

THALES



# Implementing Security Standards and Guidelines in a Multinational Company

National Security Director

Senior Regional Vice President ASIS International - Australia

February 2010

## Thales of Miletus

Tradition of Greek scholarship began with Thales (624-545 BC) of Miletus (a port near Turkey). Thales argued against superstition and sloppy thinking.

He asserted that the Earth is round on the basis of the observation that the mast of a sailing ship appears first for an incoming ship, and disappears last for an outgoing ship. This was remarkable insight: Based on certain facts interpreted in certain ways one could infer about what is well beyond the reach.



**Salus populi suprema lex** - *The safety of the people is the supreme law. (Cicero)*



**salus** : *health, safety, well-being, salvation / Salutation.*

**securus** : *safe, secure, free from care, unworried, unconcerned.*



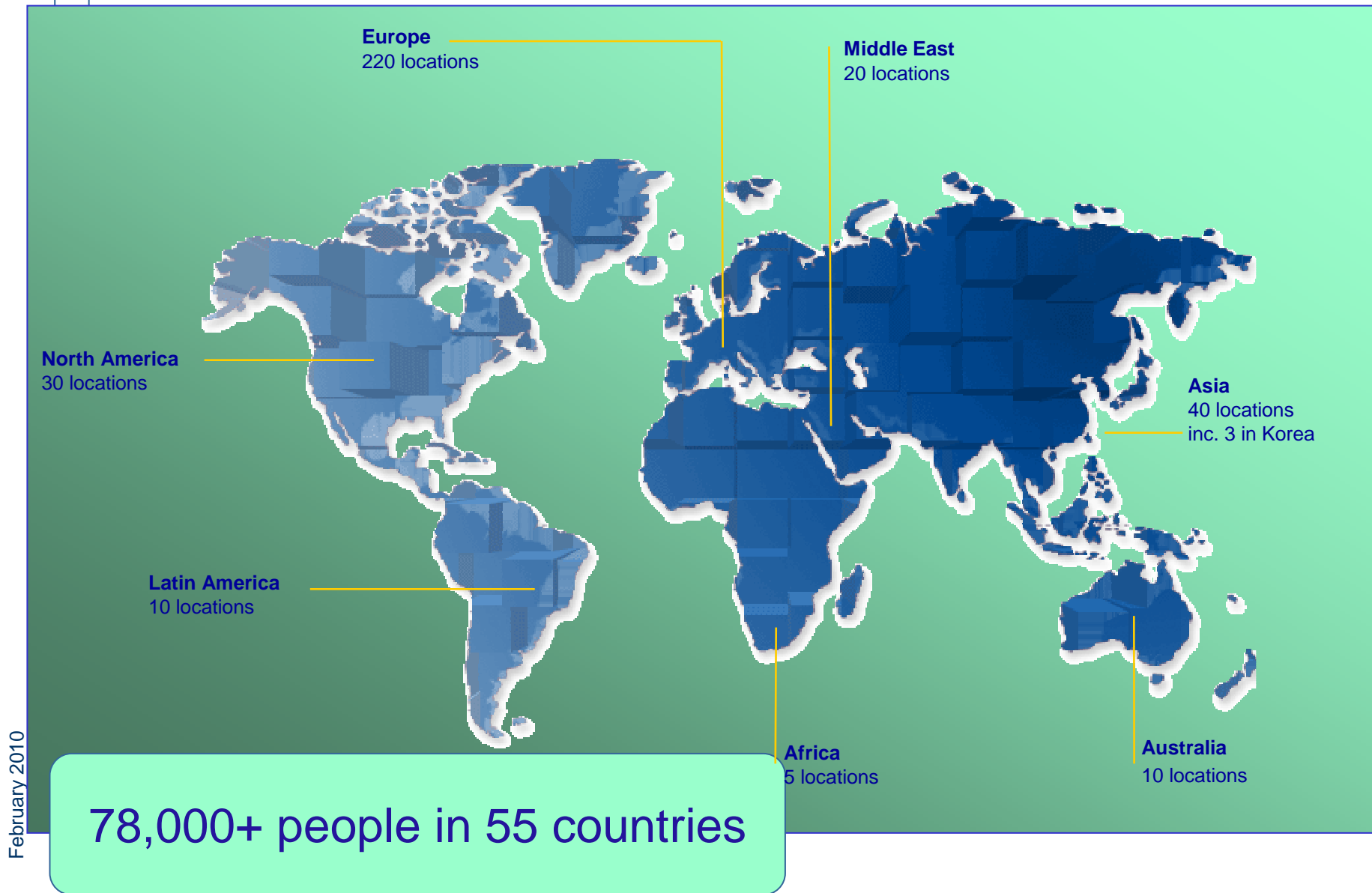
## Thales Employee Awarded Nobel Prize in Physics

The Royal Swedish Academy of Sciences has awarded the Nobel Prize in Physics for 2007 to Albert Fert, Scientific Director for Unité Mixte de Physique CNRS/Thales, and Peter Grünberg, Forschungszentrum Jülich, Germany, "for the discovery of Giant Magnetoresistance."



*Albert Fert, Scientific Director for Unité Mixte de Physique CNRS/Thales*

# Part of a Global Company



February 2010

# Security, Capability and Sustainment



Thales, like other companies in the defence and national security market, takes on an implied obligation, not writ in any commercial document, to work under certain constraints which derive from an understanding of the military's role in society and their moral responsibility to act through the profession of arms.

Companies that don't understand this connection are acting with a commercial interest only.

Companies that do understand this connection take specific actions in relation to security that goes beyond the minimum requirements and transcends the standards.

# A Secure Thales Solution with high security



# Security Outcomes

---



**Reputation**

**Product Integrity**

**Suitable people**

**Available assets**

**Trusted partnerships**

**Shareholder support**

# Sources of Security Risk

- **Compliance failure**
- **Insider threat** - disgruntled employees
- **Issue motivated actions** - Protest Groups
- **Criminal threat** - Outlaw Motorcycle Gangs, theft and extortion
- **Terrorism** - within and outside Australia
- **Espionage** - State and Commercial

The Security Mission is to protect Thales Australia from the security threats to its business.

