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

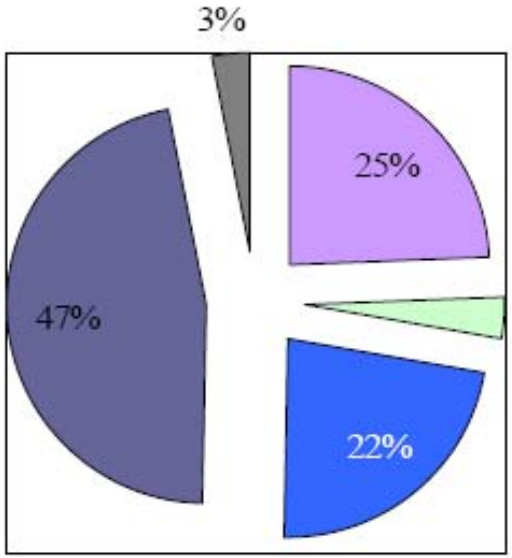
ISACA

- 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..

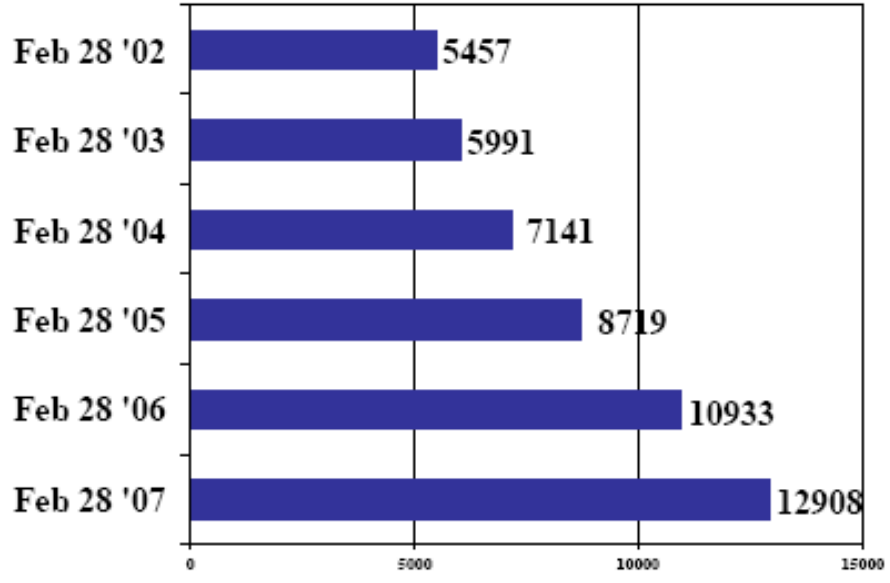
More info www.isaca.org

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.

