

# Information Security Management as a Business Driver

Georges Ataya,  
Professor at Solvay Business School



Solvay.edu/ict – itqi.org – isaca.org

## Georges Ataya **MSCS, PBA, CISA, CISM, CISSP, CGEIT**

- Professor and Academic Director of IT Management Education at Solvay Business School ([www.solvay.edu/it](http://www.solvay.edu/it))
  - Executive Master in IT Management
  - Executive Master in ICT Audit & Security
  - Executive Master in IT Governance
- International Vice President of the IT Governance Institute (ITGI.org) and member of the Board of ISACA (isaca.org)
- Managing Partner ICT Control NV-SA ([www.ictcontrol.eu](http://www.ictcontrol.eu))
- Participated in the research and development of various publications.
- [Georges@ictcontrol.eu](mailto:Georges@ictcontrol.eu) – [www.ataya.info](http://www.ataya.info)



Solvay.edu/ict – itqi.org – isaca.org

# ISACA and ITGI

The screenshot displays the ITGI website interface. At the top, there are navigation links for Media, Support, Info Request, Site Map, and Contact. Below this is a search bar and a 'My ISACA Login' section with fields for Username and Password. The main content area is divided into several columns. The left column features news articles such as 'Enterprise Value: Governance of IT Investments, Getting Started with Value Management' and 'IT Governance Roundtable Discussions'. The middle column contains a navigation menu with categories like Overview & History, What's New, Certification, Education & Conferences, Standards, Research, Publications, Chapters, Membership, Downloads, COBIT, and Val IT. The right column includes a 'COBIT Mapping: Mapping of ITIL V3 With COBIT 4.1' article and a 'Top Business/Technology Issues Survey Results' section. At the bottom of the page, there are logos for Solvay Business School, ITGI, and LOSEC, along with the text '© 2008 ITGI and Solvay Business School' and the URL 'Solvay.edu/ict - itai.org - isaca.org'.

## Publications

- Journal
- Books
- K-net

The screenshot shows the K-NET website. It features a search bar with the text 'Enter K-NET by selecting a category below, or entering a search word'. Below the search bar is a list of categories including:
 

- Certifications: IS Audit Controls & Security (CISMP)
- IS Audit Controls & Security - Specific Environments
- IS Audit Controls & Security - Tools
- IS Auditing
- IS Security: Internal/External/Internal Control & Security
- IS Security
- IS Security Management
- IS Control
- IS Governance & Business Management
- IS Governance
- IS Risk Management
- IS Professional Development

 At the bottom of the page, there are logos for Solvay Business School, ITGI, and LOSEC, and the text '© 2008 ITGI and Solvay Business School'.



The logos for Solvay Business School, ITGI, and LOSEC are displayed. Below the logos is the text '© 2008 ITGI and Solvay Business School'.

## Strategy

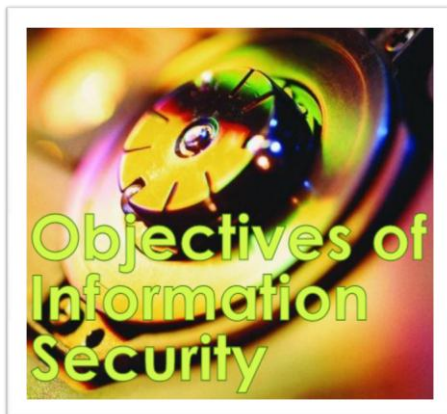


'It is no longer enough to communicate to the world of stakeholders why we exist and what constitutes success, we must also communicate how we are going to protect our existence\*

## Aspects



## Objective



- Strategic alignment
- Risk management
- Optimizing investments
- Resource management
- Performance measurement\*

## Major focus

Information is

- handled,
- processed,
- transported
- stored

Reach:

- integration,
- process assurance
- overall security

Universe of :

- risks,
- benefits
- processes



Members of executive management must have a clear understanding of what to expect from their information security programme



Solvay.edu/ict – itqi.org – isaca.org

## Benefits

	Protection for legal liability		Process improvement,
	Increased predictability		Rapid incident response
	Policy and compliance		Reduced losses
	Optimise resources		Improved reputation
	Risk management,		

Firms operating at best-in-class (security) levels are lowering financial losses to less than 1 percent of revenue, whereas other organisations are experiencing loss rates that exceed 5 percent\*.

