

ISM3: A Standard for Information Security Management

By Vicente Aceituno

The most influential standards for information security are undoubtedly the best-practice-based standards. With these, a gap analysis is fairly easy and an action plan is simple to prepare. Also, the possibility of obtaining a corporate certification under ISO 27001 is a major attraction.

There are a great many management and information security standards in addition to the well-known ISO 27001. Each standard takes a certain viewpoint, such as processes with COBIT (Control Objectives for Information and related Technology) and ITIL (IT Infrastructure Library); best practices with ISO 17799 and ISF SoGP (Information Security Forum Standard of Good Practice); controls with ISO 13335 and SP 800-53; and sometimes risk management, as with OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation).

The most influential standards for information security are undoubtedly the best-practice-based standards. With these, a gap analysis is fairly easy and an action plan is simple to prepare. Also, the possibility of obtaining a corporate certification under ISO 27001 is a major attraction. None of the other currently popular standards offers information security certifications.

Every viewpoint has advantages and disadvantages. Best practices are widely applicable and easily understandable, but undermined without good support processes. Risk orientation is more satisfactory from a theoretical point of view, but it can be expensive and is difficult to manage at a technical level. Process orientation is easy to implement, but the results are not always guaranteed. Control orientation is easy to audit, and apparently guarantees results, but is hard to implement and can be inflexible.

The origin and properties of ISM3

The starting point of ISM3 (Information Security Management Maturity Model¹) was to take the best ideas about management systems and controls from ISO 9000, ITIL, CMMI (Capability

Maturity Model Integration) and ISO 17799 / ISO 27001. ISM3 was born with the intention of helping both large and small companies obtain the maximum return on their security investment, whatever their budget, often in relation to the use of an Information Security Management System (ISMS).

ISM3 has various intended uses:

- It is a tool for managers and auditors to evaluate and enhance the ISMS
- It provides a measurable approach to IS management
- It can be used to extend ISO 9000 disciplines into the ISMS
- It provides another route to a certificated ISMS

ISM3 is a complete standard that is business-friendly, adaptable, accreditable, compatible, scalable and open.

Business-friendly

ISM3 does not aim for invulnerability or absolute security, but instead for achievement of the organization's mission, its defined security. ISM3 aligns security management with business needs via Business Objectives, Security Objectives and Security Targets. Business Objectives are derived from the organization's mission and legal environment, while Security Objectives and Security Targets are derived from the protected assets, environments and lifecycles, and the resources available for that protection. Business Objectives are documented in the Information Security Policy, and by their nature remain basically constant as the organization evolves.

Security Targets facilitate measuring the efficacy of the ISMS. If the targets are met, the system works. If the targets are not met, it is

¹ <http://www.ism3.com/>

possible that the systems are not operating correctly, the targets are unrealistic, or there are not enough resources to meet the targets. This leads to corrective action, reassessment of the targets, or claiming more resources for achieving the targets.

Business Objectives and Security Objectives help senior managers and stakeholders to clearly see and understand the linkage between business and information security. This orientation makes ISM3 applicable to all kinds of organizations: small, big, private, administrative, charitable.

Adaptable

ISM3 has five maturity levels, each of which can be accredited as a management system. Using these levels, a company can adapt its ISMS to realistic Security Targets, using resources so as to maximize improvement. As another advantage of maturity levels, it is possible to obtain intermediate certifications when reaching milestones in the development of a higher-level ISMS. Maturity levels can simplify the design of the ISMS, since a certain level may be found suitable for the needs of the whole organization.

