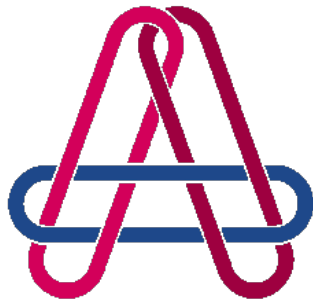


DISCUSSION DOCUMENT

Convergence of Enterprise Security Organizations: International Views

An Addendum to the 2005 Study



The Alliance for Enterprise
Security Risk ManagementSM

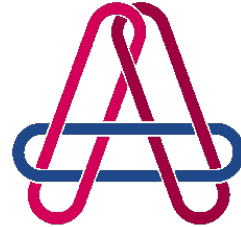
The Alliance for Enterprise Security Risk Management
24 July 2006

Presentation Outline

- ▶ **Introduction**
 - Background and context
- ▶ **Findings**
 - What we discovered
- ▶ **Implications**
 - What this means for you

Introduction—Background and Context

Convergence Study—Third Quarter 2005



The Alliance for Enterprise
Security Risk ManagementSM

▶ Alliance Study



▶ AESRM believes that enterprise security functions are rapidly converging.

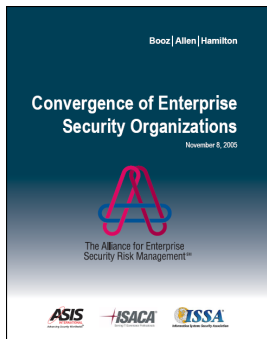
“The identification of security risks and interdependencies between business functions and processes within the enterprise and the development of managed business process solutions to address those risks and interdependencies”

To complement the convergence study findings, we added insights from security managers at internationally-based companies.

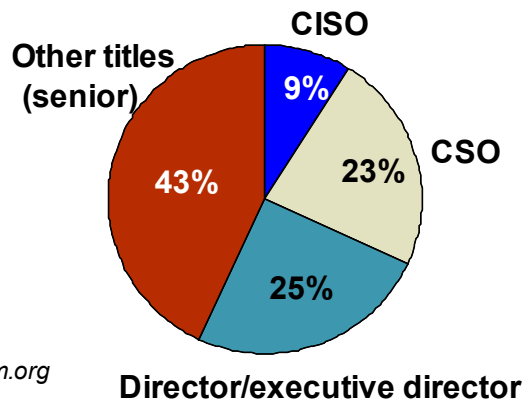
2005 Convergence Study (US)

- ▶ The 2005 study consisted of a survey and interviews to gain a greater understanding of the state of security convergence in the US.
- ▶ A published white paper explained the findings in the context of convergence.
- ▶ The result was an identification of various business operating levers, such as risk management, governance and integration, that are “actionable” and lead to convergence.

Titles of Interviewees (US-ASIS members)



Free download: www.aesrm.org

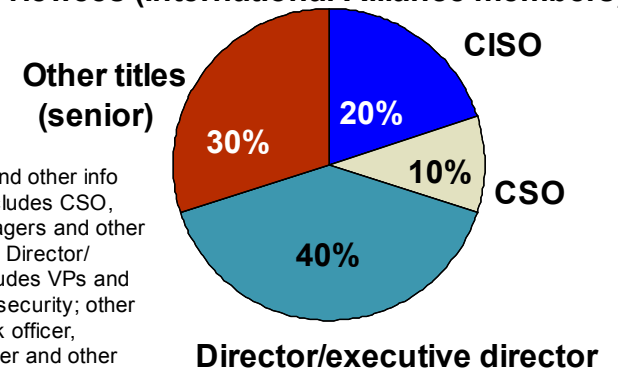


2006 International Perspectives

- ▶ Leveraging the 2005 findings, we surveyed and interviewed a similar profile of security leaders from internationally-based companies.
- ▶ Comparable industries were represented: financial services, oil and gas, tobacco, telecom and technology, and aerospace.
- ▶ Companies had primarily over US \$10B in revenues and employees between 10K to >30K.

Titles of Interviewees (International-Alliance members)

CISO includes CISO and other info security titles; CSO includes CSO, physical security managers and other physical security titles; Director/executive director Includes VPs and executive directors of security; other titles include senior risk officer, information risk manager and other risk-related titles.



Findings—What we discovered

While there was alignment with previous findings...

