



Quality and security in application development
Round Table Meeting/Discussion Group
Wednesday 23rd May 2007

Introduction to ISACA and ITGI
By Georges Ataya,
International Vice President, ISACA

The International Association



ISACA



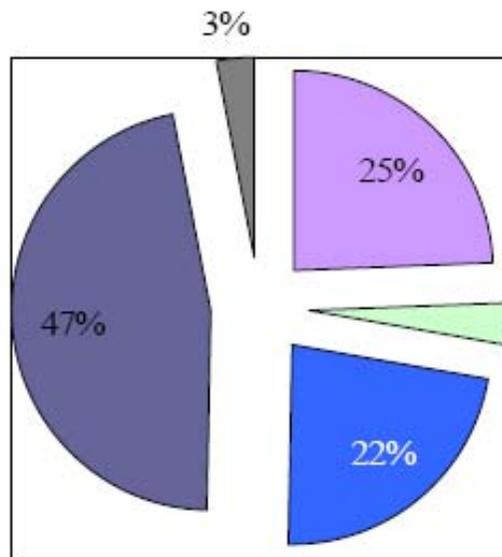
- More than 70,000 members in 170 chapters established in over 60 countries worldwide,
- Cover a variety of professional IT-related positions—to name just a few:
 - IS auditor,
 - IS security professional,
 - consultant,
 - educator,
 - regulator,
 - chief information officer
 - internal auditor
 - Etc..



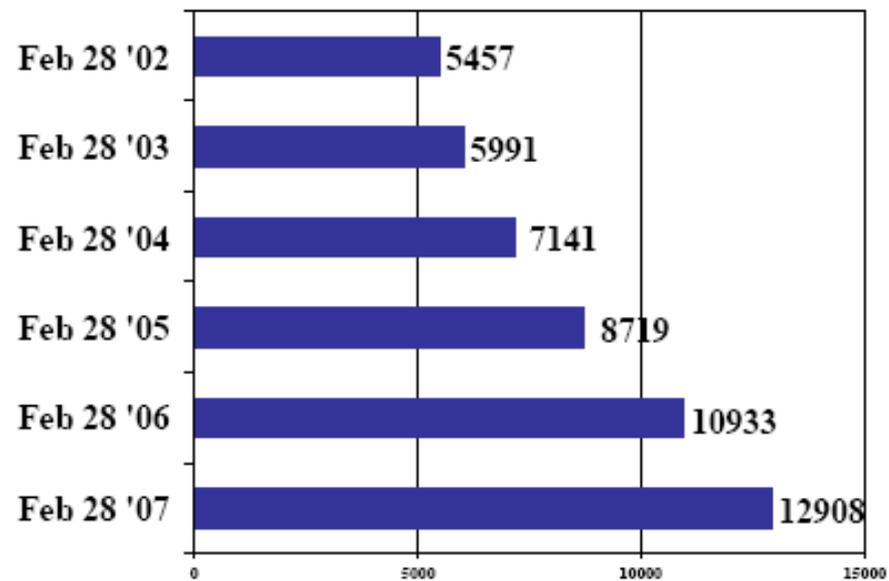
Membership



➤ Total ISACA membership worldwide: 77,276



➤ Membership growth in Europe



ISACA is also



- Member services including:
 - Education & Conferences
 - Professional Resources
 - K-NET
 - Standards
 - Bookstore
 - Discussion Forum
 - Glossary
- The IT Governance Institute (ITGI) actively promotes research and publications in three main domains
 - IT governance,
 - IT control and assurance, and
 - Security management.

Research and publications



New releases:

- *IT Control Objectives for Sarbanes-Oxley, 2nd Edition*
- *COBIT Mapping: Mapping PRINCE2[®] With COBIT 4.0*
- *COBIT Mapping: Mapping ISO/IEC 17799:2005 With COBIT 4.0*
- *COBIT Mapping: Mapping ITIL With COBIT 4.0*
- *COBIT Mapping: Mapping CMMI[®] for Development V1.2 With COBIT 4.0*

Projects scheduled for availability in the first quarter:

- *COBIT Mapping: Mapping TOGAF[®] With COBIT 4.0*

Projects scheduled for availability in the second quarter:

- *COBIT 4.1*
- *IT Governance Implementation Guide Using: COBIT and Val IT, 2nd Edition*
- *COBIT Control Practices, 2nd Edition*
- *IT Assurance Guide: Using COBIT*

Research and publications



Projects in development:

- *COBIT Mapping: Mapping COSO ERM With COBIT 4.1*
- *COBIT Mapping: Mapping NIST 800-53 With COBIT 4.1*
- *COBIT Security Baseline, 2nd Edition*
- *COBIT in Academia, 2nd Edition*
- *Information Security Governance: Implementation Guide*
- *IT Control Objectives for Basel II*

The IT Governance Institute



The IT Governance Institute



A screenshot of the ITGI website as it appeared in a Mozilla Firefox browser window on Saturday, 19 May 2007. The browser's address bar shows 'http://www.itgi.org/'. The website header includes the ITGI logo and the tagline 'Leading the IT Governance Community'. A navigation menu contains links for 'About ITGI', 'About IT Governance', 'Resource Center', 'Case Studies / Best Practices', and a search bar. The main content area is divided into several sections: a featured article about 'IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance Exposure Draft' with a photo of a man at a computer; a section titled 'ITGI Releases COBIT 4.1!' with a sub-section 'COBIT 4.0 in German'; a 'Second Edition of Sarbanes-Oxley Publication Available' section; and a 'COBIT In Use' section. A sidebar on the right contains links for 'COBIT Focus Newsletter Archive', 'COBIT Focus - Volume 2, Italian Introduction to COBIT', and 'MEET OUR SUPPORTERS'. The footer of the browser window shows 'Done' and navigation icons.

Publications



- Books
- Journal
- K-net

Home -- Members & Leaders -- Professional Resources -- K-NET

K-NET contains over 6,000 peer-reviewed web site resources pertaining to knowledge covering IT Governance, Assurance, Security and Control. Full access to K-NET is reserved for association members. In addition, a personalized tracking feature, that notifies users on a weekly basis of new references within their areas of focus, is also reserved for members (see 'back-updates' link throughout K-NET). Reference items are organized into logical categories of interest and concern.