So that

- Customers are Confident
- Intellectual Property is Protected
- Assets are Protected
- Capability is Preserved
- Partners are Assured
- Compliance Achieved



Booz | Allen | Hamilton

# Convergence of Enterprise Security Organizations

November 8, 2005

**ASIS**  
American Society for Information Security

**ISSA**  
Information Systems Security Association

**Information Security Audit and Control Association**



## 1.0 Executive Summary

ASIS International identifies security “convergence” as a trend affecting global enterprises. ASIS International defines convergence as,

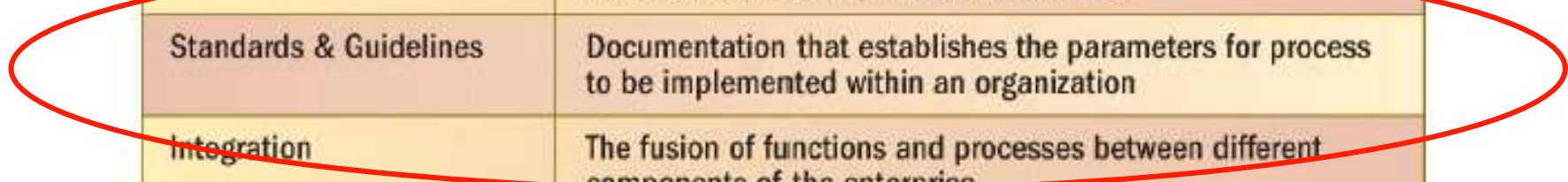
*“the identification of security risks and interdependencies between business functions and processes within the enterprise and the development of managed business process solutions to address those risks and interdependencies.”*

*—ASIS International*

This definition captures a significant shift in emphasis from security as a purely functional activity within an enterprise, to security as a “value add” to the overall mission of business.



Operating Level	Description
Risk Management	Evaluating threats, vulnerabilities, and business impacts to determine strategy for operating within an acceptable level of risk
Governance	System and processes in place to establish authority and responsibility
Budget Processes	Method by which all of the anticipated expenses and revenues of an enterprise are determined
Standards & Guidelines	Documentation that establishes the parameters for process to be implemented within an organization
Integration	The fusion of functions and processes between different components of the enterprise
Business Case	Structured document describing an analysis of the situation and an intended course of action for success
Roles and Responsibilities	Formal documentation of the responsibilities within each role of an organization
Leadership	The authority to guide or direct the actions of a company
Knowledge of the Business	Understanding of the enterprise's mission, goals, objectives, and its organization





# THE CONVERGENCE OF PHYSICAL AND INFORMATION SECURITY IN THE CONTEXT OF ENTERPRISE RISK MANAGEMENT



**Deloitte.**



**Figure 1—Shifts In Thinking: People, Processes and Strategy**

	<b>Operating Levers</b>	<b>FROM</b>	<b>TO</b>
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