- ▶ **Most participants agreed that the concept of convergence, as defined by AESRM, appears to be understood by the international enterprise security community.**
- ▶ **Convergence is influencing strategic change within enterprises related to priorities and governance.**
 - Increased evidence of active board and senior group leadership involvement in the governance of security
 - Companies are developing risk councils and group risk committees to increase transparency into enterprise risks from the top.
- ▶ **...and these changes are driving the development of process-based capabilities within security organizations**
 - Integration across security functions requires an ability to share resources, understand interdependencies, and link security with enterprisewide business processes.
 - Development of a common language for security across the enterprise requires well-articulated security policies and procedures as well as an ability to successfully communicate the business case for security.
- ▶ **...which in turn has implications for security leaders' roles and responsibilities**
 - Increased evidence of senior security leadership having responsibility for multiple security functions (e.g., physical and corporate security reporting into one security executive)
 - Evidence of an increased need for security professionals to have a broader knowledge of the business (e.g., knowledge of where in the business value chain security can have the greatest impact)
 - Evidence of a rise in the importance of a senior risk executive (e.g., a CRO or head of risk services)

...there are some differences, especially in Europe

- ▶ **Enterprises and security professionals in Europe appear to be less driven primarily by regulatory and compliance mandates.**
 - Interviewees cited cultural differences between Europe and the US which may result in different approaches to regulation (e.g., Europeans view their regulations as less explicit and prescriptive).
 - ▶ Sarbanes Oxley, in particular, was viewed as a current example of a prescriptive, US-led regulation, while current EU-led regulatory directives such as those for data protection were viewed as more flexible.
 - ▶ Another factor contributing to a different European approach is likely related to having to manage 25 member states—successful harmonization dictates that regulations be less prescriptive in nature.
 - Interviewees believe that a truly secure organization is one that possesses the flexibility to look beyond external mandates (e.g., focusing on compliance as a business goal can have the unintended affect of lulling an enterprise into a false sense of security).
 - Interviewees with large US-based operations believe that US-led compliance and regulatory mandates have a significant impact on their global risk management approach...and this could distort risk management toward more of a box-checking exercise.

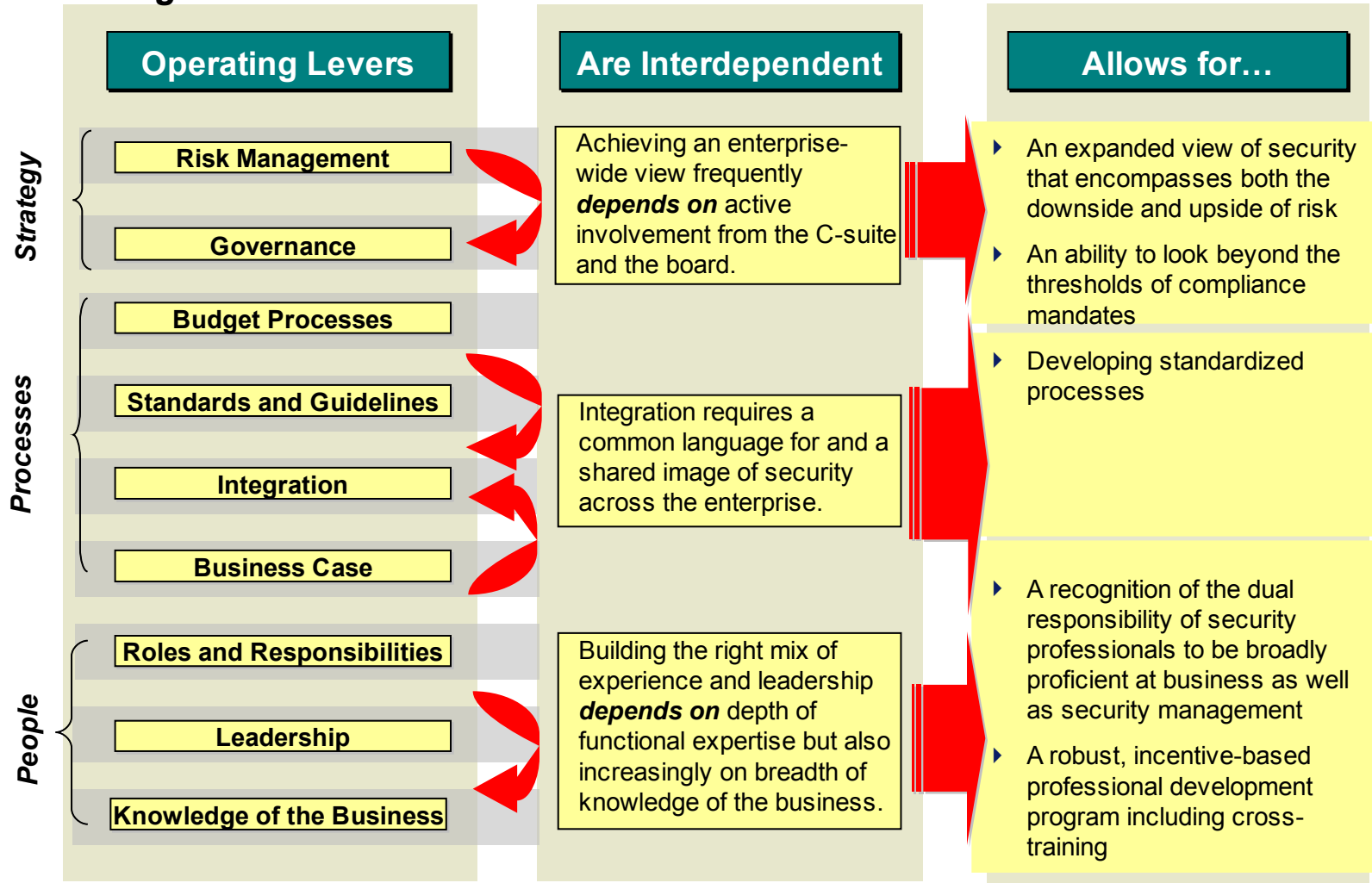
- ▶ **...believe there is a need for a better understanding of the role that compliance plays in security governance and risk management within global enterprises**
 - Compliance in itself is not seen as a business goal, but rather as a set of guidelines embedded within an organization's approach to risk management...where relevant compliance measures are leveraged to achieve an optimal risk posture.
 - Risk management involves understanding and managing the potential upside in addition to the downside of risks—an undue focus on compliance can narrow an organization's view solely to the downside of risk.