Share your web-based knowledge resources with fellow members -- forward its address (URL) to knet@isaca.org

Enter K-NET by selecting a category below, or entering a search word

Search for

[Keyword Index](#)

[Certifications: IS Audit \(CISAB\) & Security \(CISM™\)](#)
[IS Audit, Control & Security - Specific Environments](#)
[IS Audit, Control & Security - Tools](#)
[IS Auditing](#)
[Net Centric \(Intranet/Extranet/Internet\) Control & Security](#)
[IS Security](#)
[IS Security Management](#)
[IS Control](#)
[IT Governance & Business Management](#)
[eBusiness](#)
[Telecommunications](#)
[Project Management](#)
[Professional Development](#)



More info www.isaca.org ¹⁰

The Belux Chapter



ISACA Belux Chapter



Agenda
Overview of all activities organised or announced by the Chapter

Date	Topic	Speakers
18th May	IT Best Practices Assessment	Peter LEESON, Lead Appraising Visiting Assistant Software Engineer Laurent JAKET, Senior Consultant
21-25 May	CISA Luxembourg Training 2007	Mark Geisler, C Sylvain Brenna
4th June	IT Security Forum	Harc Vael, KPMG
5th September	IT Security Forum	Harc Vael, KPMG
9th December	IT Security Forum	Harc Vael, KPMG

Past ISACA Meetings

Presentations from the following round tables are available (on the Belux Forum):

Date	Topic	Presented by
21st April 2007	Identity Management	Christophe Sténuit, Ogeris
1st March 2007	Explanation of ValIT The Governance of IT investment	Erk Guldentops - ISACA Steven De Haes - UAMS Dirk Steuperaert - PWC
Saturday 20 January 2007	Governance Round Table and New year Drink <ul style="list-style-type: none"> How to audit Corporate Governance ? IT Governance at NBB CISM and CISA certification and training programs 	Patrick Soenen, Qualified Audit Partners (QAP) Philip De Picker, Audit BNB Marc Vael, KPMG
Saturday 2 December 2006	How to sell security	Jean-Luc Allard Georges Ataya (Professor Solvay Business School)
Tuesday 28 November 2006	IT Governance at Belgacom	Sylvain Brenna (Talinus Luxembourg) Erk van den Akker (Head of IT Audit, Belgacom)
Thursday 19 October 2006	ERP auditing	K. Claessens (Deloitte), O. Viseur (Deloitte), E. Moreno-Sereno (Deloitte), K. Magnus (Deloitte)
Thursday 21 September 2006	How to create a new IT audit function	Facilitated by Monique Garsoux (Dexia, vp IT Belux)
Thursday 22 June 2006	Cobit Maturity Audit in Software Development	Peter Van Mel (Manager of Business Development HeliosIT)
Thursday 27 April 2006	IT Governance Survey ISACA Body of Knowledge General Meeting /Board elections	Dirk Steuperaert (Director PWC) Georges Ataya (President ISACA)
Wednesday 14 March 2006	ITIL and IT Governance BCIE Update	Marnik Demets (Managing Director of MSD P) Carl Wethmar (Operating Officer of BCIE)
Wednesday 1st Feb 2006	Enterprise value: Governance of IT investments	John Torp (Author of "Information Paradox") Georges Ataya (President ISACA)
Thursday 15th Dec 2005	Presentation on Cobit 4.0	Georges Ataya - President ISACA Greet Volders - Vice-President ISACA
Thursday 22nd	SAS 70 Certification	Georges Ataya - President ISACA Jean-Paul Declerck - Security Officer at Ubiz

ISACA Belgium,
Rue du choux 47 3^{ème} étage
1000 Bruxelles, Belgique
Tel : 02/219.82.82

Additional activities in Belgium



BCIE Belgische Kamer van experten in Informatica Chambre belge des Experts en informatique Belgian Chamber for IT Experts **ISACA** Serving IT Governance Professionals Belux Chapter

About BCIE

The Belgium division of the international organization for computer auditors (ISACA) launched the Belgium Chamber of IT Expert Witnesses (BCIE) in 2005 to service and support IT experts. The objective of BCIE is the support of the proper administration of justice and the early resolution of disputes through fair and unbiased expert evidence.

In an IT related dispute with a technical character, the services of an IT expert is called upon to provide the court with an expert opinion over the causes and consequence of the facts, based on their expertise in a given field. It is not always evident for the court what profile of expert is required and who has the correct level of expertise to provide such opinion, especially in the field of IT.

Currently the judiciary uses dubious lists for which no acceptance criteria is applicable. The legislator took cognizance of this problem and is currently working on changing the legislation related to expert opinions.

In the future, to be accepted as an expert, the candidate will have to meet certain requirements. ISACA wants to play a leading role in this by providing certified members as information technology experts. Over and above the certification, a few additional requirements like industry- and expertise experience will have to be met in order to be presented as an IT expert.

BCIE strives to act as a voice for the IT expert witness community, supporting experts from all IT disciplines and lawyers who use the services of experts. Its functions are to encourage, train and educate experts and to improve and maintain their standards and status. BCIE actively works with associated professional bodies to achieve this. BCIE is independent of outside commercial interests and is democratic, transparent and fully accountable to its members. The objective of BCIE is the support of the proper administration of justice and the early resolution of disputes through fair and unbiased expert evidence. To achieve this objective, BCIE:

- Acts as a voice for IT expert witnesses.
- Provides a Code of Conduct for IT expert witnesses
- Provides support to experts of all IT disciplines requiring skills and judgment.
- Encourages lawyers to make use of BCIE experts for IT related disputes.
- Engages in the training of IT experts to maintain and enhance standards and their status.
- Works actively with other allied professional bodies and associations.
- Makes representations to Government and to professional bodies and associations wherever appropriate.

(ISACA) Information Systems Audit and Control Association was founded in 1967. Today, ISACA's membership—more than 47,000 strong worldwide—is characterized by its diversity. Members live and work in more than 140 countries and cover a variety of professional IT-related positions—to name just a few, IS auditor, consultant, educator, IS security professional, regulator, chief information officer and internal auditor. Some are new to the field, others are at middle management levels and still others are in the most senior ranks. They work in nearly all industry categories, including financial and banking, public accounting, government and the public sector, utilities and manufacturing. This diversity enables members to learn from each other, and exchange widely divergent viewpoints on a variety of professional topics. It has long been considered one of ISACA's strengths. Another of ISACA's strengths is its chapter network. ISACA has chapters in more than 170 chapters established in over 60 countries worldwide, and those chapters provide members education, resource sharing, advocacy, professional networking and a host of other benefits on a local level.

