

Conferencias **FIST** Marzo/Madrid 2006 @



ISM3 v1.1

Information Security Management Maturity Model



Vicente Aceituno Canal

Sponsored by:





Traditional approach to security:

- **“We want to prevent attacks from succeeding”**. With this approach, to be secure means to be *invulnerable*.
- An incident is any loss of confidentiality, integrity or availability.
- You look at a piece of data and think: Is it confidential, has it got integrity, is it available?

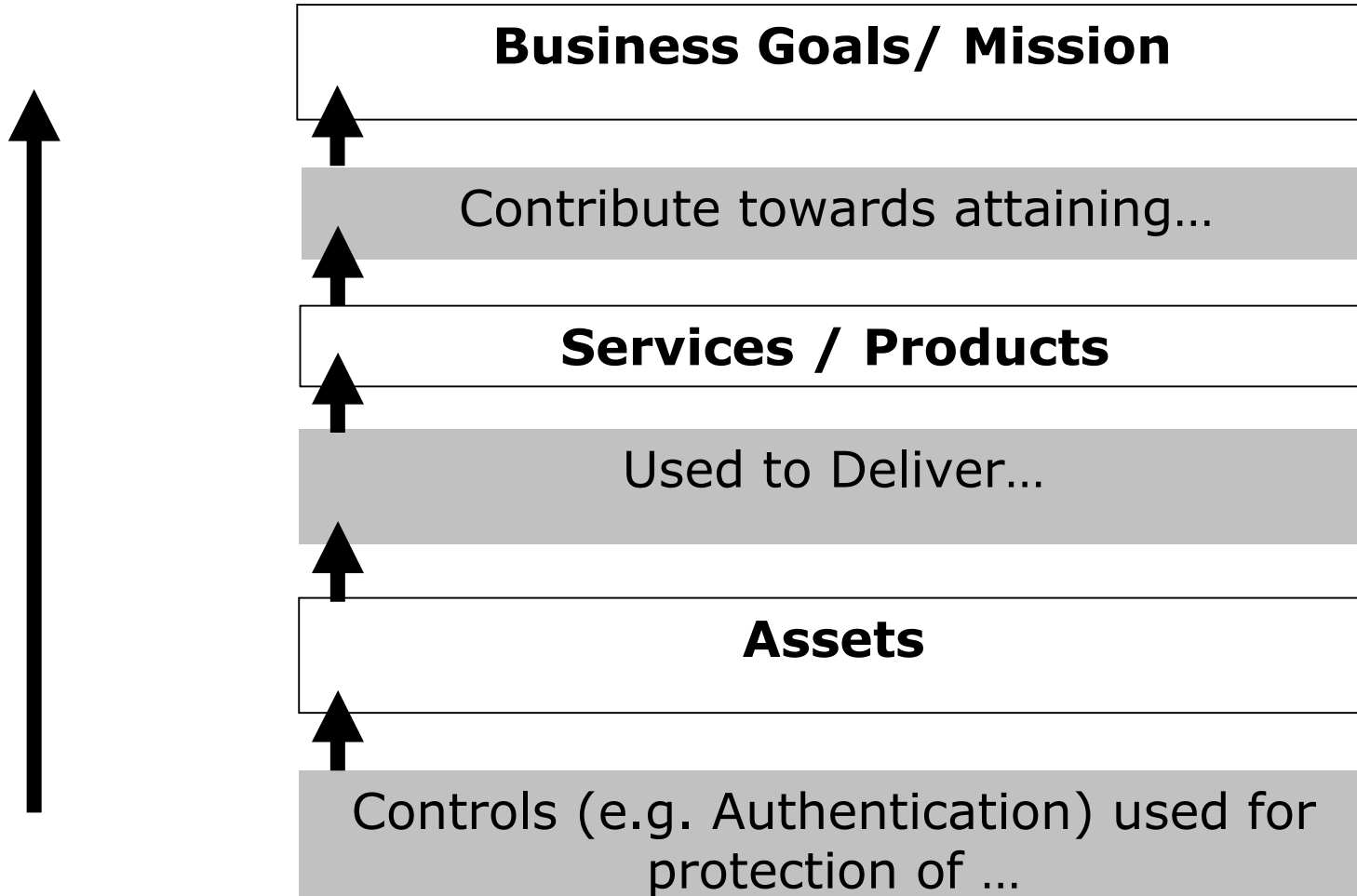


ISM3 Approach

- **“We want to guarantee that our business goals are met”**. With this approach, to be secure means to be reliable, despite attacks, accidents and errors.
- An incident is a failure to meet a security objective resulting from accidents, errors or attacks.
- Using ISM3 you look at a piece of data and think: What properties of this data must be protected for it to have business value?