Source: Booz Allen Hamilton



**Figure 15—The Risk Intelligence Framework**



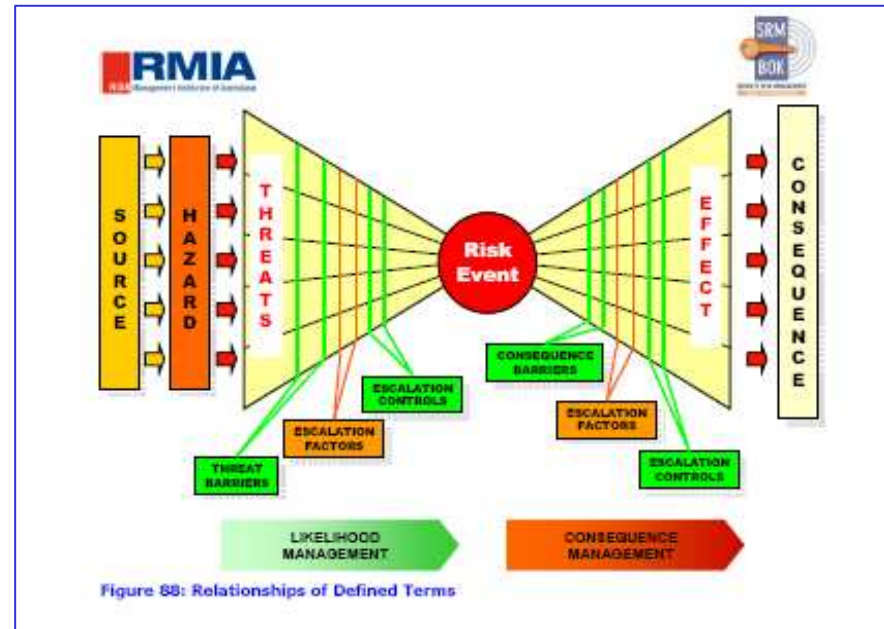
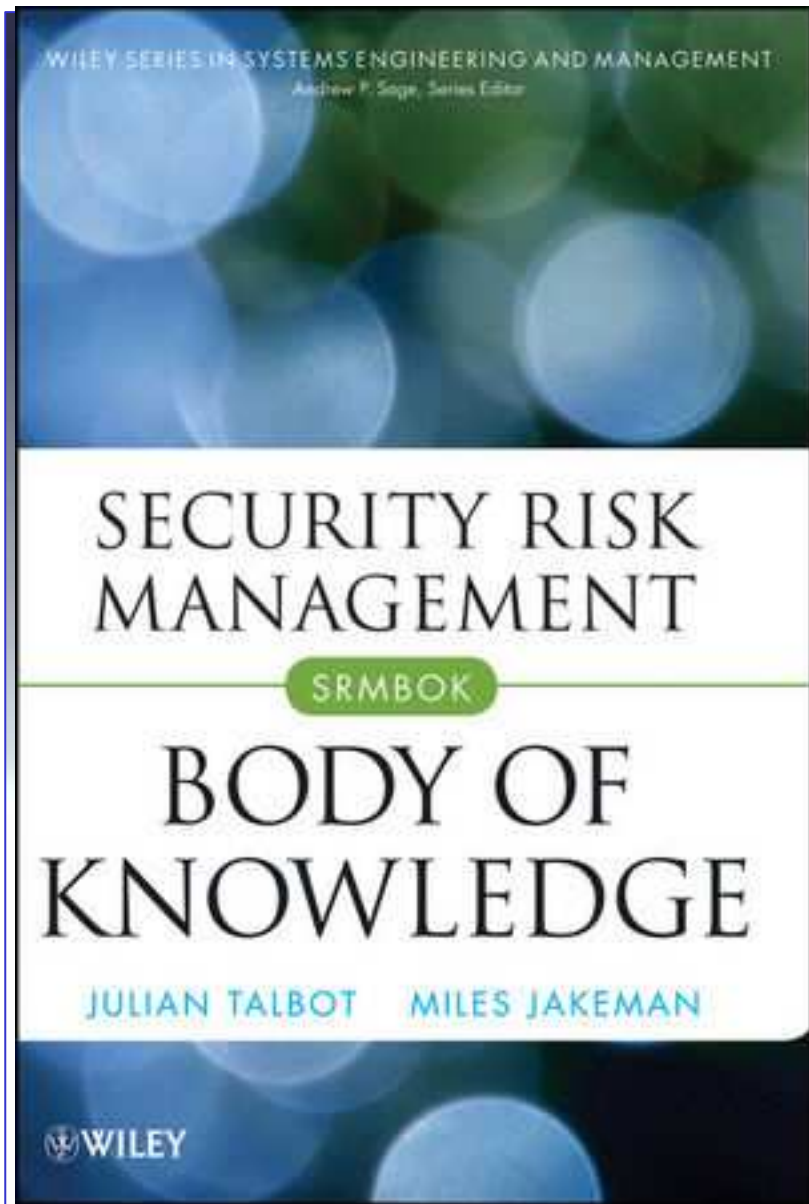
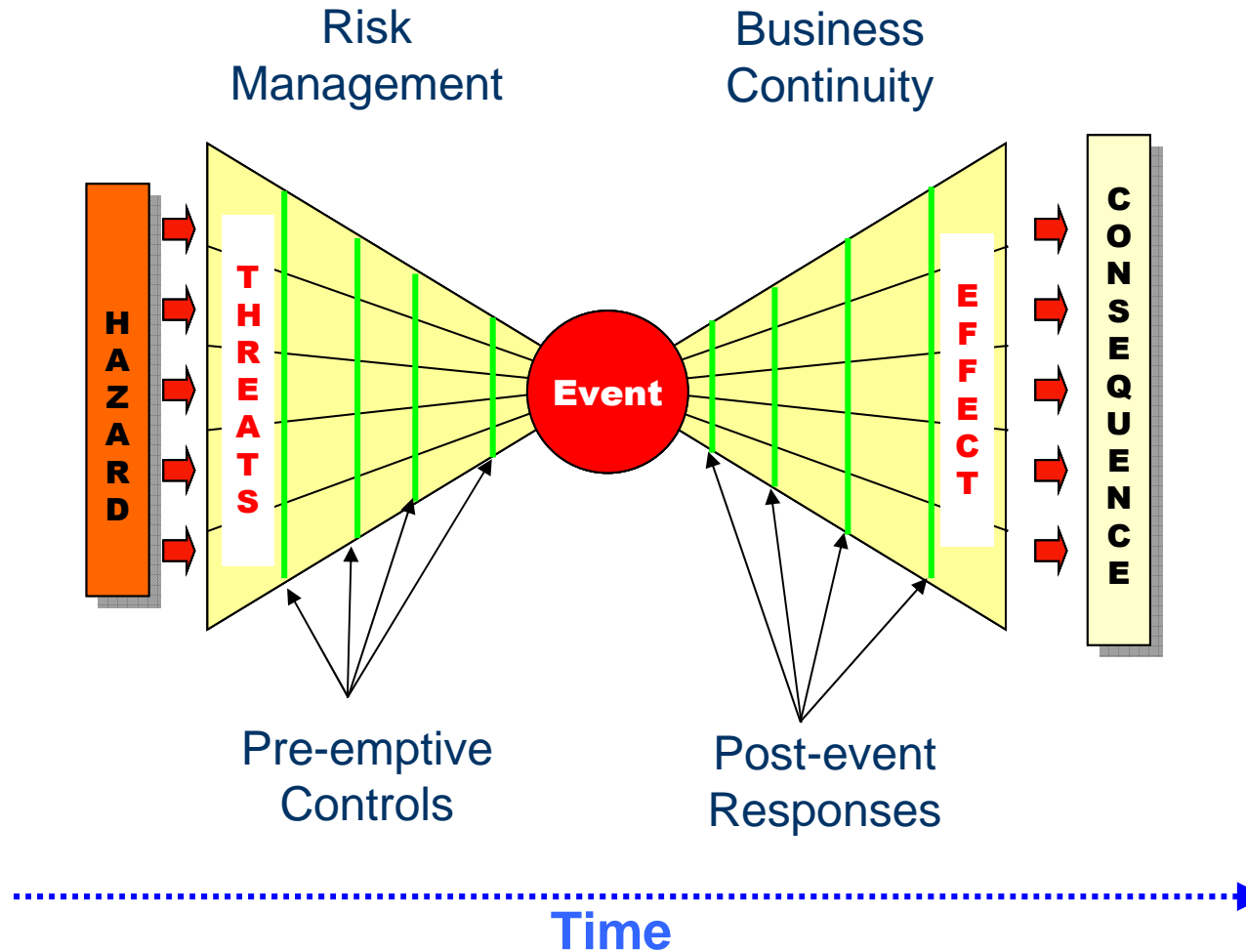