More info www.isaca.org

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*

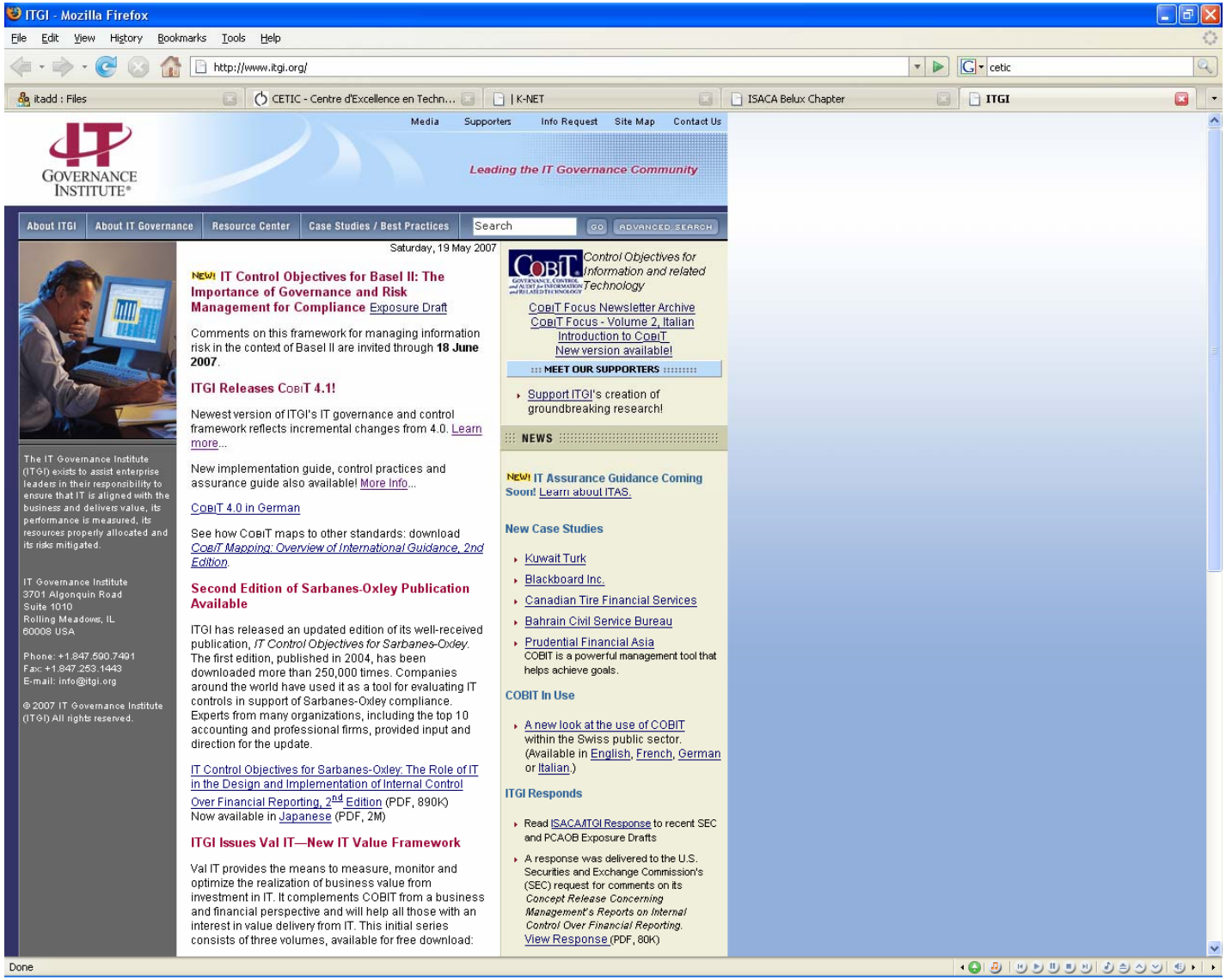
Research and publications

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



Publications

- Books
- Journal
- K-net

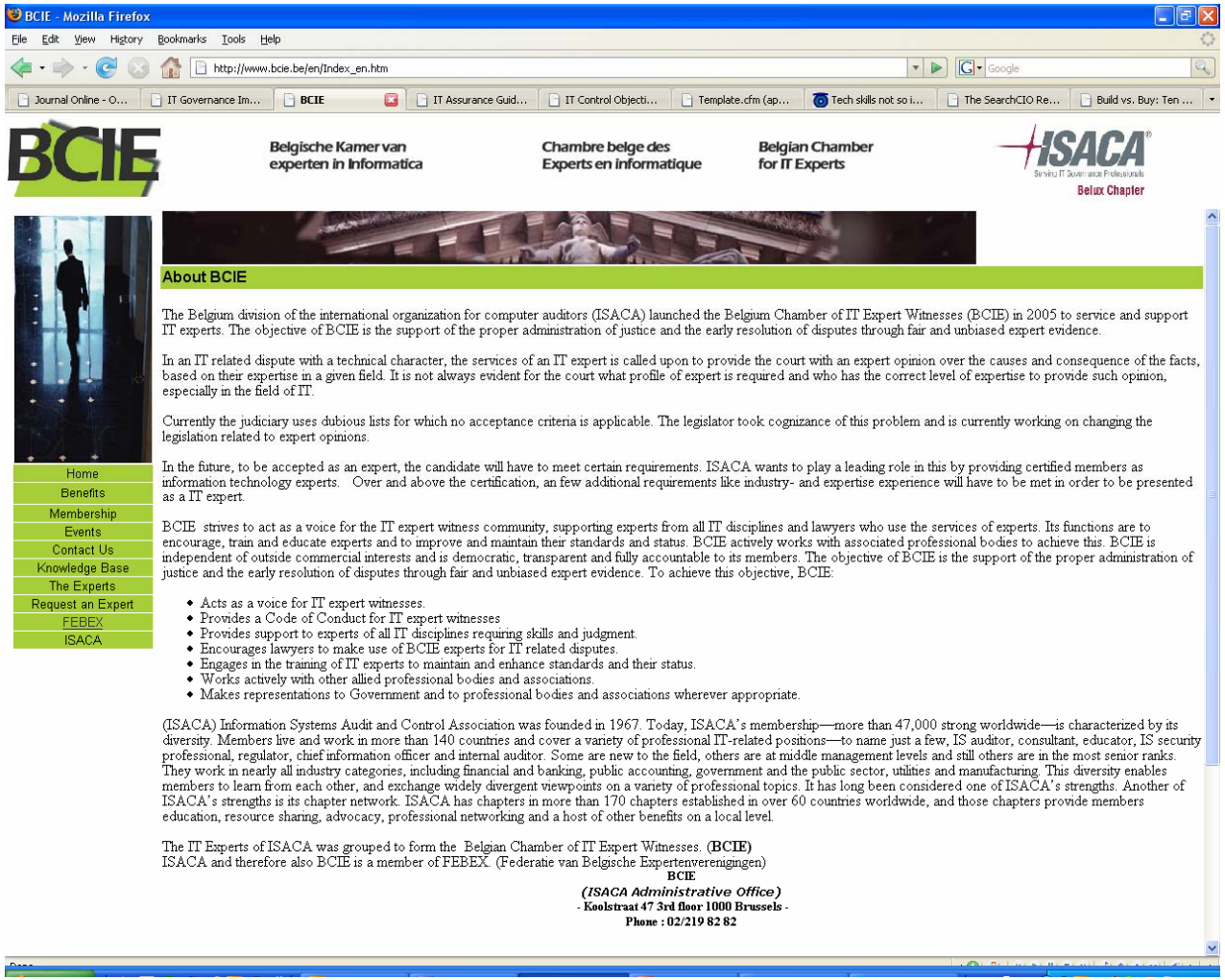
More info www.isaca.org

The Belux Chapter

ISACA Belux Chapter

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

Additional activities in Belgium