The IT Experts of ISACA was grouped to form the Belgian Chamber of IT Expert Witnesses. (BCIE)
ISACA and therefore also BCIE is a member of FEBEX. (Federatie van Belgische Expertverenigingen)
BCIE
(ISACA Administrative Office)
- Koolstraat 47 3rd floor 1000 Brussels -
Phone : 02/219 82 82

Partnership with Belgian universities



Isaca Belux and Solvay Business School are delighted to strengthen their cooperation to offer selected education sessions for ISACA Belux members to be chosen from the Executive Master in ICT Audit & Security program :

- A1. IT Systems management (30 hours)
- A2. Internal and IT audit (30 h)
- A3. Review of the IT process (Practical use of COBIT) (30 h)
- A4. IT Legislation and IT forensics (30 h)
- A5. Application Review and Data Analysis (Workshop) (30 h)
- A6. Audit of New Technologies (Workshop - 15 h) (A3 is a prerequisite for A6) / A7. Service Management - ITIL (15 h)
- B6 Soft skills for IT Professionals (15 h)
- C1: Strategy management (16 h)
- C2: Leadership skills (16 h)

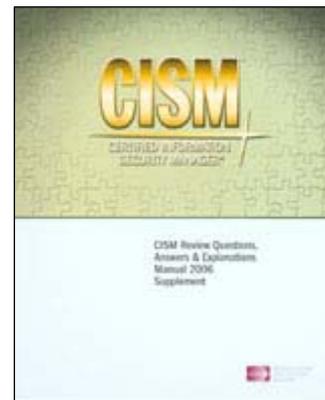
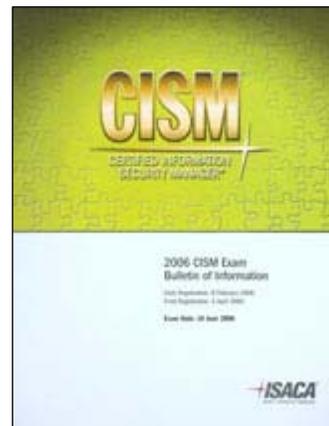
Certification



CISM



- The Certified Information Security Manager® (CISM®) certification program is developed specifically for experienced information security managers and those who have information security management responsibilities.
- Requirements:
 - Successfully pass the CISM exam.
 - Adhere to ISACA's Code of Professional Ethics.
 - Agree to comply with the Continuing Education Policy.
 - Work experience in the field of information security.



More info www.isaca.org 16



CISA Job Practice Areas

- IS Audit Process – 10%
- IT Governance – 15%
- Systems and Infrastructure Lifecycle Management – 16%
- IT Service Delivery and Support – 14%
- Protection of Information Assets – 31%
- Business Continuity and Disaster Recovery – 14%

Exam dates:

- Saturday 9 June 2007
- Saturday 8 December 2007



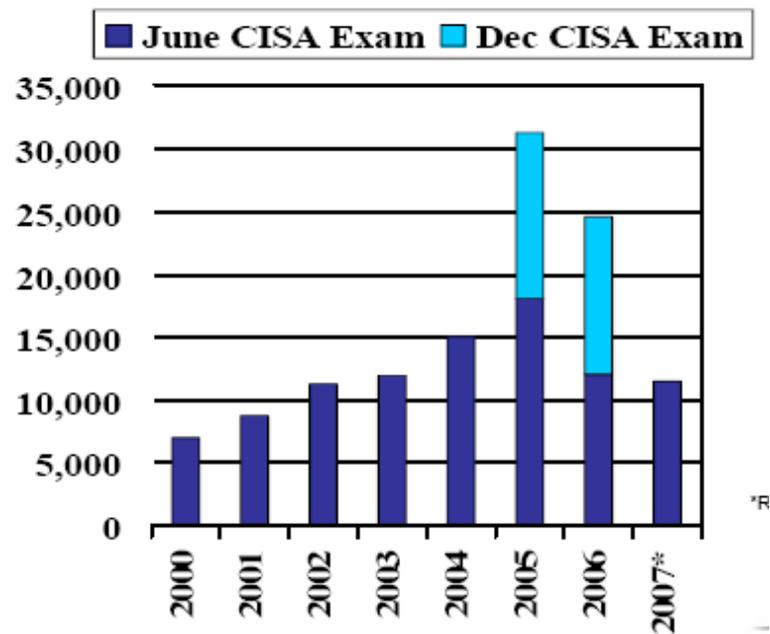
CISM Job Practice Areas

- Information Security Governance (23%)
- Information Risk Management (22%)
- Information Security Program Development (17%)
- Information Security Program Management (24%)
- Incident Management & Response (14%)

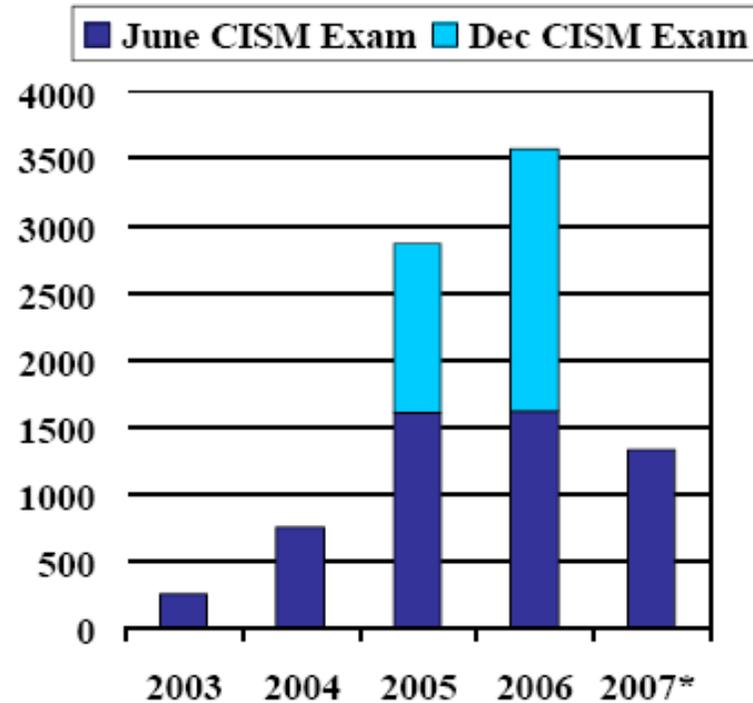
Exam dates:

- Saturday 9 June 2007
- Saturday 8 December 2007

Exam passers



© 2007, Information Systems Audit and Control Association. All rights reserved.



© 2007, Information Systems Audit and Control Association. All rights reserved.