Figure 88: Relationships of Defined Terms

# Relationships to Risk Management

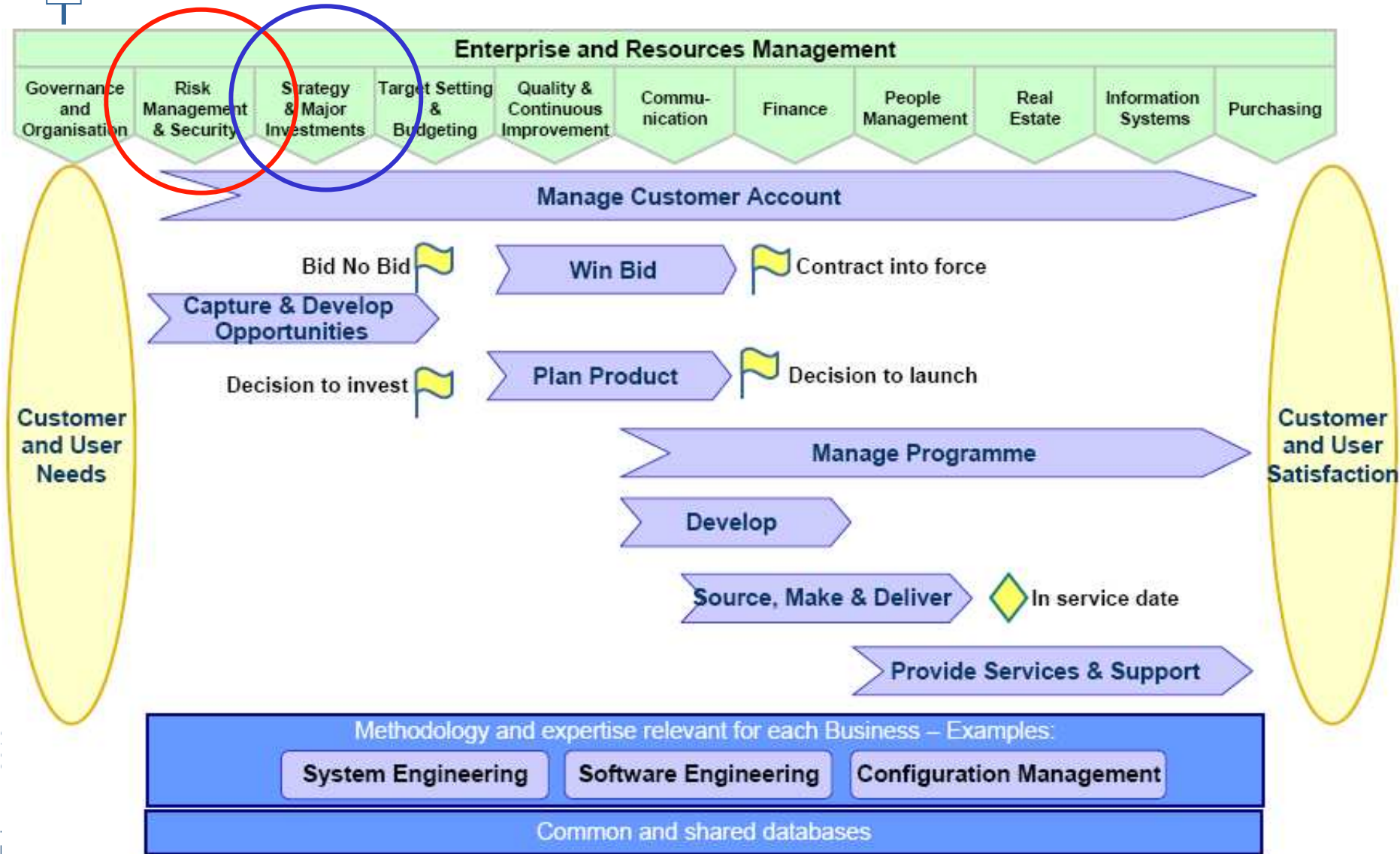


# Implementing a Standard

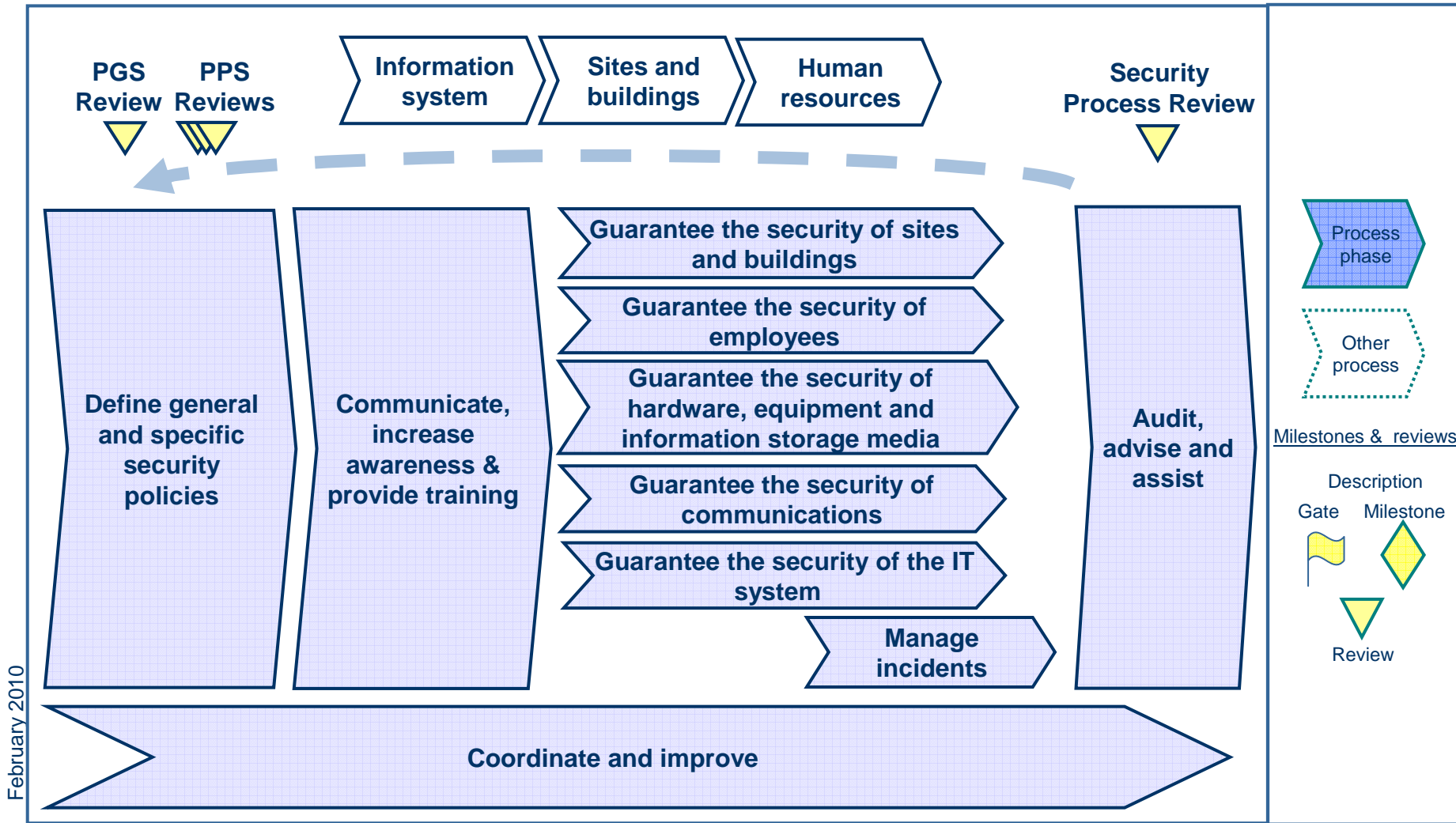
---

- Is the Standard relevant
- How mature is your system
- Review your System for adequacy
- Conduct gap analysis against the standard
- Identify and prioritise requirements
- Develop, amend and/or discard non aligned processes