Traditional Approach

MANAGEMENT FOCUS



TECHNICAL FOCUS

ISM3 Business Focus

MANAGEMENT FOCUS



TECHNICAL FOCUS



ISM3 Business Focus

- Business Objectives – Fundamental to the existence of an organization. Resilience depends on security objectives.
- Security Objectives are derived from business objectives and specify the goals of the ISM.
- Security Targets measure the achievement of security objectives in business terms.



ISM3 - What needs protection?

- Business Objectives examples:
 - Paying taxes in time;
 - Invoice all products and services provided;
 - Keep any records needed to pass successfully any audit, like a tax audit or a software licenses audit.
- Security Objectives.
- Security Targets.



ISM3 - What protection is needed?

- Business Objectives.
- Security Objectives examples:
 - “Secrets should be accessible to authorized users only”
 - “Existence of repositories and services should be assured for exactly as long as client expectations;
- Security Targets.



ISM3 - Is protection successful?

- Business Objectives.
- Security Objectives.
- Security Targets examples.
 - “Less than 2 secrets revealed every year, accounting for less than 0.1% of the value of the company”
 - “Less than 10 invoices not claimed every year because of failed security objectives, accounting for less than 0.3% of the value of the company”



ISM3 - Continuous Improvement

- What you can't measure you can't manage.
- What you can't manage you can't improve.
- ISM3 uses PDCA per process & Metrics for continuous improvement.



ISM3 - Continuous Improvement

- Security Targets.

- Process Management Metrics:
 - Activity.
 - Coverage.
 - Update.
 - Availability.



ISM3 Compatibility & Process Orientation

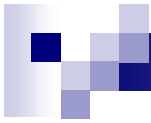
- Process Oriented.
- ISM3 is compatible with ISO27001/BS7799, Cobit, ITIL and ISO9001.
- Organizations don't have to drop their current investment in ISM systems to adapt to ISM3.
- ISM3 has references to the best practices for performing each process.



ISM3 & BS7799 / ISO27001

- ISM3 can be used for a better BS7799 Implementation or alone.
- *Example for Patching of Critical Systems*
12.5.2 Technical review of applications after operating system changes:

When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.



ISM3 Guidance on Patching of Systems

Process	OSP-5 Environment Patching
Description	This process covers the on-going update of services to prevent incidents related to known weaknesses.
Rationale	Patching prevents incidents arising from the exploitation of known weaknesses in services.
Documentation	OSP-051-Services Update Level Report Template, OSP-052-Services Patching Management Procedure
Inputs	Inventory of Assets, Alerts and Fixes Report
Work Products	<i>Up to date services in every environment, Services Update Level Report.</i>
Activity	Number of Work Products submitted, Number of patching updates in information systems
Scope	Percentage of information systems covered by the process
Update	<p>Time since last Work Products submission</p> <p>Mean time between Work Products submissions</p> <p>Update level, calculated as follows:</p> <ol style="list-style-type: none"> 1. Every information system update level is equal to the sum of the number of days old that are all the security patches pending to apply. 2. The environment update level is equal to the sum of the individual update levels, divided by the number of information systems. <p>The lower this metric, the better. This metric allows checking of the progress of the patching process, and comparison of the update level of different environments.</p>
Availability	Percentage of time the patching systems are available

ISM3 Guidance (Explained)