\* Aberdeen Group, 'Best Practices in Security Governance', USA, 2005

## Responsibilities

		
Executive management	Chief Information Security Officer	Steering committee

Sixty percent of respondents report that their organizations employ a chief information security officer (CISO) or a chief security officer (CSO), up from 43 percent in 2006\*.

\* CIO, CSO and PricewaterhouseCoopers, 'The State of Information Security 2007, A Worldwide Study by CIO, CSO and PricewaterhouseCoopers', USA, 2007

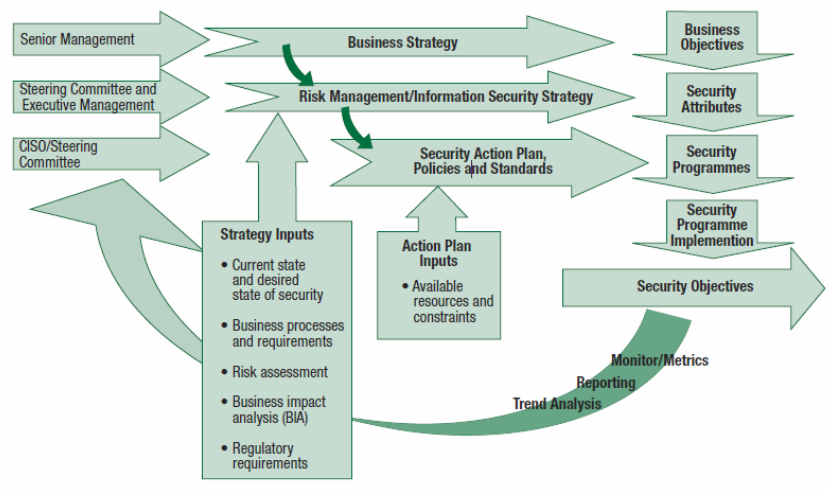
**Figure 2—Relationship of Information Security Governance Outcomes to Management Responsibilities**

Management Level	Strategic Alignment	Risk Management	Value Delivery	Performance Measurement	Resource Management	Process Assurance
Board of directors	Require demonstrable alignment.	<ul style="list-style-type: none"> <li>Establish risk tolerance.</li> <li>Oversee a policy of risk management.</li> <li>Ensure regulatory compliance.</li> </ul>	Require reporting of security activity costs.	Require reporting of security effectiveness.	Oversee a policy of knowledge management and resource utilisation.	Oversee a policy of assurance process integration.
Executive management	Institute processes to integrate security with business objectives.	<ul style="list-style-type: none"> <li>Ensure that roles and responsibilities include risk management in all activities.</li> <li>Monitor regulatory compliance.</li> </ul>	Require business case studies of security initiatives.	Require monitoring and metrics for security activities.	Ensure processes for knowledge capture and efficiency metrics.	Provide oversight of all assurance functions and plans for integration.
Steering committee	<ul style="list-style-type: none"> <li>Review and assist security strategy and integration efforts.</li> <li>Ensure that business owners support integration.</li> </ul>	Identify emerging risks, promote business unit security practices and identify compliance issues.	Review and advise on the adequacy of security initiatives to serve business functions.	Review and advise whether security initiatives meet business objectives.	Review processes for knowledge capture and dissemination.	<ul style="list-style-type: none"> <li>Identify critical business processes and assurance providers.</li> <li>Direct assurance integration efforts.</li> </ul>
CISO/information security management	Develop the security strategy, oversee the security programme and initiatives, and liaise with business process owners for ongoing alignment.	<ul style="list-style-type: none"> <li>Ensure that risk and business impact assessments are conducted.</li> <li>Develop risk mitigation strategies.</li> <li>Enforce policy and regulatory compliance.</li> </ul>	Monitor utilisation and effectiveness of security resources.	Develop and implement monitoring and metrics approaches, and direct and monitor security activities.	Develop methods for knowledge capture and dissemination, and develop metrics for effectiveness and efficiency.	<ul style="list-style-type: none"> <li>Liaise with other assurance providers.</li> <li>Ensure that gaps and overlaps are identified and addressed.</li> </ul>
Audit executives	Evaluate and report on degree of alignment.	Evaluate and report on corporate risk management practices and results.	Evaluate and report on efficiency.	Evaluate and report on degree of effectiveness of measures in place and metrics in use.	Evaluate and report on efficiency or resource management.	Evaluate and report on effectiveness of assurance processes performed by different areas of management.