# Compliance in CHORUS

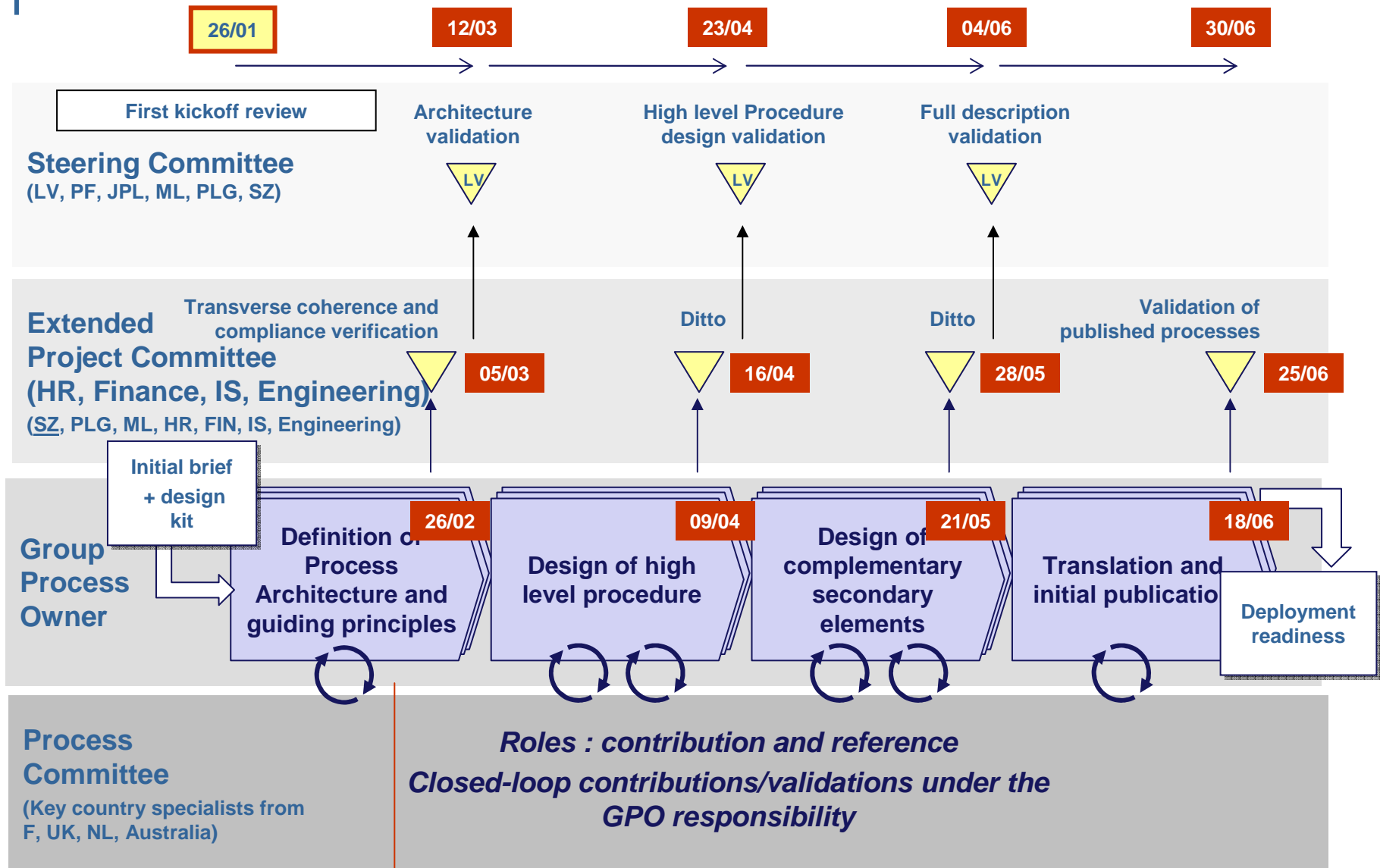


# OVERVIEW



February 2010

# Proposed Process Design methodology



February 2010



**FIGURE 1.3** Risk-Management Framework (ISO 31000:2008)

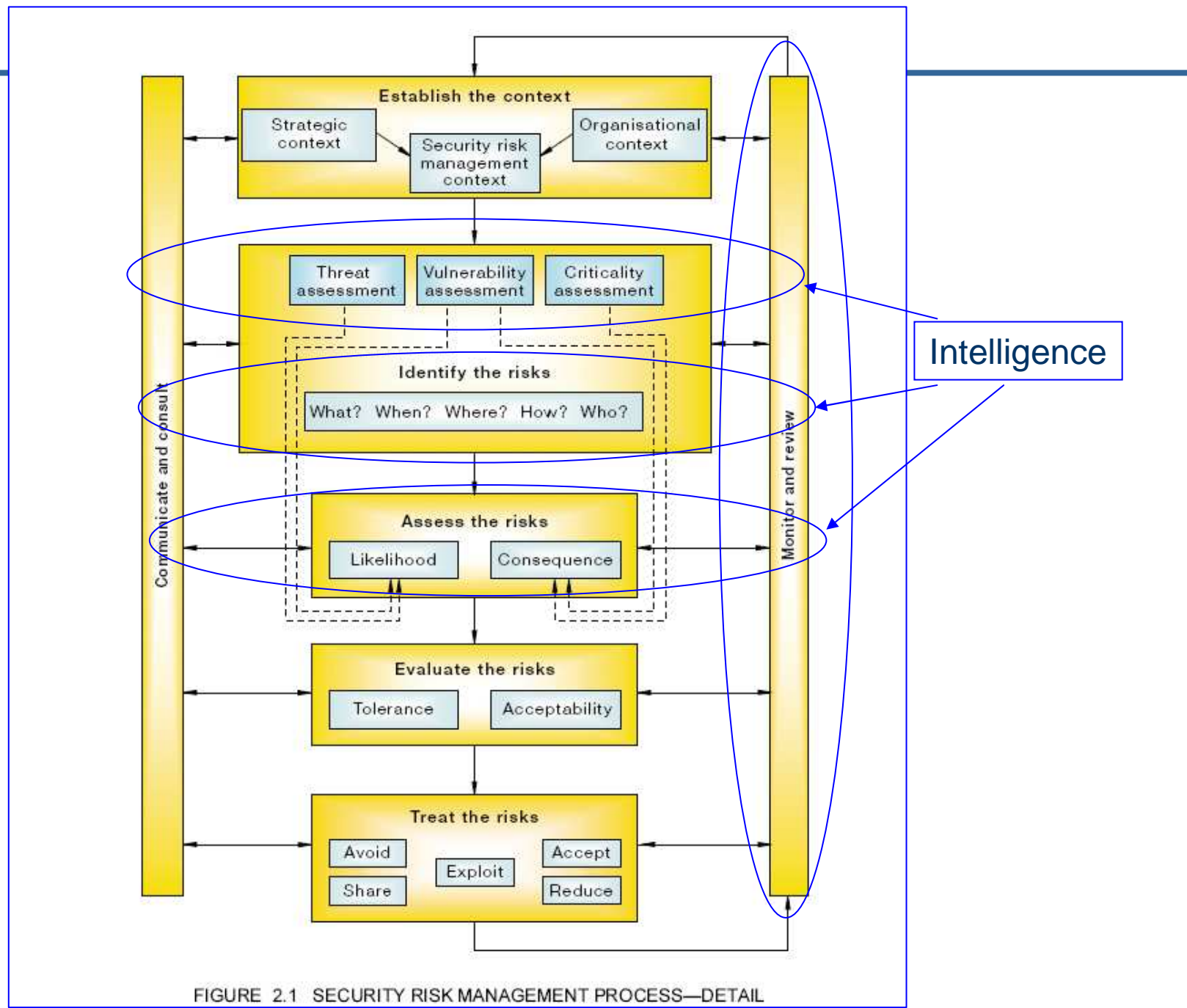
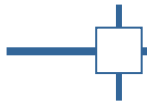
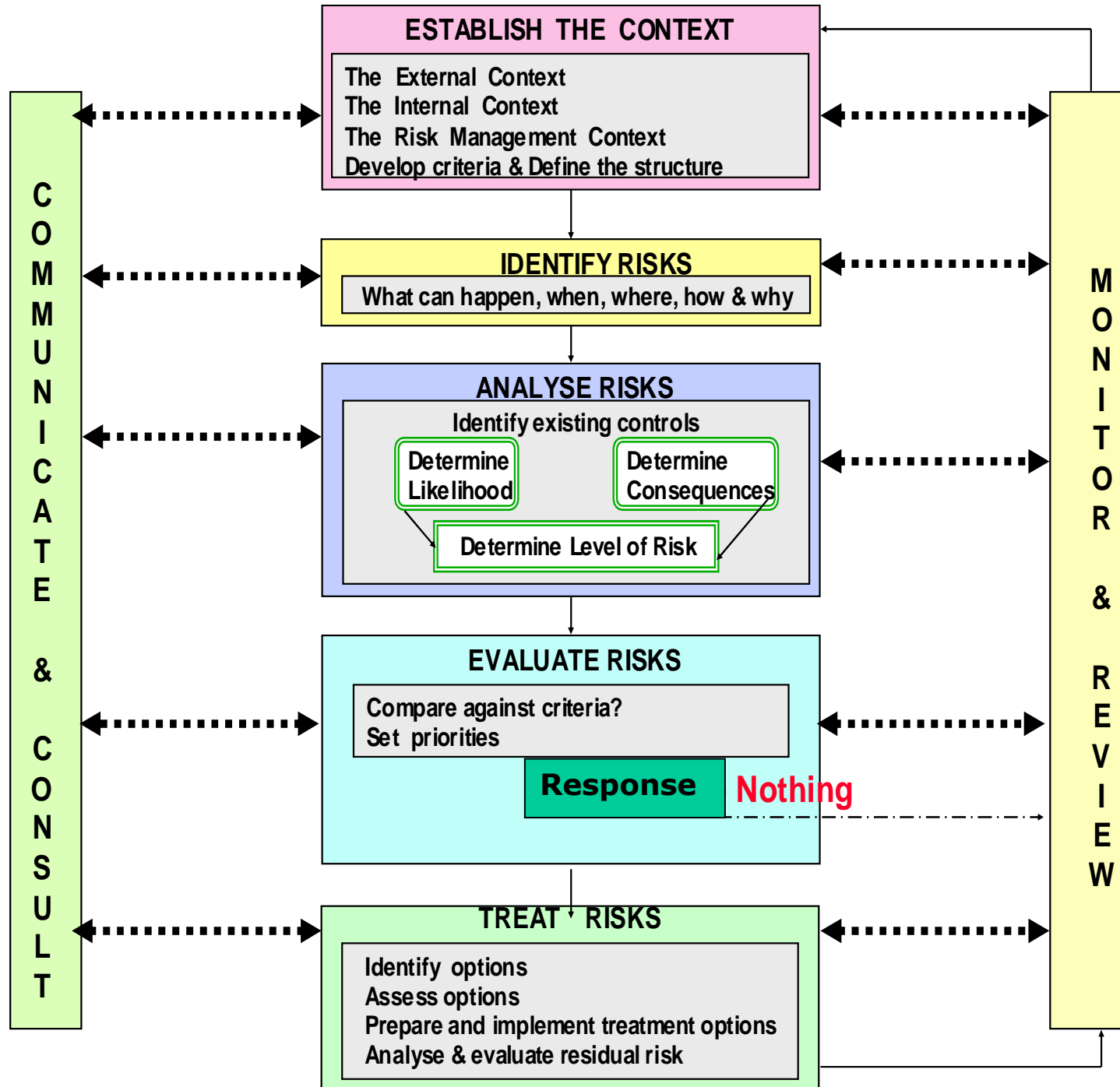


FIGURE 2.1 SECURITY RISK MANAGEMENT PROCESS—DETAIL



# Information Security Standards



AS/NZS ISO/IEC 27001:2006  
Information technology – Security techniques  
– Information security management systems  
– Requirements



A1 | AS/NZS ISO/IEC 27002:2006  
Information technology – Security techniques  
– Code of practice for information  
security management



This is a free 15 page sample. Access the full version online.