IT Governance

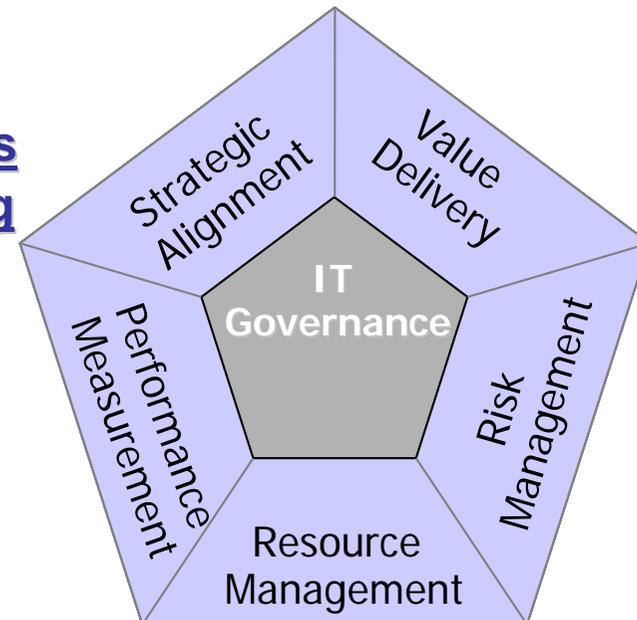
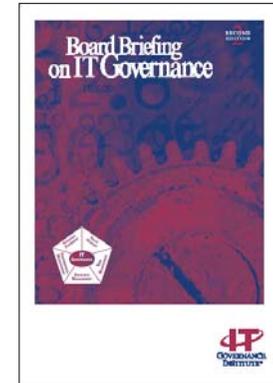


What is IT Governance?



Leadership, process and structure to ensure the enterprise's IT enables and supports the enterprise's strategies and objectives by defining:

1. what key decisions need to be made;
2. who is responsible for making them;
3. how they are made; and
4. the process and supporting structures for making them, including monitoring adherence to the process and the effectiveness of decisions



Focusing on five areas



What is IT Governance?



DOMAINS

1. Strategic Alignment

Aligning with the business and providing collaborative solutions

2. Value Delivery

Executing the value proposition throughout the delivery cycle focussing on IT expenses and proof of value

3. Resource Management

Optimising the development and use of available resources: knowledge, infrastructure and partners

4. Risk Management

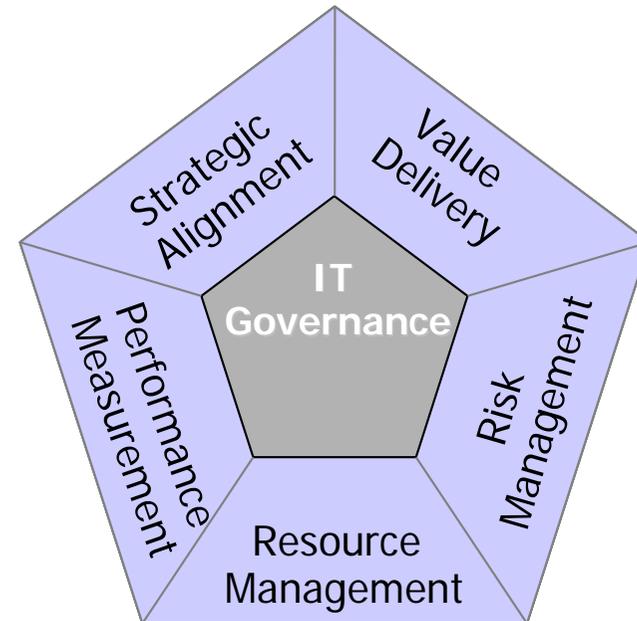
Safeguarding assets, disaster recovery and compliance

5. Performance Measurement

Monitoring results for corrective action through scorecards



ITGI Survey of 700 CEO/CIO's worldwide by PwC – Oct 2005



The Four “Ares”- continually asking:

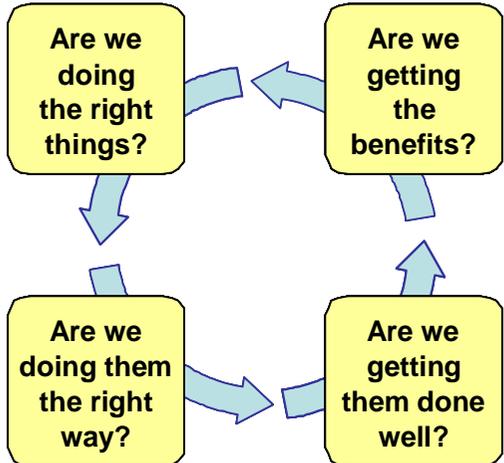


The *strategic* question. Is the investment:

- In line with our vision?
- Consistent with our business principles?
- Contributing to our strategic objectives?
- Providing optimal value, at affordable cost, at an acceptable level of risk?

- In the *value* question. Do we have:
- A clear and shared understanding of the expected benefits?
- Clear accountability for realising the benefits?
- Relevant metrics?
- An effective benefits realisation process?

Some fundamental questions



about the value enabled by IT

The *architecture* question. Is the investment:

- In line with our architecture?
- Consistent with our architectural principles?
- Contributing to the population of our architecture?
- In line with other initiatives?