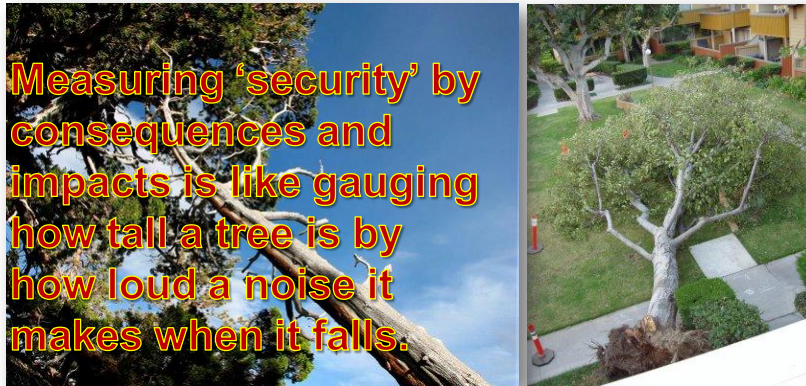


**Concept**

**Information Security Governance Conceptual Framework**



## Metrics



Solvay.edu/ict – itqi.org – isaca.org

## Governance Metrics

### Strategic Alignment

- The information security programme demonstrably enables specific business activities.
- The information security organisation is responsive to defined business requirements.
- The organisational and information security objectives are defined and clearly understood by all involved in information security and related assurance activities.
- The information security programme is mapped to the organisational objectives, and executive management has validated this mapping.
- There is an information security steering committee consisting of key executives with a charter to ensure ongoing alignment of information security activities and business strategy.



Solvay.edu/ict – itqi.org – isaca.org

## Governance Metrics

### Risk Management

- Organisational 'risk appetite' or risk tolerance is defined in terms relevant to the organisation.
- An overall information security strategy and programme for achieving acceptable levels of risk exist.
- Mitigation objectives for identified significant risks are defined.
- Processes for management or reduction of adverse impacts exist.
- Systematic, continuous risk management processes exist.
- Trends of periodic risk assessment indicate progress towards defined goals.
- Impacts are reviewed for trends.
- A tested business continuity plan (BCP)/disaster recovery plan (DRP) exists.
- Complete asset valuation and assignment of ownership exist.
- Recovery time objectives (RTOs) for all critical systems are developed.



Solvay.edu/ict – itqi.org – isaca.org

## Governance Metrics

### Value Delivery

- Information security activities are designed to achieve specific strategic objectives.
- The cost of security is proportional to the value of assets.
- Information security resources are allocated by degree of assessed risk and potential impact.
- Protection costs are aggregated as a function of revenues or asset valuation.
- Controls are designed well, based on defined control objectives, and are fully utilised.
- The number of controls to achieve acceptable risk and impact levels is adequate and appropriate.
- Control effectiveness is determined by periodic testing.
- are in place that require all controls to be re-evaluated periodically for cost, compliance and effectiveness.



Solvay.edu/ict – itqi.org – isaca.org

## Governance Metrics

# Resource Management

- Problem recurrence is infrequent.
- Knowledge capture and dissemination are effective.
- Processes are standardised.
- Roles and responsibilities for information security functions are clearly defined.
- Information security functions are incorporated into every project plan.
- Information assets and related threats are covered by security resources.
- The appropriate location in the organisational structure, level of authority and number of personnel for the information security function exist.