There is consensus on the operating levers and the need for a shift in emphasis.

	Operating Levers	FROM	TO
Strategy	Risk Management	Asset-based view	Enterprisewide view
	Governance	Passive and infrequent	Active board involvement
Processes	Budget Processes	"Not my domain"	Common language with peers
	Standards and Guidelines	Functionally focused	Common and shared widely
	Integration	Forced	Adaptive
	Business Case	Technical/jargon-filled or None	"C-suite" language
People	Roles and Responsibilities	Functionally defined	Multiple competencies
	Leadership	Command and control	Empowering and enabling
	Knowledge of the Business	Functional knowledge	Broad business understanding

However, interviewees expressed the need to understand the evolving interdependencies among the levers...

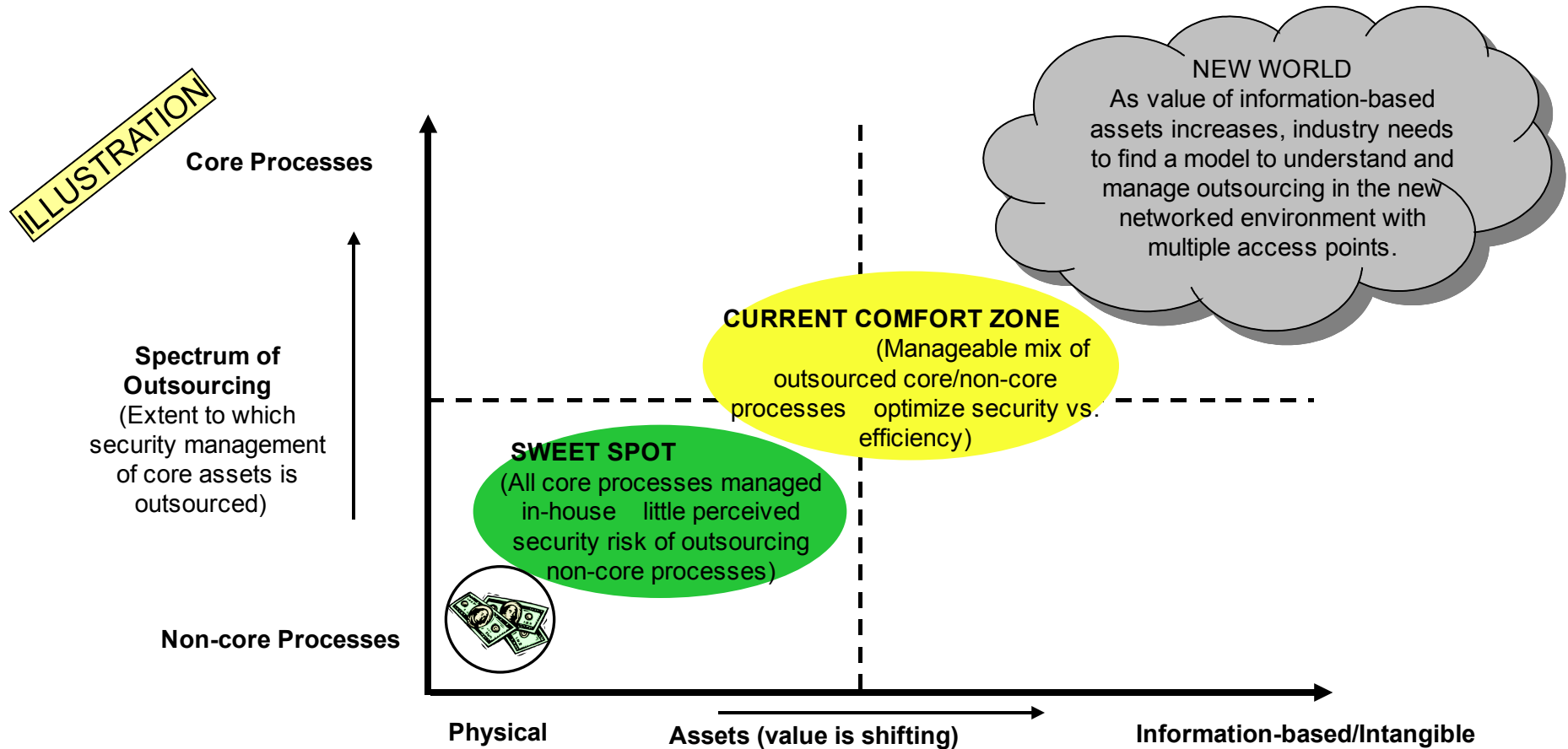
Understanding how:



...as well as the imperatives.

Evolving Imperatives

- ▶ The accelerating shift in enterprise value from physical to information-based assets has security implications
- ▶ Simultaneously, these information based assets are becoming network based, outsourced readily, and consist of multiple access points



Implications—What this means for you



Incorporating new perspectives...

▶ Cultural differences...

- The view from Europe is that compliance mandates can have the unintended affect of narrowing an organization's view of security.

▶ ...can drive different approaches to security risk management.

- Most European interviewees either sat on, or reported to an individual who sat on, a risk council or group risk committee.
- Senior leadership of the organization participated including representatives from HR, legal, strategy, operations and security.
- **Interviewees highlighted the benefits to include:**
 4. Decision-makers have a greater understanding of risks that face the organization, leading to a more positive perception of, and active role for, security across the enterprise.
 5. A designated forum for discussing security and risk-related issues specific to each region allows an opportunity for senior leadership to look for interdependencies and synergies when crafting a response.
 6. This helps align priorities at the top and links security with the strategic decision-making process of the enterprise



- ▶ Simply "Liability" management
- ▶ Ignores non-US standards
- ▶ Could hamper global competitiveness
- ▶ Invites audit



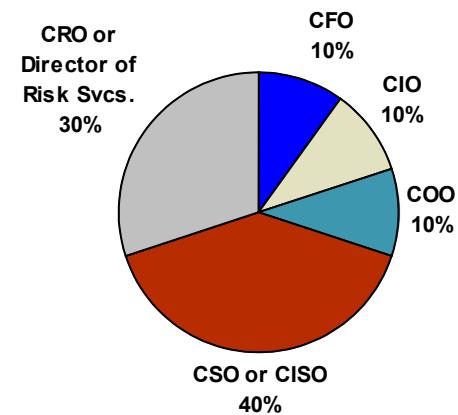
- ▶ Market indexed risk agenda
- ▶ Appropriate levels of accountability
- ▶ Compliance and audit processes embedded
- ▶ Guidelines rather than standards



- ▶ Distortion of risk priorities & agenda
- ▶ False sense of security
- ▶ Distorted asset allocation

ILLUSTRATIVE ONLY

Who are security managers reporting to?



...could benefit both the membership and the AESRM organization.

▶ **For AESRM founding organization members:**

- Develop an ability to look beyond the thresholds of compliance mandates.
- Include potential upside of risk as part of the dialog.
- Achieve a more optimal risk posture resulting in a more secure enterprise.

▶ **For the AESRM organization:**

- Opportunity to capitalize on this knowledge and incorporate it into conferences, member education initiatives, and internal strategic planning processes
- Opportunities for membership growth in new regions (e.g., better alignment with European membership)