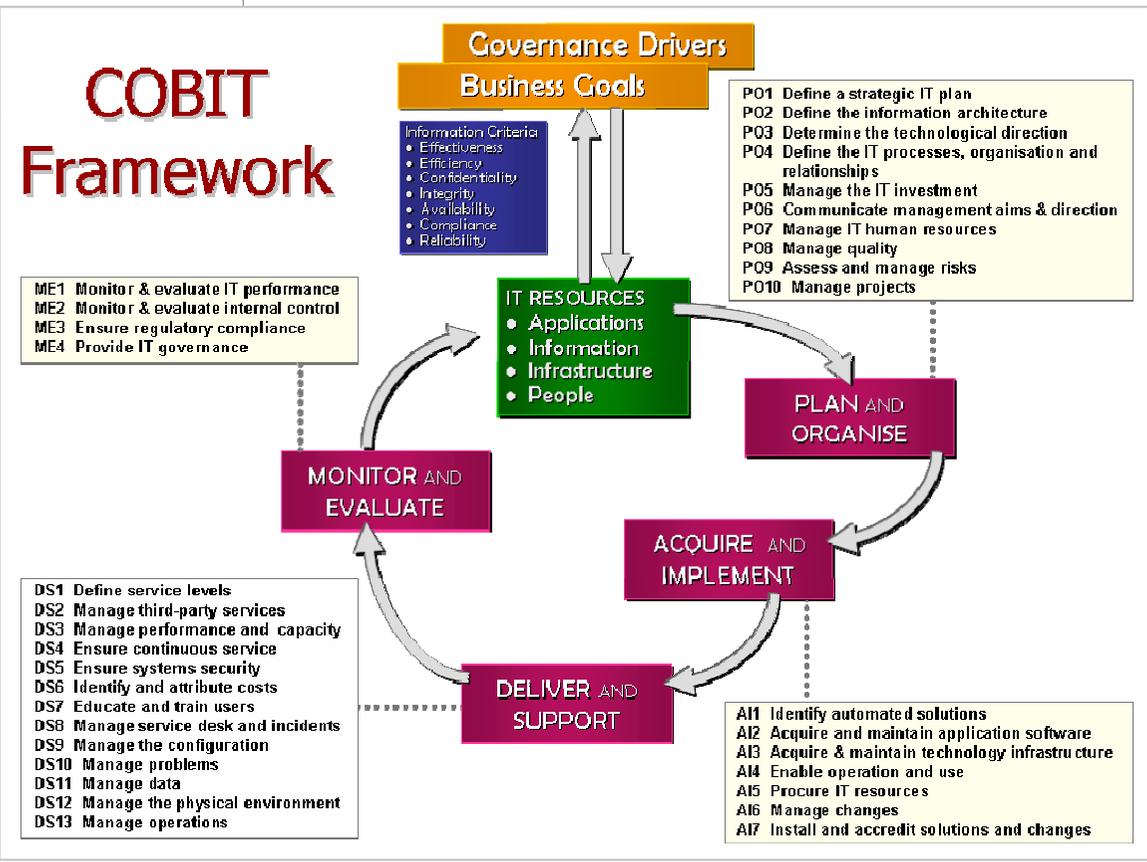
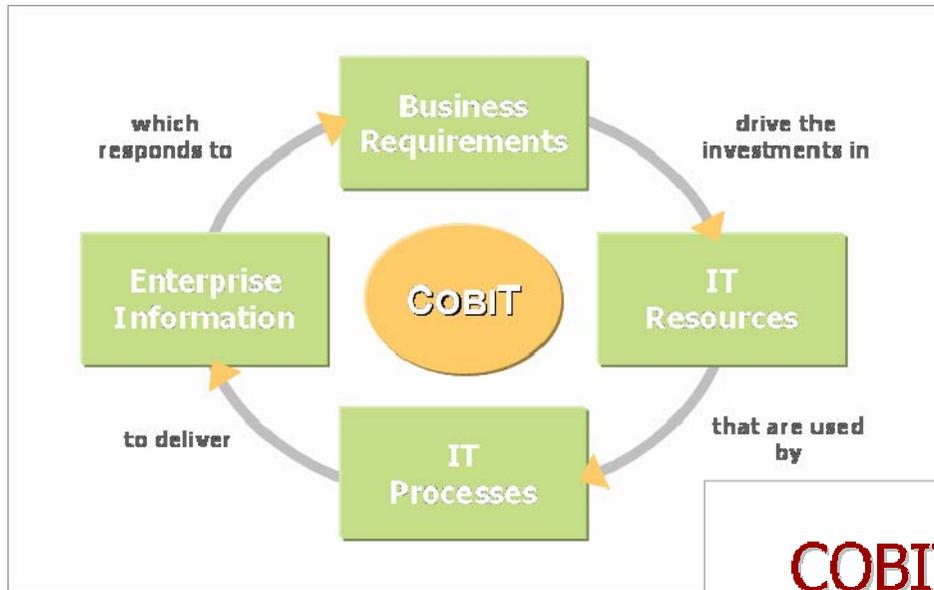
The *delivery* question. Do we have:

- Effective and disciplined delivery and change management processes?
- Competent and available technical and business resources to deliver:
 - the required capabilities; and
 - the organisational changes required to leverage the capabilities?