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

CISA®
CERTIFIED INFORMATION SYSTEMS AUDITOR

ISACA®
Serving IT Governance Professionals

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

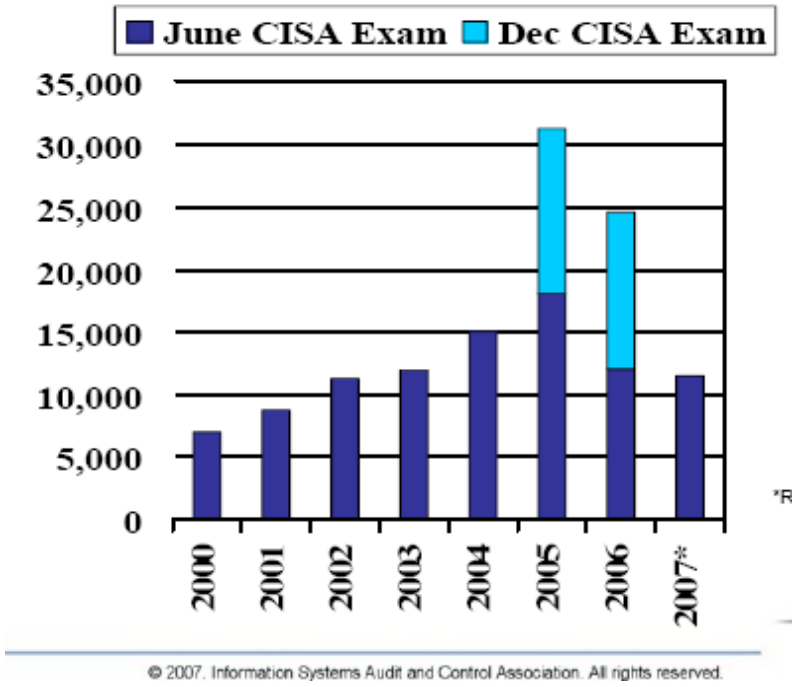
CISM Job Practice Areas

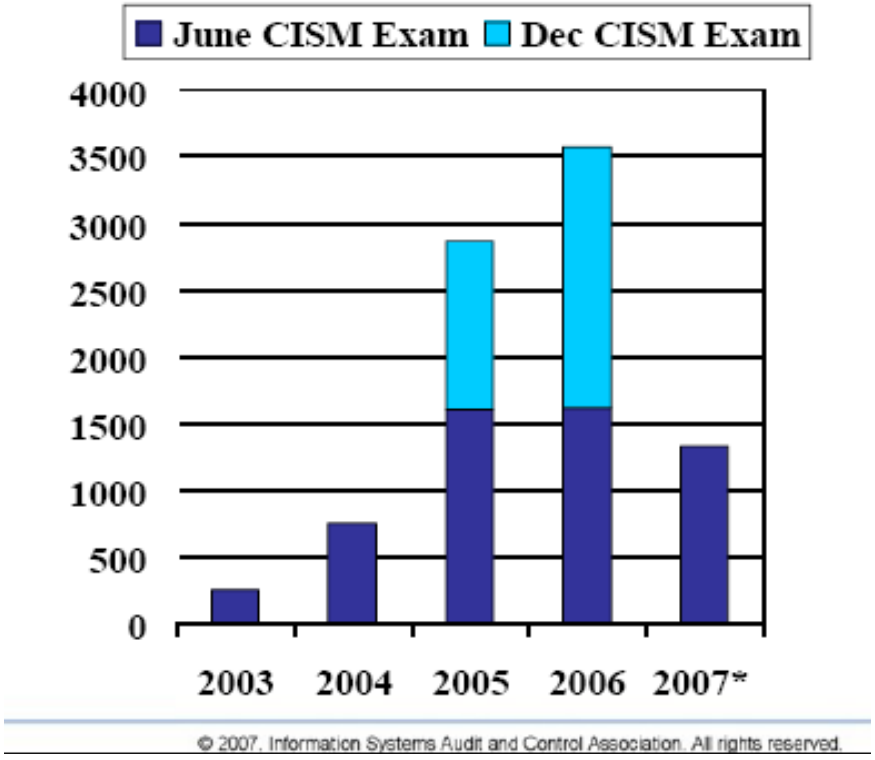
- Information Security Governance (23%)
- Information Risk Management (22%)
- Information Security Program Development (17%)