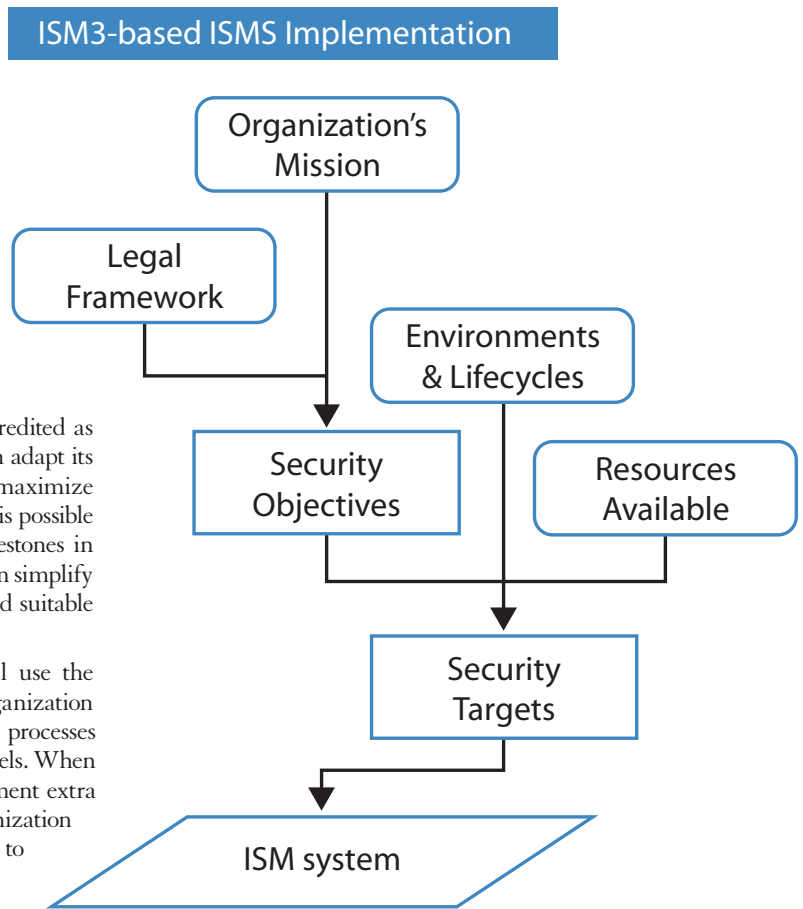
Organizations that do not desire accreditation can still use the maturity levels as a guide to ISMS design. Every organization chooses the processes best suited to protect its mission, processes that may or may not match a particular set of maturity levels. When an organization accredits a Level 2 ISMS, it may implement extra processes in line with the Business Objectives. If an organization opts not to accredit the ISM system, it does not have to meet all the documentation requirements – which helps organizations that desire only a guide to ISMS implementation.

Accreditable

An ISMS based in ISM3 is accreditable under ISO 9001 or ISO 27001 schemes, which means that you can use ISM3 to implement an ISO 27001-based ISMS. The ISM3 processes definition is derived from CMMI and ISO 9001. This means that an ISM3 system can be accredited when an auditor finds evidence of all processes belonging to a certain maturity level, in the form of documentation, supervision and sufficient resources. As a result of the compatibility between ISM3 and ISO 9001, organizations with experience in quality management probably have in-house some of the expertise and tools needed to manage an ISM3-based ISM system.

Easy to implement

There is a clear division of responsibilities between leaders, managers and technical personnel using the concepts of Strategic, Tactical 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 operational (technical) processes.

In the implementation of ISM3, it is easy to determine security responsibilities thanks to this division of the ISM3 processes into layers. This division doesn't mean that every layer must be performed by different teams. Rather, it represents a way of thinking about what results are to be achieved, and who the results will be reported to.

Compatible

ISM3 requires the existence of inputs and Work Products (which are not compulsorily documents), but it doesn't define which activities are performed in each process, or with what frequency. The best current practices in the industry should be used, and ISM3 contains extensive appropriate references. This way the current investment in security is protected, and you can evolve from what you have.

ISM3 is ISO 27001-compatible to the point that ISM3 can be used as a tool to help with implementation of ISO 27001, or even to certify an organization by both standards. ISM3 deepens the security context of ITIL-based service management systems, and offers a detailed framework for mapping ISO 17799 to COBIT.