CobiT



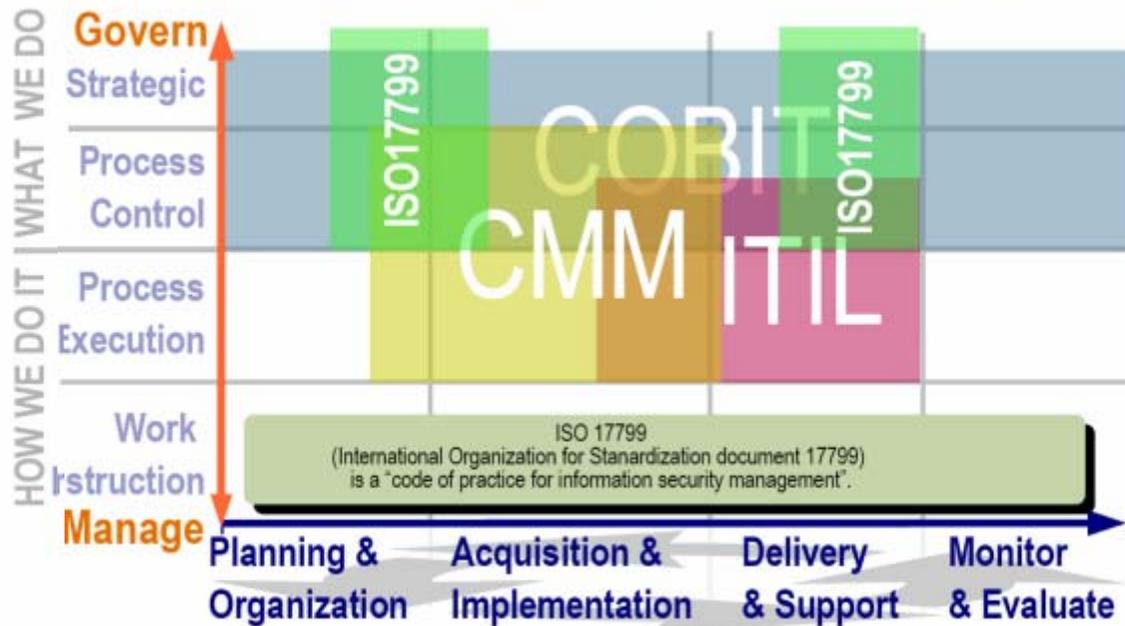
The Basic COBIT Principle



The use of management frameworks



Positioning of Industry Frameworks

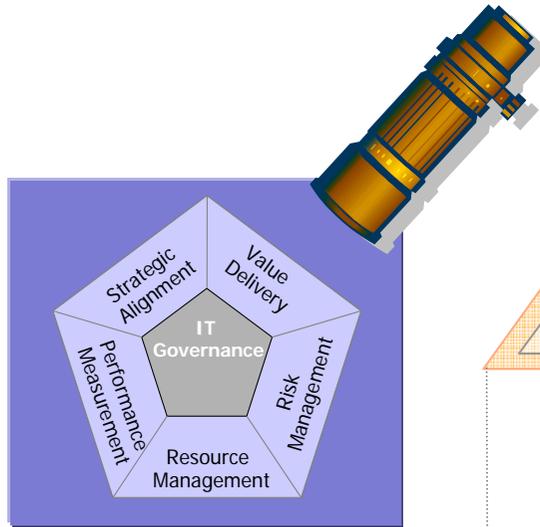


Val-IT



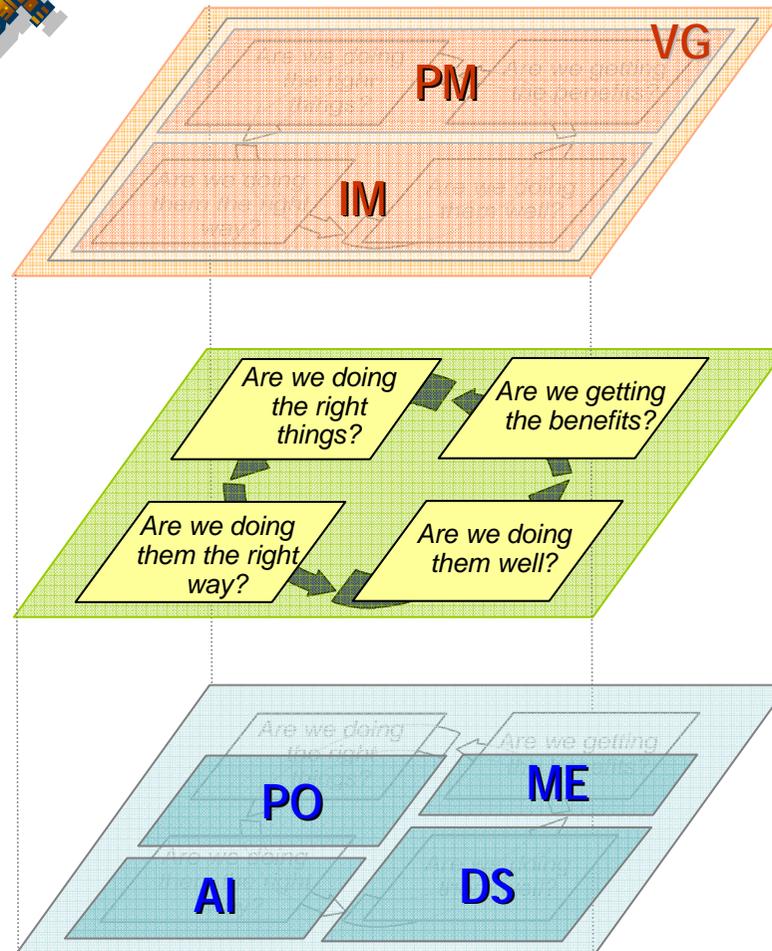
Va/IT Initiative

...a value lens into COBIT



COBIT

Governance & management of a portfolio of technology projects, services, systems & supporting infrastructure