STANDARD

AS/NZS

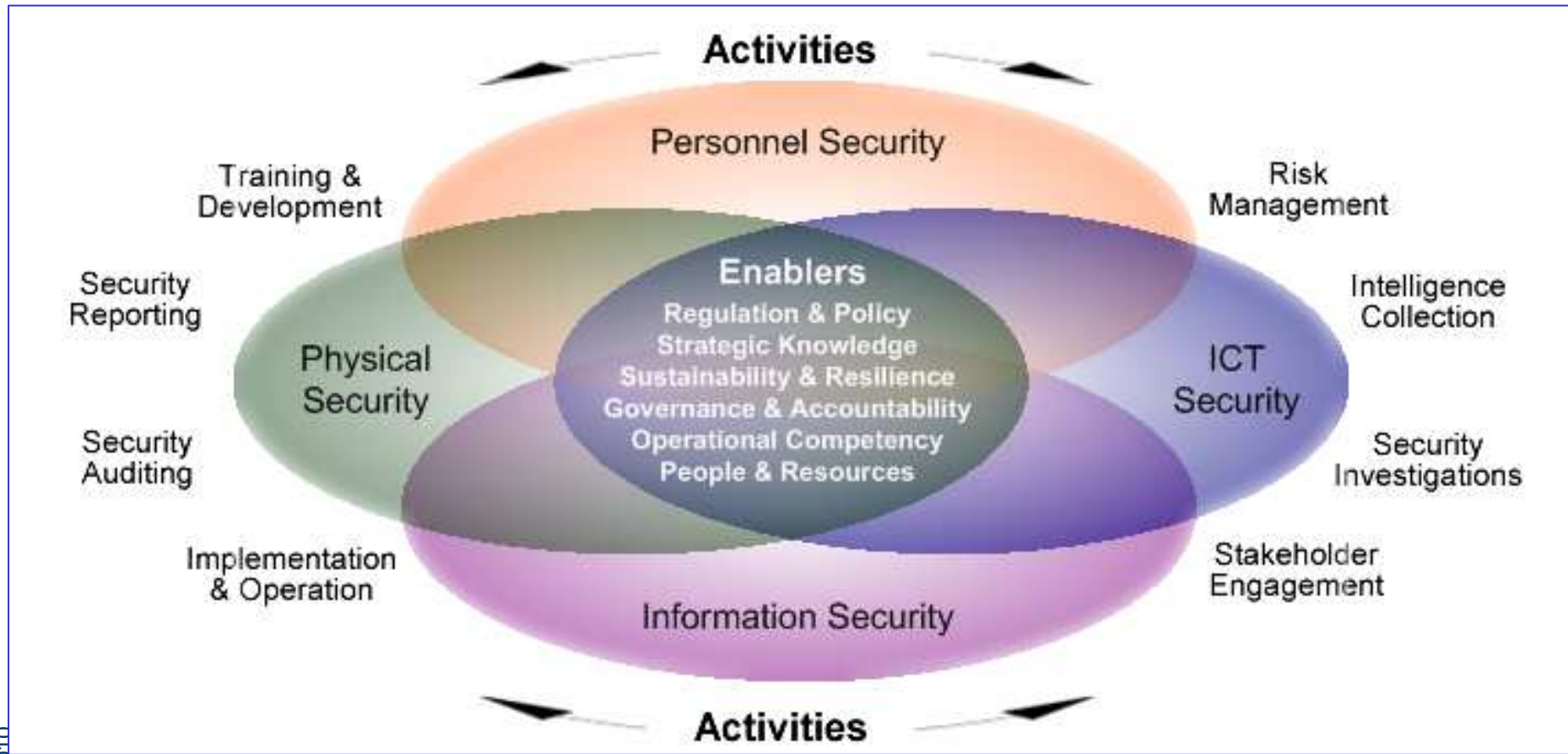


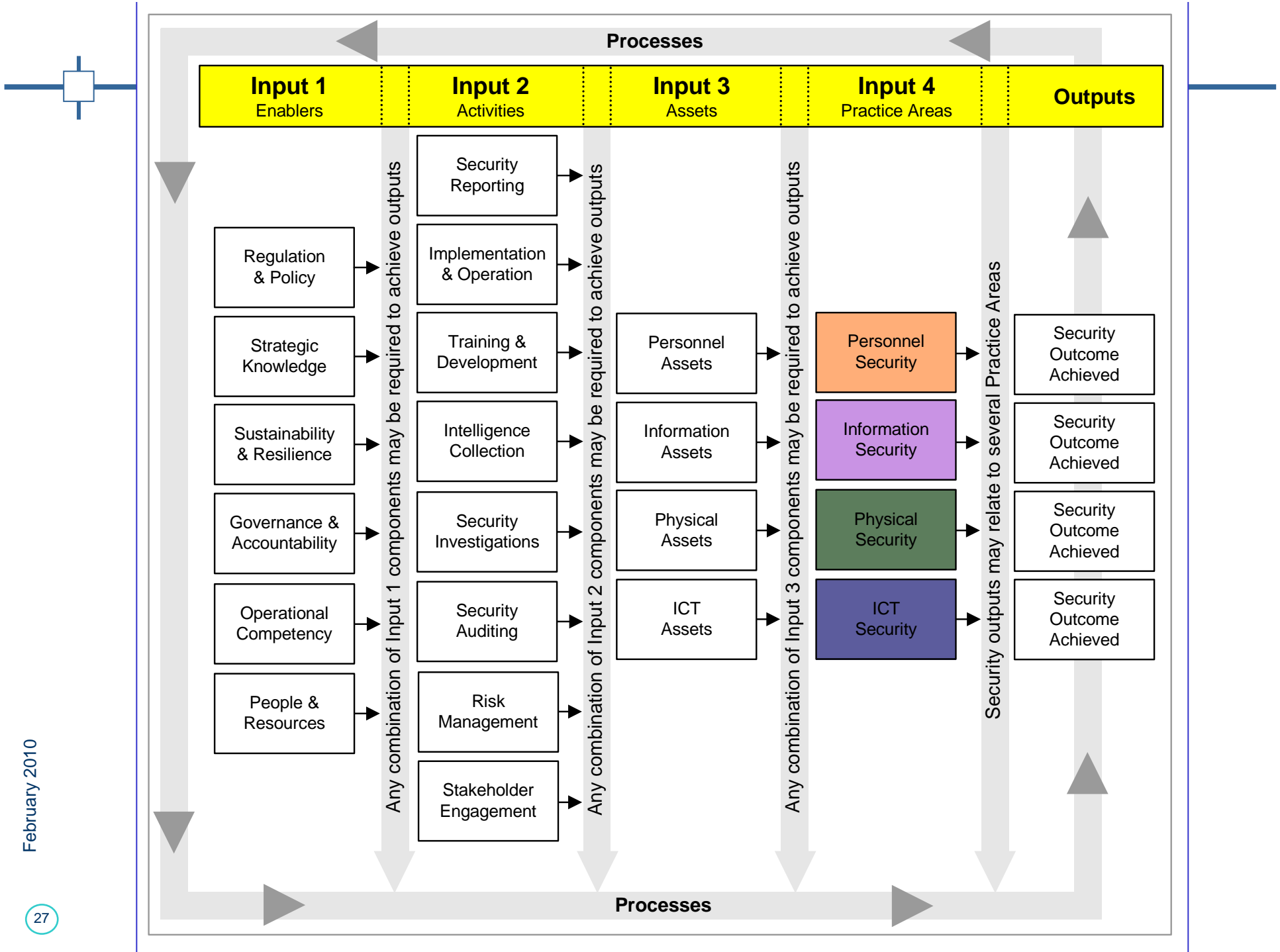
This is a free 15 page sample. Access the full version online.