- Information Security Program Management (24%)
- Incident Management & Response (14%)

Exam dates:

- Saturday 9 June 2007
- Saturday 8 December 2007

Exam passers





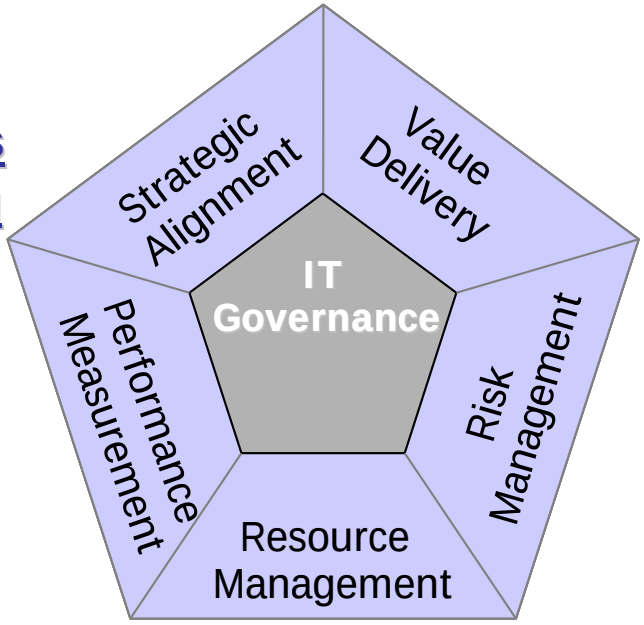
IT Governance

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

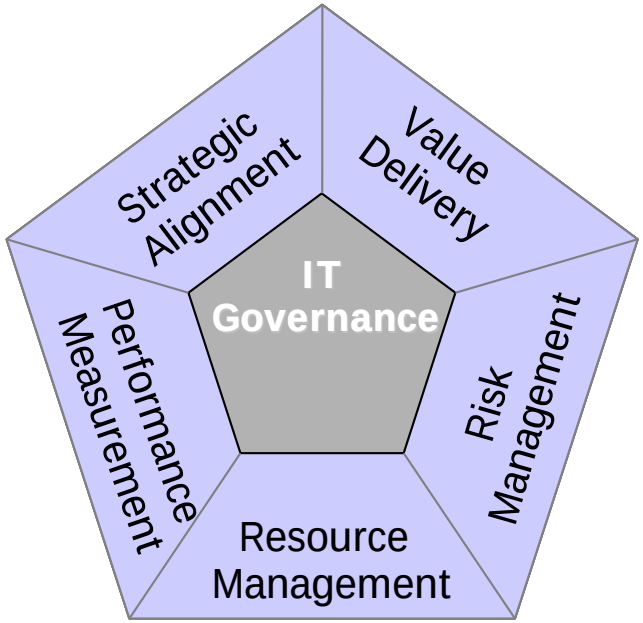
2. Value Delivery
Executing the value proposition throughout the delivery cycle focussing on IT expenses and proof of value