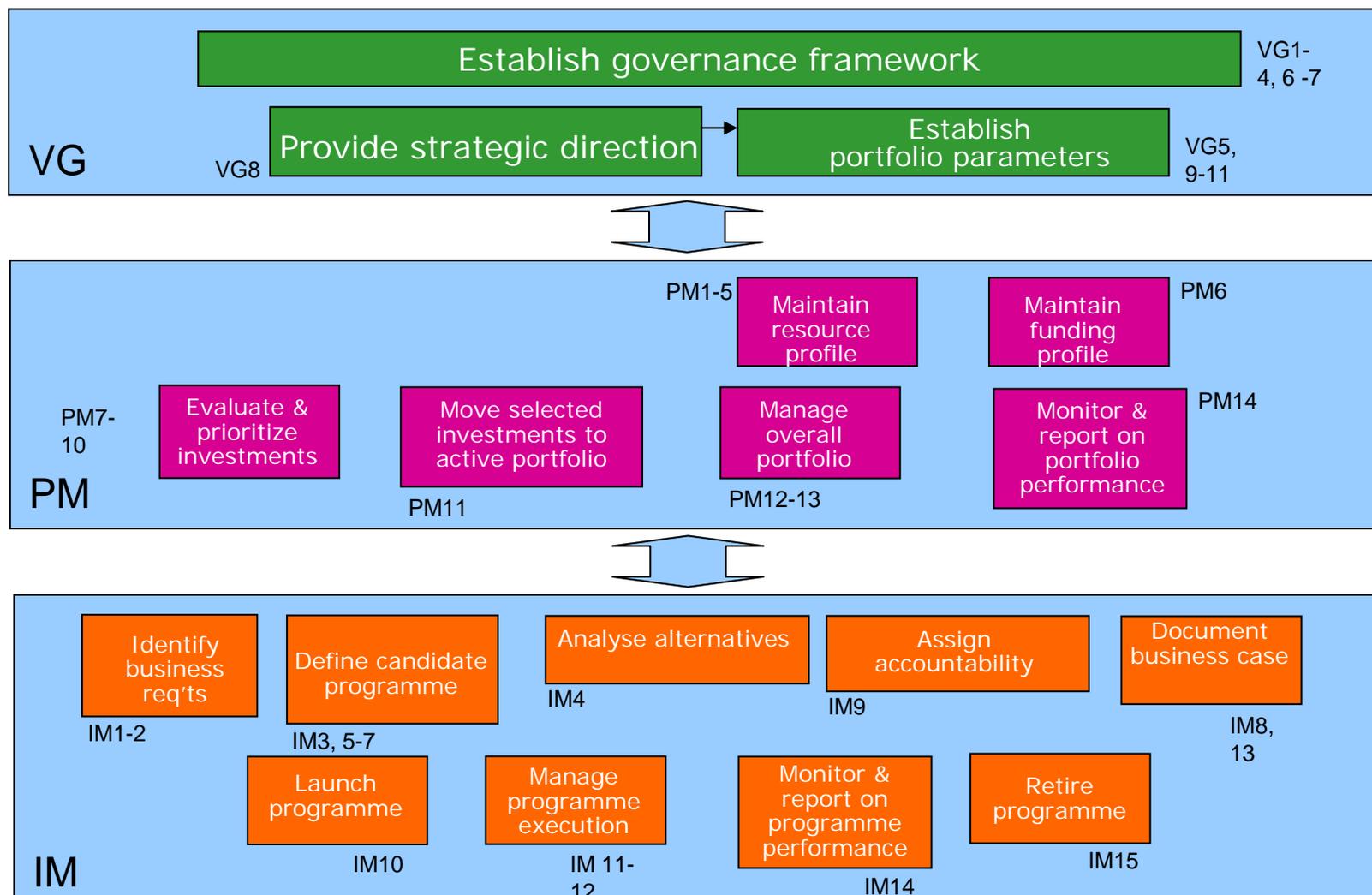


Va/IT

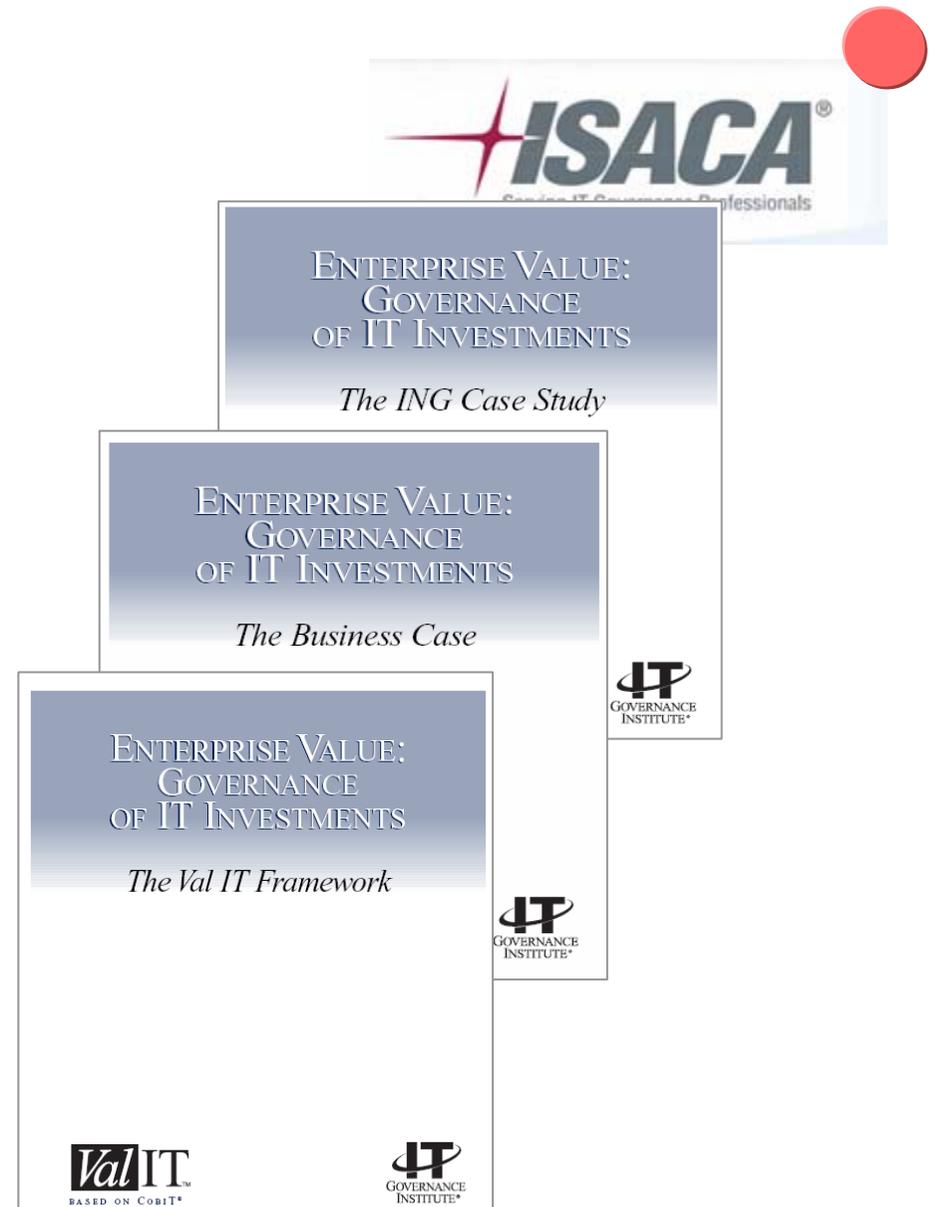
Governance & management of a portfolio of business change programmes

Val IT

Relationship between Processes & Practices



Val IT Initiative- Deliverables



Available for free download from:
www.isaca.org or www.itgi.org 30

IT Audit



Background of IT Auditing



- Started in assisting financial auditors in accessing the data
 - Auditing data
 - Audit general controls
 - Auditing applications controls
- Today additional requirements for IT Audit
 - Audit the complete IT Process
 - Audit specific environments
 - Security audits
 - Focus on Risk and on Internal Controls

Audit Mission and Planning

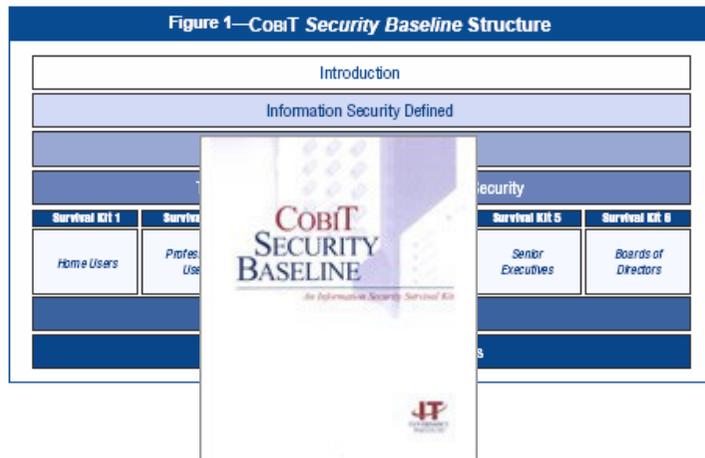
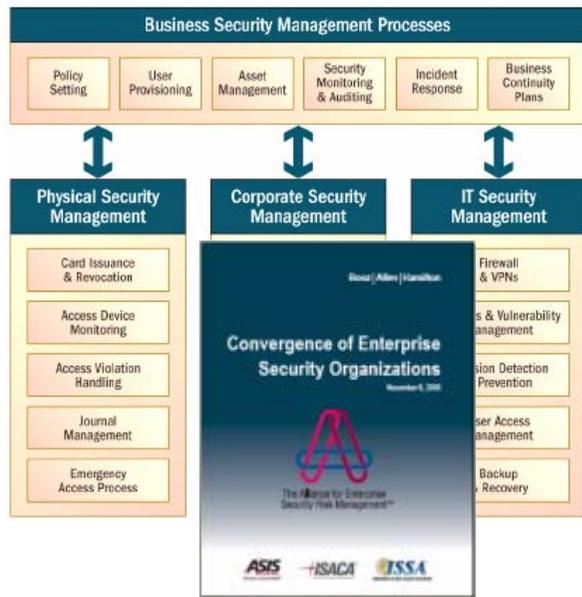