Process	OSP-5 Environment Patching	ID
Description	This process covers the on-going update of services to prevent incidents related to known weaknesses.	WHAT
Rationale	Patching prevents incidents arising from the exploitation of known weaknesses in services.	WHY
Documentation	OSP-051-Services Update Level Report Template, OSP-052-Services Patching Management Procedure	DOCUMENTS
Inputs	Inventory of Assets, Alerts and Fixes Report	INPUTS
Work Products	<i>Up to date services in every environment, Services Update Level Report.</i>	RESULTS
Activity	Number of Work Products submitted, Number of patching updates in information systems	METRICS
Scope	Percentage of information systems covered by the process	METRICS
Update	<p>Time since last Work Products submission</p> <p>Mean time between Work Products submissions</p> <p>Update level, calculated as follows:</p> <ol style="list-style-type: none"> 1. Every information system update level is equal to the sum of the number of days old that are all the security patches pending to apply. 2. The environment update level is equal to the sum of the individual update levels, divided by the number of information systems. <p>The lower this metric, the better. This metric allows checking of the progress of the patching process, and comparison of the update level of different environments.</p>	METRICS
Availability	Percentage of time the patching systems are available	METRICS



ISM3 Processes – Extensive! Few Examples

- GP-1 Document Management
- GP-2 ISM System Audit
- SSP-3 Strategic vision
- OSP-7 Environment Hardening
- OSP-10 Backup & Redundancy Management
- OSP-11 Access control
- OSP-12 User Registration
- OSP-16 Segmentation and Filtering Management
- OSP-17 Malware Protection Management
- OSP-23 Events Detection and Analysis



ISM3 Responsibility Guidance

- **Transparency:** Responsibilities and reporting channels should be clearly defined, documented and communicated.
- **Partitioning:** All instances of ISM processes should have one and only one Process Owner.
- **Supervision:** All ISM processes should have at least one supervisor.
- **Rotation:** All sensitive processes should be transferred periodically to another competent process owner.
- **Separation:** No process owner will own incompatible processes.