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



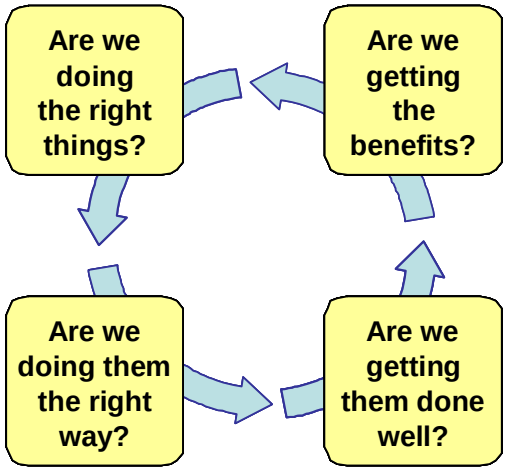
The Four "Ares"- continually asking:

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?

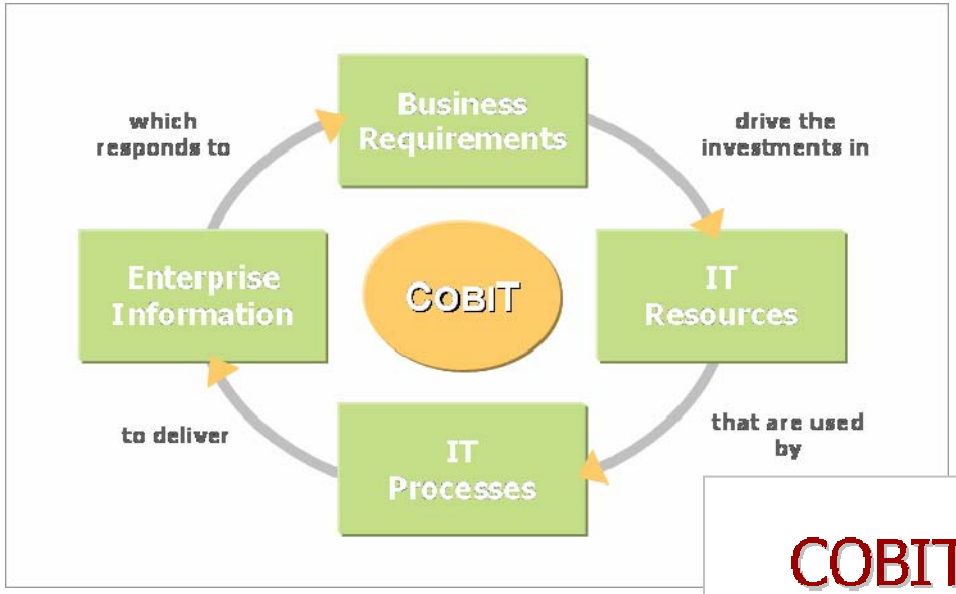
The *delivery* question. Do we have:

- 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?