Management Layers
<p>Strategic – Direct and Provide</p> <ul style="list-style-type: none"> • Coordinate • Security Objectives – Security Policy • Provides Resources
<p>Tactical – Implement and Optimize</p> <ul style="list-style-type: none"> • Design ISM system • Manage Resources
<p>Operational – Execute and Report</p> <ul style="list-style-type: none"> • Technical Processes

Scalable and complete

ISM3 acknowledges explicitly the existence of environments within an organization, with different roles and protection needs, such as the user environment, production environment, development environment, Internet services environment, etc. To use object-oriented terminology, processes defined by ISM3 are classes of processes, not unique objects in themselves.

This way, different process instances can be used in different environments,affordingscalability from small company to complex international conglomerate. ISM3 requires coverage of all information systems critical to the business. It is not possible to limit accreditation to a single part of the business, but it is permitted to outsource processes to a suitably assured organization. This is a key need for many organizations that can't afford in-house talent for certain security processes.

Using ISM3 fosters collaboration between information security clients and providers, as the outsourcing of security processes is enabled by explicit mechanisms for outsourcing. For example, Work Products and metrics help to define the scope of the outsourced service and the definition of the service level agreement (SLA).

ISM3 treats both technical and non-technical threats like fraud, corruption and human error by using transparency, partitioning, supervision, rotation and separation of responsibilities (TPSRSR). These concepts can be used in both ISMS management and other business processes, making ISM3 a very complete standard.

Open

ISM3 has been published under a Creative Commons license and is freely available in the electronic version at www.ism3.com. The Creative Commons license allows unlimited reproduction and use of the standard.

Process-based

ISM3 uses a process-oriented approach towards Information Security Management. ISM3 defines Information Security as the result of a

set of processes. The better the process performance, the better the security achieved using the available resources. The definition of a process includes various components, such as the person entrusted with ownership of the process, the scope of protection, the updates on the control, the availability of systems protected by the process, etc.

ISM3 process orientation aligns with ISO 9001 or those that use ITIL as the IT management model. This makes ISM3 friendly for organizations already using ISO 9001 and ITIL.

Everyone knows incidents are a fact of life. Upon an incident, it should be possible to determine whether the ISMS has been successful, what has failed, and how to improve the ISMS accordingly. Unfortunately, control-based ISMSs lack success

criteria, as controls don't have a defined tangible output. Both controls and process can be audited by testing them, but managers need a grip on their management systems when auditing is not being performed. For this reason, ISM3 doesn't use controls but processes, which have defined and tangible inputs and outputs.

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 a 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.