STANDARD

AS/NZS







# Security Management

**Security management activities** are performed by all security personnel.  
They include:

- **Security Reporting**
- **Training and Development**
- **Intelligence Collection**
- **Security Investigations**
- **Travel Security**
- **Auditing, Reviews and Inspections**
- **Security Risk Management**





# Chief Security Officer

G U I D E L I N E

2008 Edition

**ASIS**  
INTERNATIONAL  
Advancing Security Worldwide®

## 12.1 Model Profile of a Chief Security Officer Function

<u>Risks</u>	<u>Potential Processes &amp; Services</u>	<u>Skill Set Required</u>
Human Resources & Intellectual Assets	Global Security Policy & Procedures Administration	<b><u>Relationship Manager</u></b> <i>Develops, influences and nurtures trust-based relationships with business unit leaders, government officials and professional organizations. Acts as a consultant to all organizational clients.</i>
Ethics & Reputation	Technology & Infrastructure Protection	
Financial Assets	Information Risk Management	
Information Technology (IT) Systems	Business Continuity, Crisis Management & Response	<b><u>Executive Manager &amp; Leadership</u></b> <i>Builds, motivates and leads a professional team attuned to organizational culture, responsive to business needs and committed to integrity and excellence.</i>
Transportation, Distribution & Supply Chain	Employee Risk Awareness	
Legal, Regulatory & General Counsel	Investigative & Forensic Services	<b><u>Subject Matter Expert</u></b> <i>Provides or sees to the provision of technical expertise appropriate to knowledge of risk and the cost-effective delivery of essential security services.</i>
Physical & Premises	Safe & Secure Workplace Operations	
Environmental, Health & Safety**	Tailored Business-Process Safeguards	<b><u>Governance Team Member</u></b> <i>Provides intellectual leadership and active support to the organization's governance team to ensure risks are made known to senior management and the Board.</i>
	Insurance & Risk Transfer	
	Risk Assessment, Evaluation, & Testing	
	Executive Protection	<b><u>Risk Manager</u></b> <i>Identifies, analyzes and communicates on business and security-related risks to the organization.</i>
	Background & Due Diligence Investigations	
	Business Conduct & Security Compliance	<b><u>Strategist</u></b> <i>Develops global security strategy keyed to likely risks and in collaboration with organization's stakeholders.</i>
	External & Government Relations	
	Business Intelligence & Counter-Intelligence Support	<b><u>Creative Problem Solver</u></b> <i>Aids competitiveness and adds value by enabling the organization to engage in business processes to mitigate risk. Be a positive change agent on behalf of organizational protection.</i>

\*\*Recognizing that EH&S may be structured outside the scope of security functions, there are still significant risk issues to an organization. Since many organizations have combined their EH&S and security functions, we have chosen to present it in this Guideline for consideration.



### 13.1 Key Success Factors

- Ability to build sustainable competitive advantages through pragmatic, innovative security solutions.
- Demonstrated integrity and ability to maintain principles under internal and/or external pressure.
- High-quality analytical skills, management experience, and exceptional relationship management competencies.
- Qualitative experience in strategic planning and/or policy development at a senior level.
- Ability to anticipate, influence, and assist the organization to assess and rapidly adjust to changing conditions and trends (internal and external) of importance to the direction of the organization.
- Effectiveness in communicating recommended courses of action for innovative, business-oriented responses.
- Passion for excellence and a demonstrable orientation toward successful staff development.



The CSO will need skills and competencies to accomplish the following:

- Relate to and communicate with senior executives, the Board of Directors and its operating committees.
- Understand the strategic direction and goals of the business and how to intertwine security needs with the goals and objectives of the organization. This implies the ability to establish a vision for the global and individual business security programs and to build support for their implementation and ongoing development.
- Understand and assess the impact of changes in the areas of economics, geopolitics, organizational design and technology, and how they relate to potential threats and risks to the organization.
- Ensure security incidents and related ethical issues are investigated and resolved without further disrupting operations, and are conducted in a fair, objective manner in alignment with the organization's values and code of business conduct.
- Facilitate the use of traditional and advanced scenario planning techniques in assessing risks and threats to the organization.
- Understand how to successfully network and develop working relationships with key individuals in staff and line positions throughout the organization.
- Promote organization learning and knowledge sharing through internal and external information resources in line with the culture of the organization.
- Be politically astute but not politically motivated.
- Be realistic and comprehend the need to assess the financial, employee, or customer implications of any plan or recommendation.
- Function as an integral part of the senior management team with regard to planning and capital expenditures.
- Develop organization-wide security awareness as appropriate for the business and the culture of the organization.



A description of the ideal CSO also should include the following personal characteristics:

- Strategic orientation with ability to act tactically, as required
- Highly skilled in succeeding in a matrix-management environment
- Global perspective, multi-cultural understanding and approach
- Detail focused, as required
- Excellent conceptual and critical thinking skills
- High integrity
- Emotional maturity
- Strong negotiator/facilitator and consensus builder
- Understands principles of process management

# Role of the Chief Security officer



## **Principal Responsibilities:**

The CSO is responsible for the operational development, coordination and audit of Thales Australia's Protective Security Program, in accordance with the General Security Policy, Plans and legal and statutory obligations. Where required the CSO assumes the role of Acting National Security Director, exercising corresponding delegations and authorities for the duration of the appointment.

## **Specific Duties/Responsibilities:**

Implement and coordinate protective security measures for Thales Australia based on requirements of the Security Committee of the Board of Directors and National Security Director.

Represent and liaise on behalf of Thales Australia to Government on necessary issues.

Liaise with Defence Security Authority and other agencies as required for the Defence Industry Security Program.

Develop and maintain the TASON.

Provide strategic and operational security advice to security managers and employees.

Develop and maintain arrangements for an ongoing program of security education and training for employees.

Ensure the investigation and report on significant security breaches; make recommendations and audit the effectiveness of corrective actions.

Develop and maintain an ongoing audit program designed to promote early identification of issues and instances of non-compliance.

Liaise with State and Federal Police for investigative and protective action, as required.

Liaise with the appointed Chief Information Security Officer (CISO) and Technology Control Manager (TCM) to ensure effective coverage of security across Thales Australia.

Support Vice President Operations in business continuity and risk management activities.

Implement and observe effective security risk management practices.

Undertake other duties as directed by National Security Director.

## **Essential Qualifications and Experience:**

A current Australian security clearance at **TOP SECRET** (minimum) or ability to obtain one

## **Preferred Qualifications and Experience:**

Tertiary qualifications in Security Risk Management, Intelligence, International Relations and/or Investigations.

Experience and involvement in the development of commercial protective security programs.

Experience and involvement in the development of Defence protective security programs.

A current Australian security clearance at **TOP SECRET** (minimum).

Availability to undertake national and regional travel as required.

Management and operational experience in working for or with Government on security issues in areas such as: Attorney General's Portfolio; Defence; Defence Industry; National or State Police, relevant compliance or investigation agencies.

# Summary and Questions

---



vado iam quod prospicio