COMPARED TO ISO27001

CONTACT INFORMATION

Calle Olímpico Francisco Fernández Ochoa, 9
28923 Alcorcón (Madrid) Spain
Mail: consortium@ism3.com
Phone:+ 34 620 527 478

LEGAL DISCLAIMER

This is an informational document, and it doesn't represent legal or professional advice from the ISM3 Consortium, the authors or reviewers of this document. This document is offered as is without any warranty of completeness, accuracy or timeliness. The ISM3 Consortium, the authors and reviewers of this document disclaim any implied warranty or liability.

LICENSE AND COPYRIGHT

Consortium Members

ESTEC Security (http://www.security.estec.com/) - Canada

First Legion Consulting (http://www.firstlegion.net/) - India

Global4 (http://www.g4ii.com/) - Spain

M3 Security (http://www.m3-security.net/) - USA

Seltika (http://www.seltika.com) – Colombia

Valiant Technologies (www.valiant-technologies.com) - India

1 Comparison

Criteria	ISM3	ISO27001	Implications
Maturity Levels	Five	No	With ISO27001 whether you get certified or not. Initial investment, which brings the highest return on investment, is discouraged by this posture. If your optimum level of investment requires less far fewer controls than 27001, you can't show it because it is not accreditable. If you have limited resources, you can't show you are doing efforts in security. Only with maturity levels it is possible to show progress towards better security management. Maturity levels enable prioritizing investment, as processes are required in order of importance..
Certificate Value Protection	Certificate can choose maturity levels. Detailed processes leave little for Auditor interpretation.	Certificate can choose scope, risk assessment method, control. Compliance with the standard requires Auditor interpretation.	Freedom of interpretation on the side of the Auditor, Risk Assessment method and choice of controls and scope leads to very different implementations. As a certificate holder gets same the prestige as the worst certificate holder, mock implementations can hurt serious implementations. High protection levels are more difficult to achieve for big and complex organizations. ISM3 brings some rationality to certification, as a company with many resources and only 2 CPD could get Enterprise Level certified; while that could be out of reach for a multinational. With ISO27001 and choosing scope, they have the same chances, and the effort could be similar.
Organizational Model	Process owner Customer Roles Responsibilities TPSRSR Processes	Management / Not Management Asset owners	With ISM3 the distribution of responsibilities is granular and specific. (Customer, Process Owner, Supervisor, Owner of Assets), division of duties and reporting among Strategic, Tactical and Operational Levels, etc. With ISO27001 you detail the ownership and responsibilities of Assets.

Criteria	ISM3	ISO27001	Implications
Link between Business Goals and Information Security	Information qualities: - Business - Compliance - Technical Security Objectives - Attacks Prevention - Errors Prevention - Accidents Prevention Security Targets - Incident: Breach of a security objective.	Information qualities - Confidentiality - Availability - Integrity - Attacks Prevention - Incident: Breach of CIA.	ISO27001 example: Confidentiality: LOW Availability: HIGH Integrity: MEDIUM With ISM3, Compliance, Technical and Business Needs and Limitations become central from the start. Example: • **Business**: Invoices should be accessible to the Accountancy department and the Collection department only. • **Business**: Paid Invoices are to be kept for 3 years and destroyed after no more than four years. • **Business**: The system has to register the user account the date and time of creation. • **Business**: The system need to be available 9 to 5 Monday to Friday, with no more than 5 interruptions per week, with a duration of no more than one hour in total, and causing no more 15 Invoices to be re-entered. • **Business**: There must be less than 5 errors per hundred invoices. • **Business**: More than 99,8% of products served must be invoiced. • **Compliance**: The system is a third party application that which license must be kept current. • **Compliance**: The invoicing system keeps personal information, according to the law the database must be registered at the Data Protection agency. • **Technical**: The system must not be visible to systems from outside the company or have any remote access. • **Technical**: The system must be kept in the Data Centre under controlled environmental conditions and company safeguards against fire, flood, etc (This level of detail is enable but is not mandatory)
Goal	Achievable Security / Maximize ROSI Rationale specified per process	Absolute Security / Invulnerability Rationale not specified	As ISO27001 doesn't specify a rationale per control, it can be difficult to explain why implement some controls beyond "you need to be compliant". Aiming for absolute security is a road to managing by fear and uncertainty. Managing with defined goals makes easier to focus on improvement.
Inputs	Yes	No	Many ISM3 inputs are outputs of other ISM processes, showing dependencies.