To perform an audit planning, the IS auditor should

- 1. Gain an understanding of the business' mission, business' objectives, business' processes, information and processing requirements such as availability, integrity and security and information architecture requirements. In general terms, processes and technology.**
- 2. Perform risk analysis.**
- 3. Conduct an internal control review.**
- 4. Set the audit scope and audit objective(s).**
- 5. Develop the audit approach or audit strategy.**
- 6. Assign resources to audit and address engagement logistics.**

Information Security





Security



- Research and publications
 - Security Governance
 - Security technology
- Security Knowledge Centre
 - K-NET contains over 6,000 peer-reviewed web site resources
 - Pertaining to knowledge covering IT Governance, Assurance, Security and Control.
- Glossary
- Security Management Committee
 - Establishes and oversees the execution of an ISACA strategy for serving the information security management profession.
- Discussion Forum ([Information Security Manager](#))
- Career, Forum, Conferences, etc...

More info www.isaca.org

▶ COBIT Security Baseline (revised) (PDF, 395K) Dec 2004

▶ Information Security Governance: Guidance for Boards of Directors 2nd Edition (PDF, 500K) Mar 2006

▶ Project Management: Skills & Knowledge Requirements in an Environment (PDF, 865K)

▶ [Certifications: IS Audit \(CISA®\) & Security \(CISM™\)](#) [IS Control](#)

▶ [IS Audit, Control & Security - Specific Environments](#) [IT Governance & Business Management](#)

▶ [IS Audit, Control & Security - Tools](#) [eBusiness](#)

▶ [IS Auditing](#) [Telecommunications](#)

▶ [Net Centric \(Intranet/Extranet/Internet\) Control & Security](#) [Project Management](#)

▶ [IS Security](#) [Professional Development](#)

▶ [IS Security Management](#)

IS Security

Denotes access limited to ISACA members.

[Education Opportunities](#)
[Books & CD-ROMs](#)
[Articles & Papers](#)
[Web Resources](#)

Note: All links will open in a new browser window.

[\[General Subject References\]](#)
 [Laptops](#)

Glossary

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#)

[View entire glossary in print](#)

Term	Definition
Abend	
Access control	
Access control table	
Access method	
Access path	
Access rights	
Accountability	
ACK (acknowledgement)	
Active recovery site (mirrored)	
Active response	
Address	
Address space	
Addressing	

Further references



- www.ITGI.org
- www.ISACA.org
- www.ISACA.be

The collage consists of three overlapping screenshots of the ISACA website:

- Top Screenshot:** Shows a browser window with the address bar at <http://www.itgi.org/>. The main header features the IT Governance Institute logo and the tagline "Linking Business Objectives and Information Technology". A navigation bar includes "About ITGI", "About IT Governance", "Resource Center", "Case Studies / Best Practices", and a search bar. A featured article titled "IT Value: Delivering on the Promise" is visible, along with a COBIT logo and a sidebar with "What's new with COBIT?".
- Middle Screenshot:** Shows the ISACA website's main content area. A navigation menu on the left lists categories like "Systems & Policy", "What's New", "Certification", "Education & Conferences", "Standards", "Research", "Publications", "Chapters", "Membership", "Solutions", "Downloads", and "Career Centre". The main content area features a news article titled "New CISACISM Exams Now Held Twice a Year!" and another article about "Information Security Harmonization: Clarification of Global Guidance".
- Bottom Screenshot:** Shows the "Member Information" section. It includes "Upcoming Events" with a "Round Table" on the "Convergence of ISACA/ITGI/ISSAI", a "Security Forum" on "Security in the Cloud", and a "Education Event" on "The Business of Enterprise Business and IT". There is also an "ISACA Announcements" section and an "Advertising Section" with logos for uams, Deloitte, and MIS.

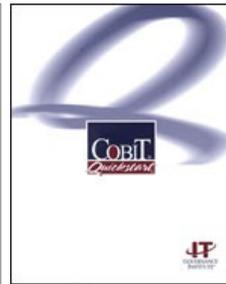
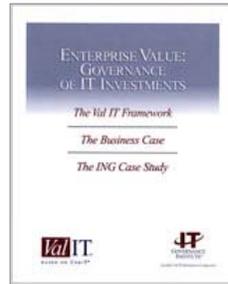
Jean-Luc Allard



- Chairman of the Education Committee at ISACA Belux Chapter
- Managed telecommunication and Information Systems at the Belgian Air Force
- Active involvement with the Belgian Shadow Committee for developing standards such as ISO/IEC 13335, 27005, 2700x
- Member of the Belgian Chamber of IT Expert Witnesses (BCIE) for risk management and information security management
- Wide experience in Security Governance as a delegate of Belgium in NATO and WEU workgroups dealing with information security management
- Past Senior Security Consultant at Cybertrust (Ubizen) where he was involved with the development of a process and method for information security risk management (based on EBIOS) and application with a dozen of clients in countries such as Belgium, United States, Saudi Arabia, The Grand Duchy of Luxembourg, the Netherlands. Activity domains included Banking, Finance, Stock Exchange, Media, Telecommunications, Industry, Sciences, and Energy
- Industrial Engineer in Electronics, ETSE Anderlecht (Belgium); Capitaine-Commandant d'Aviation E.R., Technical Officer (Telecommunications) by the Belgian Air Force; CISM Certified Information Security Manager (ISACA); CISA Certified Information System Auditor (ISACA).



- Professor and Academic Director at Solvay Business School (www.solvay.edu/it)
 - Postgraduate in ICT Audit & Security
 - Executive Master in IT Governance
- International Vice President of the IT Governance Institute (www.ITGI.org)
- Managing Partner of ICT Control SA-NV (www.ictcontrol.eu)
- Member of the Belgian association for Board Directors and the International commission of the Institute for French Board Directors.
- Participated in the development of various publications.
- Georges@ataya.net – www.ataya.info
- +32 475 705709





Questions ?