Source: *The Information Paradox*

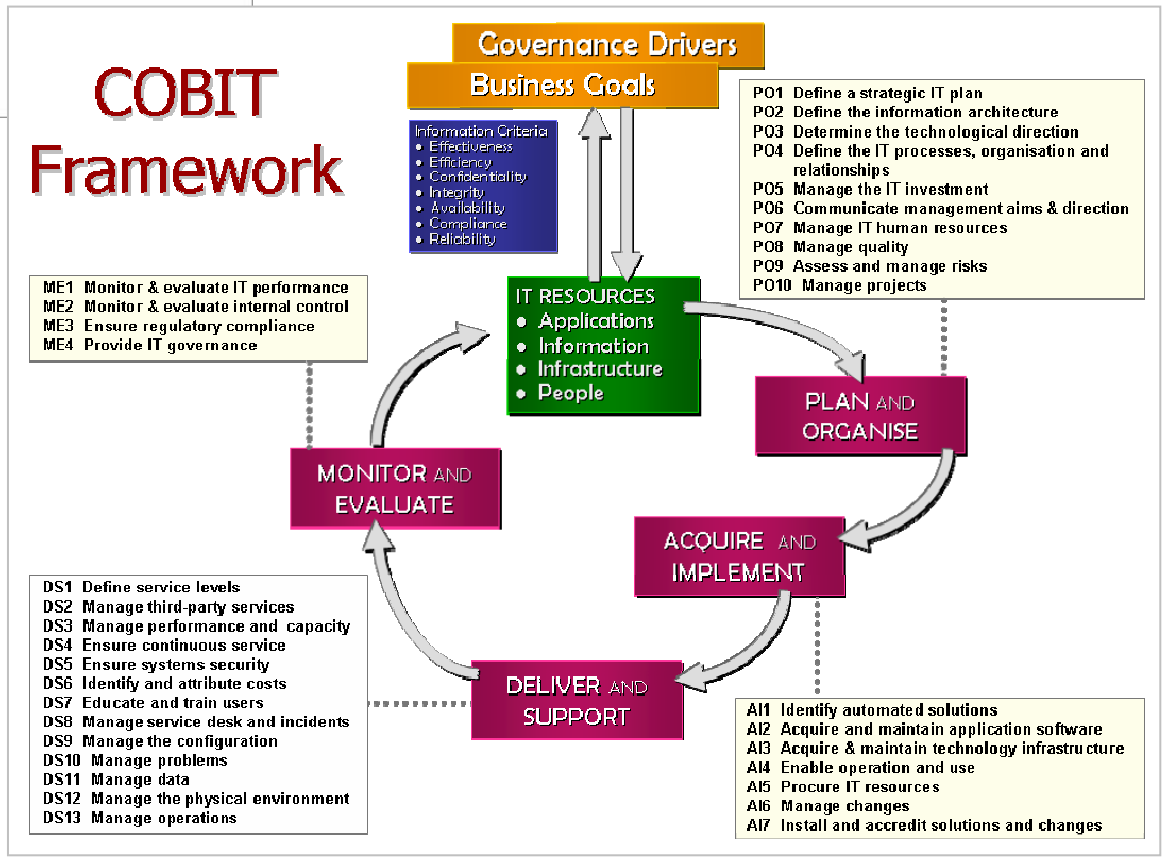
CobiT

The Basic COBIT Principle

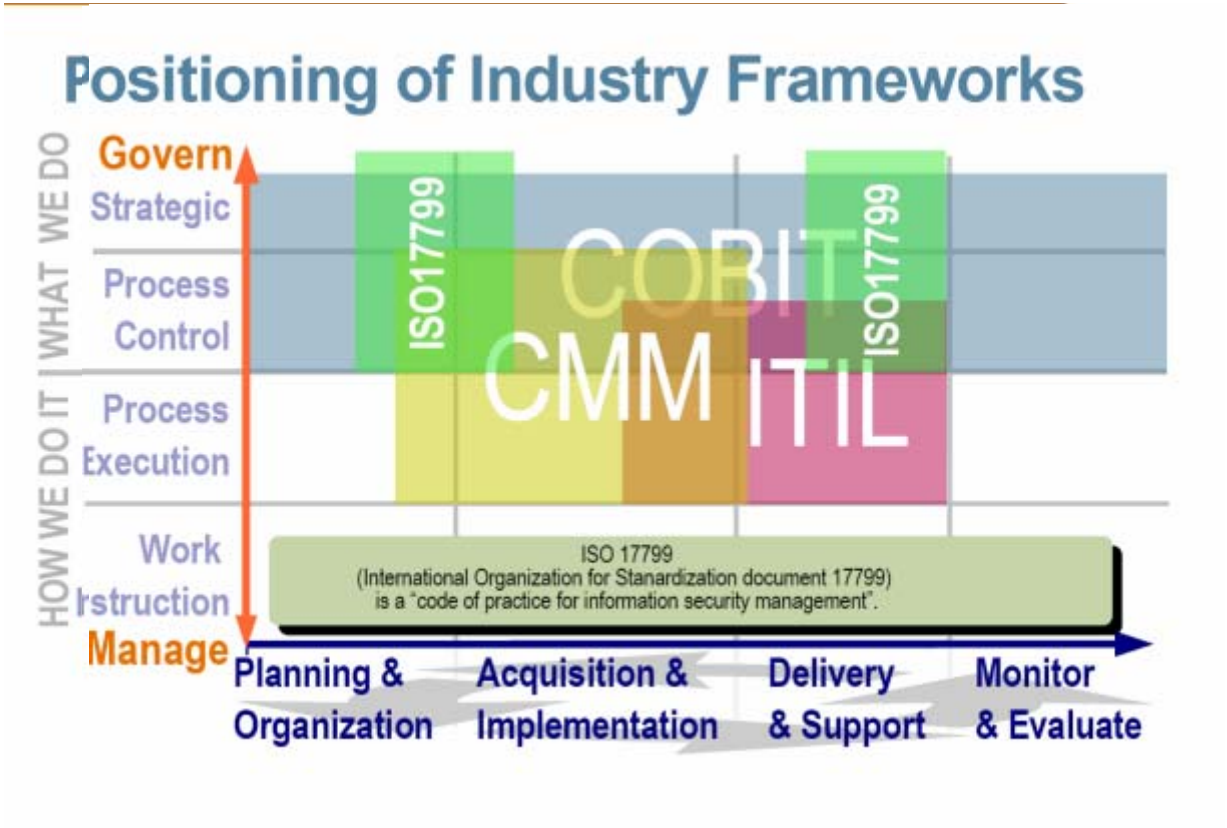