Criteria	ISM3	ISO27001	Implications
Outputs	Yes	No	ISM3 metrics are based on the defined outputs, which makes managing the processes possible.
Metrics	Security Targets Activity Scope Unavailability Load Efficacy Efficiency Quality	No	Metrics allow finding incidents and faults in the process, enabling continuous improvement.
Accreditable	Yes, ISO27001 compatible	Yes	Certification enables trust relationships.
Distribution of responsibilities	Strategic Tactical Operational Process owner example	No	With ISM3 the distribution of responsibilities is granular and specific. (Customer, Process Owner, Supervisor, Owner of Assets), division of duties and reporting among Strategic, Tactical and Operational Levels, etc. With ISO27001 you detail the ownership and responsibilities of Assets.
References	Rich in references to best practices Too many to list!	ISO27002 ISO 13335	References make implementation easier.
Cost	The implementation cost depends on the maturity level and the scope of the ISMS.	The implementation cost depends on the scope of the ISMS.	While ISM3 Basic Level and SME Level can be cheaper that ISO27001, Enterprise and Military Levels can be more expensive than ISO27001 as requirements can be more difficult to meet.
Implementation Guidance	Details inputs, outputs, metrics and references.	Comments about implementation with varying detail.	The more implementation guidance is provided, the easier is to implement the ISMS.

Criteria	ISM3	ISO27001	Implications
Security Processes Selection	Suited to Security Objectives and Targets Types of assessment: -Threat Assessment; - Vulnerability Assessment; - Business Impact Analysis; - Risk Assessment; - ROSI Analysis.	Controls not adopted have to be justified for successful accreditation. - Risk Assessment	ISM3 gives several choices for techniques for ISM design and evolution. A full Risk assessment can be difficult and expensive for an organisation doing the first efforts in information security. ISM3 focuses on information security processes that traverse business processes, but ISO27001 can have a limited scope leavings lots of assets unprotected.
Success criteria	Yes	No	Incidents are a fact of life. You can tell if your ISMS is ISO27001 compliant after an audit, but How can you tell if your ISMS is successful?. ISM3 has security targets, when they are met the ISM is successful, otherwise it has failed and remediation action has to be taken. ISO27001 accreditation requires an ongoing incident monitoring and response process for review and improvement.
Outsourcing	Metrics can be used to create SLAs, KGIs, KPIs	No support	Companies frequently outsource security processes. With ISO27001 you can control contractors, but it doesn't explain how to outsource parts of you ISMS to a contractor, or if outsourcing some controls has any effect on accreditability of the ISMS.
Capability	Defined in terms of the Metrics used.	Undefined	Having an objective definition of capability helps continuous improvement.

Criteria	ISM3	ISO27001	Implications
Paradigm	Process based	Controls based	Process based management is easier to integrate with Cobit, ISO9001 and ITIL. Controls and processes can be audited testing them. For example a control like "No information or information systems should be removed from the premises without authorization" can be audited by trying to remove an information system from the premises without authorization. A process like "Premises access control", with Access granted and Access Denied logs can be audited the same way. Controls don't have a defined output, but processes do. This means processes can be managed using metrics of the outputs. On the other hand a malfunctioning control doesn't produce information (metrics from the output) necessary to learn what went wrong and take a management decision to fix it
Use of PDCA	Per process basis	Whole ISMS basis	PDCA used at a high level has limited utility. Example: - Plan for building a Space Shuttle. - Build it. - Check if it flies by launching it. - Fix it if it didn't launch successfully.
Improvement Cycle	Continuous using metrics	Discrete, with long Audit - Risk Assessment cycles.	ISO27001 way for continuous improvement is repeated audits, while ISM3 improvement is driven by process metrics. ISO27001 approach is discrete, ISM3 is continuous.
Approach	Top-Down	Bottom-up	With ISO27001 assets are the focus, instead of business goals.
Information System Model	Repositories Messages Channels / Networks Interfaces Services	Information Information in transit Network Terminal Information being processed	Using the information system model, policies can be written using technology independent terminology and don't need to be updated as often. For example "no confidential documents must be left at interfaces" includes fax, printer, scanner and any other foreseeable device.
Scope	It is mandatory to include the information systems that keep the organization running.	It is optional to include any set of information systems chosen by the company.	The narrower the choice, the more similar are the certificate holders. As any certificate gets the prestige of the worst of the pack, a narrow choice protects the value of the certificate.

Criteria	ISM3	ISO27001	Implications
License and Availability	Creative Commons License Attribs-Nonderivs 3.0 Available for free	Copyright by ISO Available for a fee	Making the standard widely available make it more affordable to evaluate how useful it is for the information security strategy of the company.
Issuer	ISM3 Consortium	ISO	ISO is a widely recognized standards organization, while the ISM3 Consortium is a newcomer.
Timeliness	Last update published January 2009	The 2005 version is nearly identical to the 2001 version.	Standards need to keep up to date with best practices and research, while they have to be stable enough to prevent confusion among users.
Organization Model	Business Functions Environments Assets	Assets	Modelling an Organization just as a set of assets is like modelling an organism as a set of cells.