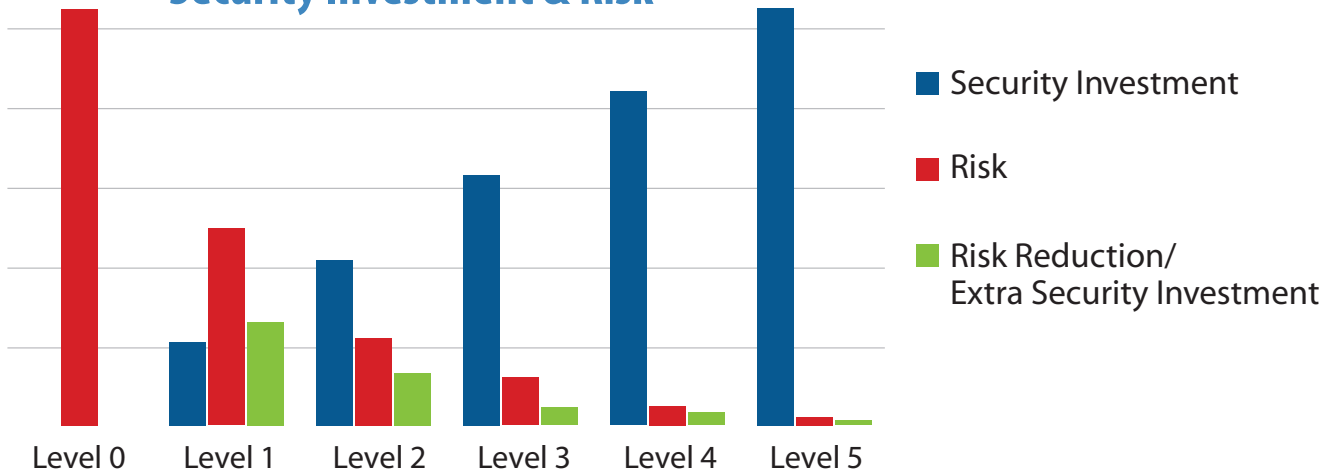
Metrics

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 criteria to measure the performance of the ISMS.

Information security processes are manageable using metrics. This lets managers show results, show how results benefit the organization, and check what changes in the process make the process improve and

Business Objectives and Security Objectives help senior managers and stakeholders to clearly see and understand the linkage between business and information security.

Security Investment & Risk



by how much. It also facilitates accountability. 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); the activity (the number of packets passed and dropped); and the coverage (what percentage of network boundaries are protected with firewalls).

Results of processes with ISM3 are defined and termed as “Work Products.” For example, in the case of the access control 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

The process could be tested in two ways. The first method is similar to testing the control, but this would reflect only the current state of the system. A more comprehensive way to test the process is to measure the results of the process by using the metrics. Using the above example, this 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 expiration
- **Scope** – The following values could be checked:
 - Percentage of “Access Control Databases” in which unused user accounts actually expire in comparison with the total of Access Control Databases
 - Percentage of “Access Control Databases” in which user accounts’ password length has a lower limit in comparison with the total of Access Control Databases
- **Update** – The following values could be checked:
 - Mean time between access rights granted
 - Mean time between access rights revoked
- **Availability** – The following value 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, and “Activity” and “Update” would be used to improve security indirectly by improving the process. The benefits could be explained by the following examples.

If 100 access rights are normally granted every month, but in one month it is noticed that only 10 access rights were granted, an investigation of the process would be called for.

This could indicate different scenarios. For example, people are not asking for access rights any longer and are sharing them. Or the findings could indicate that the person who is in charge of the access control system is not doing his job properly and is slow. Or perhaps the second condition is causing the first condition.

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

Conclusion

If you have an ISMS already, using ISM3 is compatible with your approach, and can help with enhancing current ISM systems beyond compliance with current standards to higher, and more difficult to achieve, maturity levels. If you don’t have an ISMS yet and you are familiar with process-based management approaches like ISO 9001 and ITIL; if you need a top-down approach that roots on your business mission; if you have limited resources; or if you are looking for an accreditable ISMS, then ISM3 is for you.

About the Author

Vicente Aceituno, Ingeniero Técnico en Telecomunicaciones (Universidad Politécnica de Madrid), authored the ISM3 (Information Security Management Maturity Model, www.ism3.com); leads the FIST information security conferences in Spain (www.fistconference.org); has published his first book Seguridad de la Información (ISBN: 84-933336-7-0); and maintains a Website at www.seguridaddelainformacion.com. He can be reached at vac@zenobia.es.

Standards and Best Practices Referenced

BS7799-2:2002, BS ISO/IEC 17799:2000, CMMI, COBIT, ISO13335, ITSM, ITIL, SP800-53, SP800-55, CIS, CISA, CISSP, CRAMM, DIBS, ISO9001:2000, ISO12207, ISO15408, ISO15228, ISO18044, MAGERIT, NSA, RBAC, SPSMM, SSE-CMM, SVRRP, OCTAVE, OPSA, OPST, OSSTMM, OWASP, P-CMM.