ISACA®
Serving IT Governance Professionals

COBIT Framework



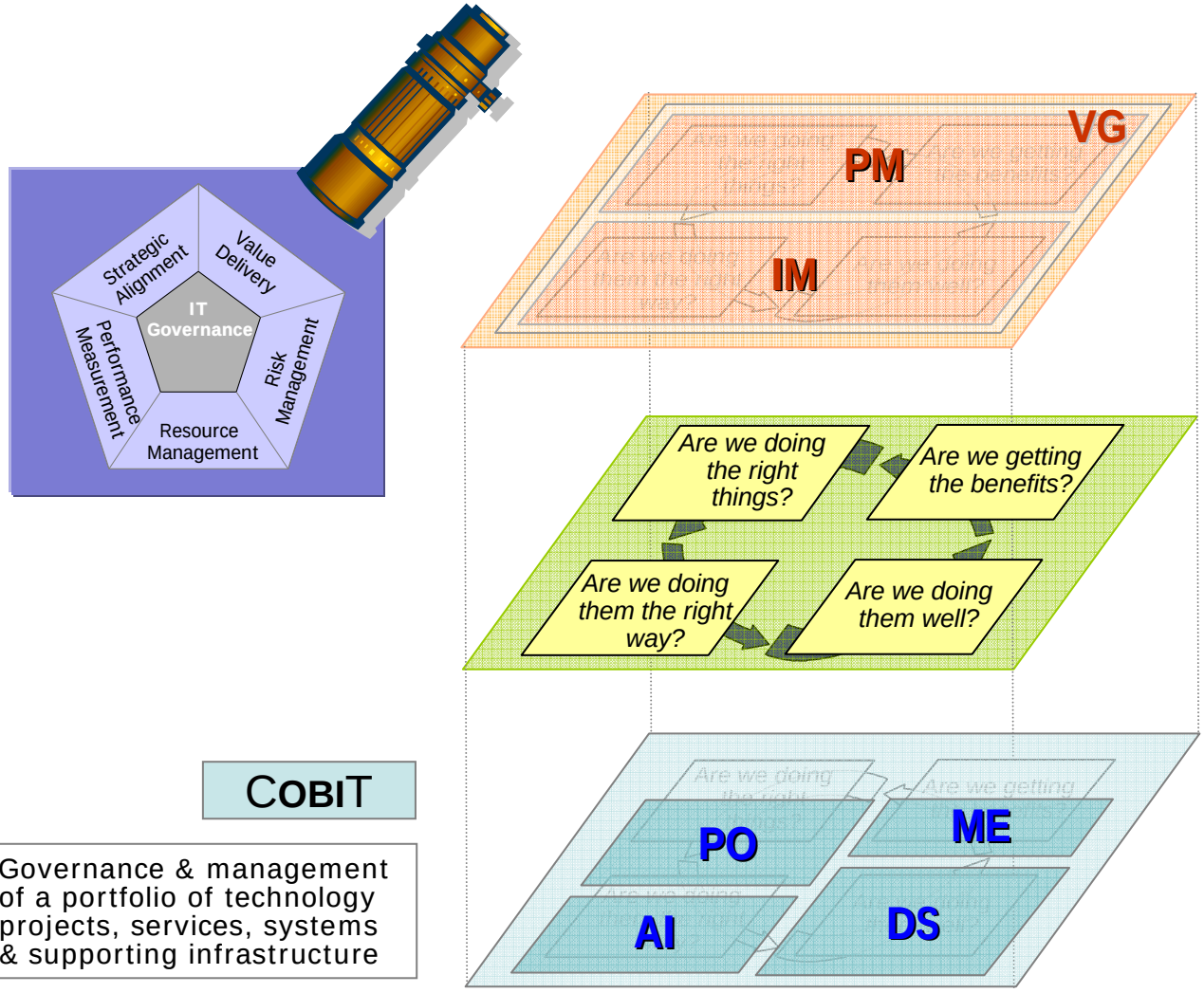
The use of management frameworks



Val-IT