Solvay.edu/ict – itqi.org – isaca.org

## Governance Metrics

# Performance Measurement

- Time it takes to detect and report information security-related incidents
- Number and frequency of subsequently discovered unreported incidents
- Benchmarks with comparable organisations for costs and effectiveness
- Ability to determine the effectiveness and efficiency of controls
- Clear indication that information security objectives are being met
- Absence of unexpected information security events
- Knowledge of impending threats
- Effective means of determining organisational vulnerabilities
- Methods of tracking evolving risks
- Consistency of log review practices



Solvay.edu/ict – itqi.org – isaca.org

## Required management actions



Develop an Information Security strategy



Identify Critical Success Factors for Effective Information Security



Assess maturity of Information Security Governance



Solvay.edu/ict – itqi.org – isaca.org



Develop an Information Security strategy

### Resources

- Policies
- Standards
- Processes
- Methods
- Controls
- Technologies
- People
- Skills
- Training
- Education
- organisational support and assurance providers

### constraints

- Law
- Physical
- Ethics
- Culture
- Costs
- Personnel
- Resources
- Capabilities
- Time
- Risk tolerance



Solvay.edu/ict – itqi.org – isaca.org



Identify Critical Success Factors for Effective Information Security

58 | Information Security Governance  
Guidance for Information Security Managers

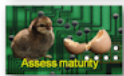
**Appendix A—Critical Success Factors for Effective Information Security**

To achieve successful information security, it is critical to ensure the following:

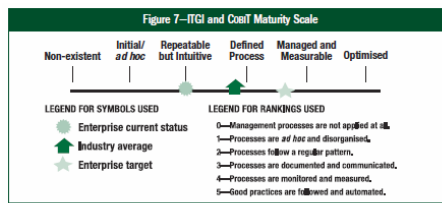
- There is awareness that a good information security programme takes time to evolve.
- The corporate information security function reports to senior management and is responsible for executing the information security programme.
- Management and staff have a common understanding of information security importance, requirements, vulnerabilities and threats, and understand and accept their own security responsibilities.
- Third-party evaluation of information security policy and architecture is conducted periodically.
- The information security function has the means and ability to administer security, especially to detect, record and analyse significance, and report and act on security incidents when they do occur, while minimising the probability of occurrence by applying intrusion testing and active monitoring.
- Clearly defined roles and responsibilities for risk management ownership and management accountability are in place.
- A policy is established to define risk limits and risk tolerance.
- Responsibilities and procedures for defining, agreeing on and funding risk management improvements exist.
- A reality check of the information security strategy is conducted by a third party to increase objectivity and is repeated at appropriate times.
- Critical infrastructure components are identified and continuously monitored.
- Service level agreements (SLAs) are used to raise awareness of and increase co-operation with suppliers relative to security and continuity needs.
- Policy enforcement is considered and decided on at the time of policy development.
- A confirmation process is in place to measure awareness, understanding and compliance with activities.



Solvay.edu/ict – itqi.org – isaca.org



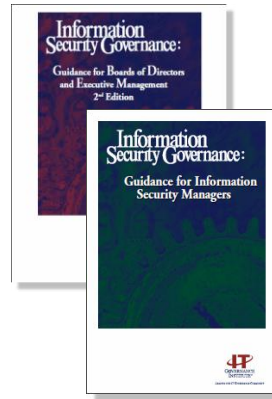
Assess maturity of Information Security Governance



<sup>29</sup> Adapted from IT Governance Institute, CoBIT 4.1, USA, 2007



Solvay.edu/ict – itqi.org – isaca.org



[Solvay.edu/ict](http://Solvay.edu/ict) – [itqi.org](http://itqi.org) – [isaca.org](http://isaca.org)

## Questions



[Solvay.edu/ict](http://Solvay.edu/ict) – [itqi.org](http://itqi.org) – [isaca.org](http://isaca.org)