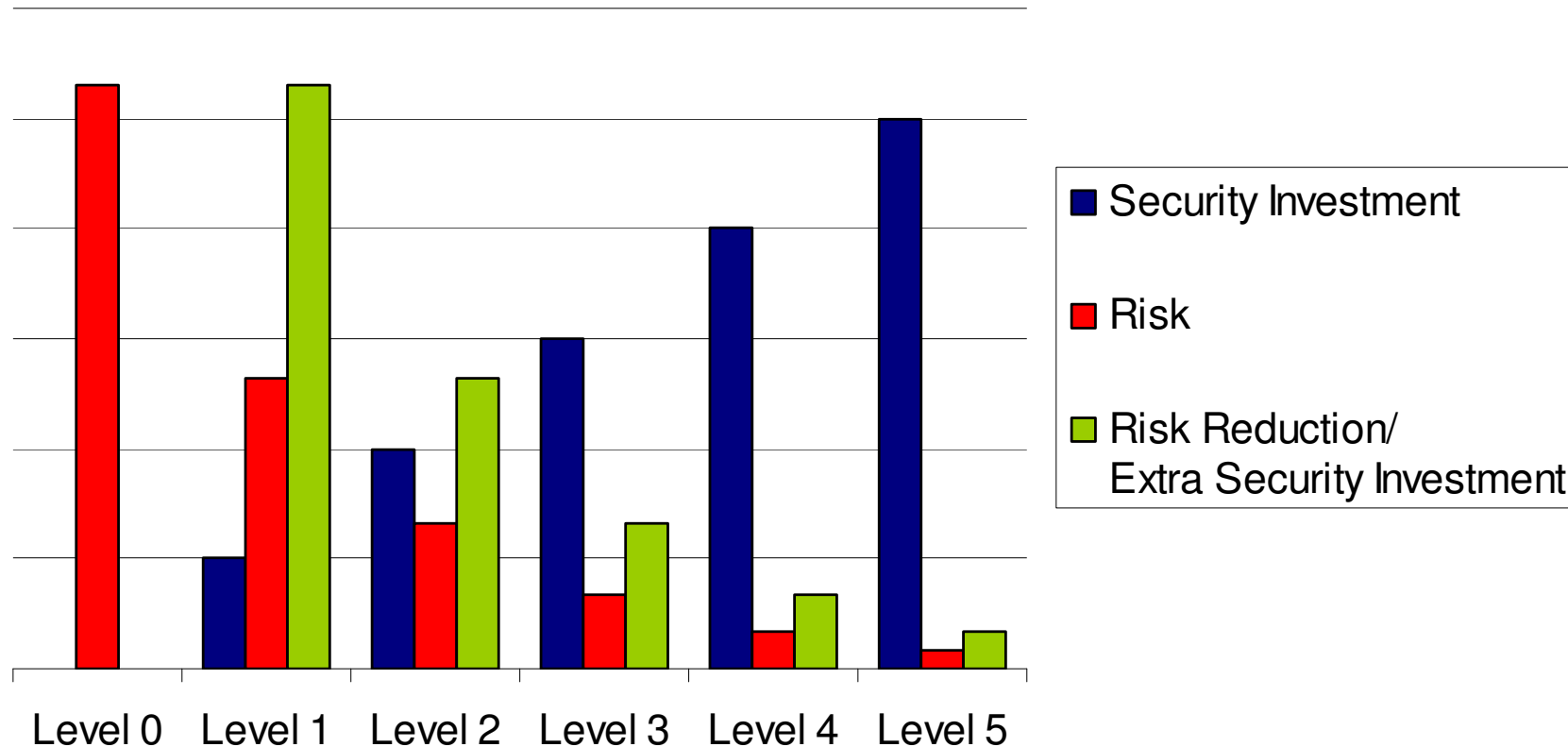


ISM3 Flexibility

- ISM3 is adaptable to organizations with different missions and contexts.
- ISM3 is adaptable to organizations with different resources.
 - Security investment is driven by business need.
 - Some organizations may not have a huge budget for Information Security (20 / 80 Rule).
 - Maturity levels describe different levels of sophistication of ISM systems.
 - Organizations can identify appropriate processes, choose a level suitable for them, and show implementation progress.

ISM3 Maturity Levels

Security Investment & Risk



(Qualitative Graphic. Risk Reduction / Extra Security Investment, scaled x40 for readability)



ISM3 Maturity Levels

- **ISM3 Level 1** - Significant risk reduction from technical threats, for a minimum investment in essential ISM processes.
 - For organizations with low Information Security Targets in low risk environments.

- **ISM3 Level 3** - Highest risk reduction from technical threats, for a significant investment in Information Security processes.
 - For organizations with high Information Security Targets in normal or high-risk environments.

- **ISM3 Level 5** - Highest risk reduction from technical and internal threats, for a high and optimized investment in Information Security processes.
 - For organizations affected by specific requirements (such as utilities, and financial institutions) with high Information Security Targets in normal or high-risk environments.



Advantages

- Maturity Levels make easier to prioritize and optimize investment in information security.
- ISO9001 compatible certifications; Some companies can't make big investments. It is well known that 20% of investment can give 80% of the results, but there is no way to show this. ISM3 levels 1 to 3 can help here.
- It scales to small and big organizations. The use of separate process in every environment prevents using procedures for restrictive environments all over the organization.



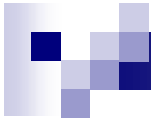
Advantages

- It supports explicitly the outsourcing of security management and operations processes. The results for each process are defined and the responsibilities to perform each process are defined too.
- It provides work product metrics, that help to manage the processes and measure the success of the ISM system.
- It provides Information Security Governance guidance.



Summary

- Business Focused
- Manageable (with Metrics)
- Compatible (ITIL, ISO27001, ISO9001)
- Adaptable
- Flexible
- Open Standard, readily available
- Rich in implementation guidance



Questions?

?

?

?

?



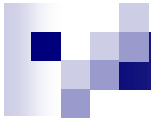
Conferencias **FIST** Marzo/Madrid 2006 @
www.fistconference.org



Thanks for your attention!

Sponsored by:





Creative Commons Attribution-NoDerivs 2.0

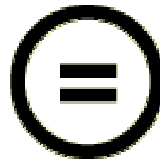
You are free:

- to copy, distribute, display, and perform this work
- to make commercial use of this work

Under the following conditions:



Attribution. You must give the original author credit.



No Derivative Works. You may not alter, transform, or build upon this work.

For any reuse or distribution, you must make clear to others the license terms of this work.

Any of these conditions can be waived if you get permission from the author.

Your fair use and other rights are in no way affected by the above.

This work is licensed under the Creative Commons Attribution-NoDerivs License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nd/2.0/> or send a letter to Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.