking for access rights any longer and are sharing access rights.
- Or it could also indicate that the person who is in charge of the access control system is not doing his job properly and is slow.
- Or, the second condition could be leading to the first condition.

Implementing processes and measuring the performance of the process can help in improving security directly or indirectly. Metrics may impact directly on protection or they make security more manageable.

ROSI and Processes

Though ROSI (Return on Security Investment) is not easy to calculate, certain key indicators can be provided using metrics. For example,

- **Availability** – If Availability is far higher than expected then it may be a case of investing too much to ensure availability. Perhaps investments can be re-aligned for improving areas with weak security.

The Responsibilities Model

ISM3 divides Information Security Management responsibilities into Strategic Management, Tactical Management and Operational Management. Strategic Managers are involved with the long term alignment of IT with Business needs. Tactical Managers are involved in the allocation of resources and configuration and management of the ISM system. Operational Managers are involved in setting up, operating and monitoring the specific processes.

Aligning Processes (Process Model) with Responsibilities model

While an accurate mapping of processes with the Responsibilities model may not be viable, the basic principles could be aligned.

Role	Mapping with Process	Example
Strategic Manager	Review ISM status	Set expectations from ISM system. Example – Customer data should not be compromised.
Tactical Manager	Check processes using metrics	Check mean time between patch updates on database server. Example – mean time between patching of critical systems.
Operational Managers	Implement processes and feed value to metrics	Do patching of systems and update process metrics.

ISM3 enhances process management using the concept of TPSRSR, explained below.

Enhancing responsibilities model using the principles of TPSRSR

ISM3 prescribes a set of best practice guidelines to be followed for managing Information Security processes. They are briefly described as TPSRSR, which expands to Transparency, Partitioning, Supervision, Rotation and Separation of Responsibilities.

Transparency: Responsibilities should be clearly defined and reports must be made available to authorized parties. Additionally,

- **Strategic** ISM reports must be made available to stakeholders as per regulatory requirements.
- **Operational** ISM reports must be made available to tactical and strategic ISM managers.
- **Tactical** ISM reports should be available to strategic ISM managers.

Partitioning: All instances of ISM processes must have one and only one process owner. The process owner can be an individual or one group of people.

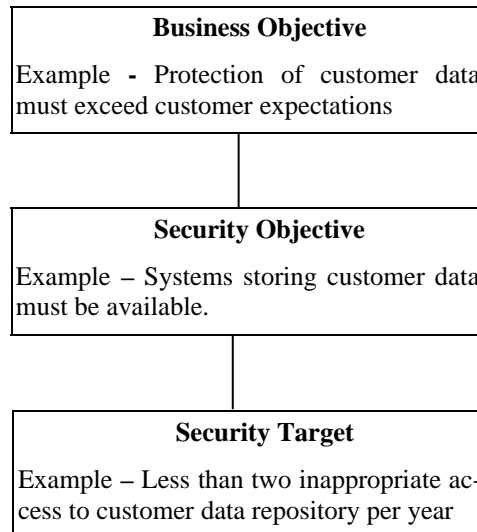
Supervision: All ISM processes must have at least one supervisor.

Rotation: All sensitive processes such as audits must be periodically transferred to another process owner.

Separation: Separation of responsibilities prevents Internal Fraud. This combines with the rule of Transparency to bring accountability for incidents and results pertaining to a process.

The Security in Context (SIC) Model

The ISM3 definition of security is context dependent. Organizations have objectives (business objectives). The Security in Context (SIC) model defines “Security as the result of continuous meeting or surpassing of a set of objectives”. This would in turn ensure the business objectives are attained. An example is provided below.



In the SIC model, security targets are defined for attaining security objectives in the context of business. This enables organizations to have targets which are attainable and affordable as per the resources they have. A small organization may have smaller security targets based on availability of less resources. An example is provided below,

Integrating Process Model with SIC Model

The link between the SIC Model and the process model is “Security Targets”. Security Target is a threshold of a metric that measures success in meeting business and security objectives. This is explained using an example below.

Security & Business Objectives	Availability of customer information must exceed customer expectation			
Security targets	Loss due to System downtime must not exceed 5 man-hours a year.			
Process Selected	“Access Control to Repositories”			
Work product (Expected Results)	Grant of Access to authorized users Denial of Access to unauthorized users Logs of access			
Process Metrics	Activity	Scope	Update	Availability
Results (Examples) 1st week	50 access attempts on average per day.	Customer Database	Time between 2 consecutive access denials is one month	Access control system is available 99.5% of time.
Variations (after 3 weeks)	Nil	Nil	Time between 2 consecutive access denials is 2 days	same
Diagnosis	Nil	Nil	Cause for concern	Nil
Business Decision	Nil	Nil	Investigation is required to check for, Unauthorized attempts Efficiency of access control administrator, Sharing of access rights by users.	

Conclusion

ISM3 focuses on business processes and considers how "bad things" that can happen to business processes. This ensures that decisions are always based on business needs. More importantly, every ISM3 process has a Rationale section, which expresses how the process contributes to the goals of the Operational, Tactical, Strategic level. This enables you to know what the goal of the business is and the contribution of the process towards the same, the expected work products from the process and hence there is far more context for an informed decision.

In a controls oriented approach there is no expected result because the focus is on the protection of an asset and not a business process. ISM3 helps by focusing not on "what approach can do it", but "what approach helps me better to make the right decisions".

Acknowledgment

My sincere thanks to Mr. Vicente Aceituno Canal, the principal author for encouraging me to review ISM3.

References

ISM3, <http://www.isecom.org/projects/ism3.shtml>
ISO 27001-2: 2002, <http://www.bsi-global.com>

Websites

www.ism3.com