Val IT Initiative

…a value lens into COBIT



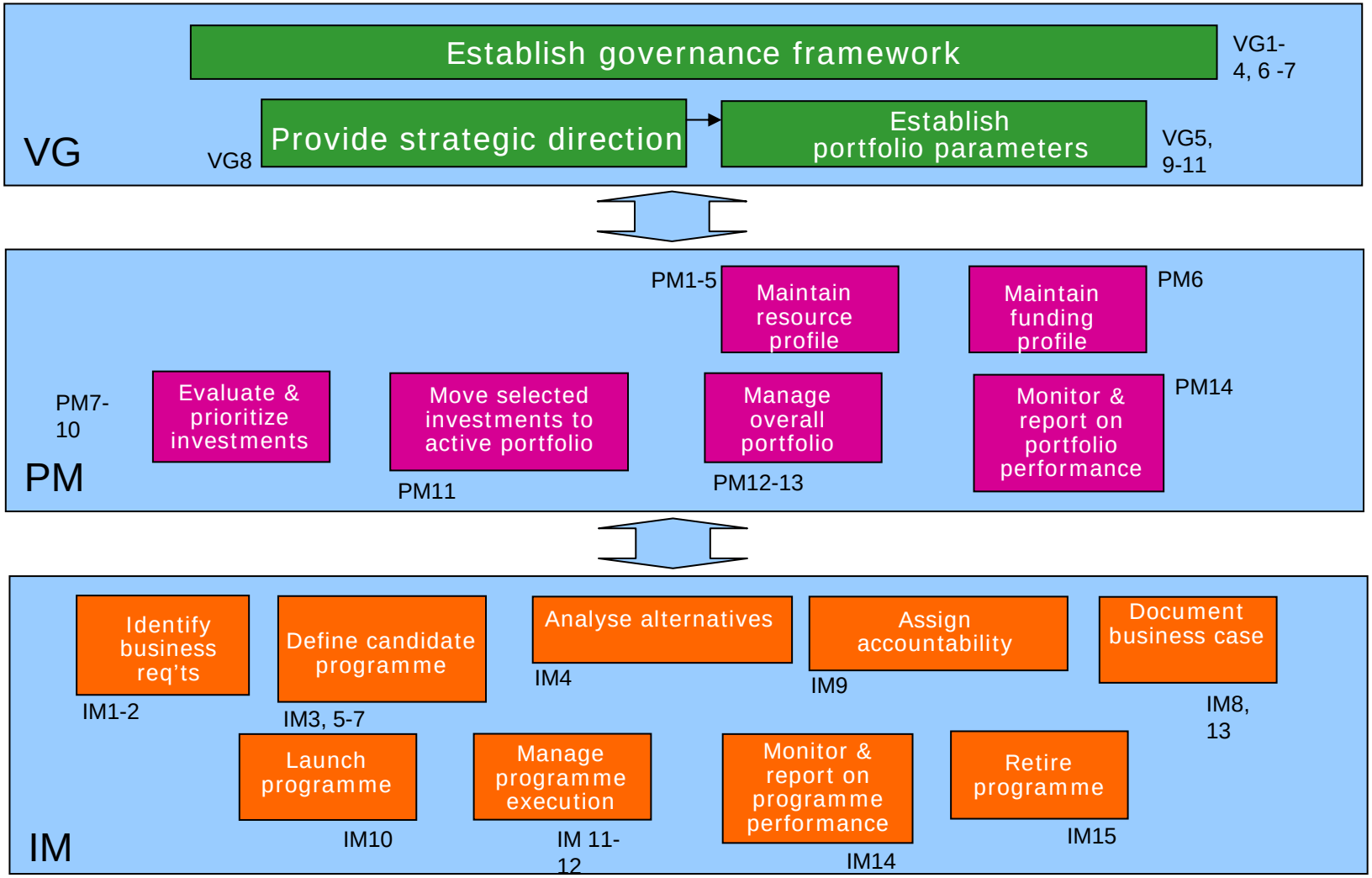
COBIT

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

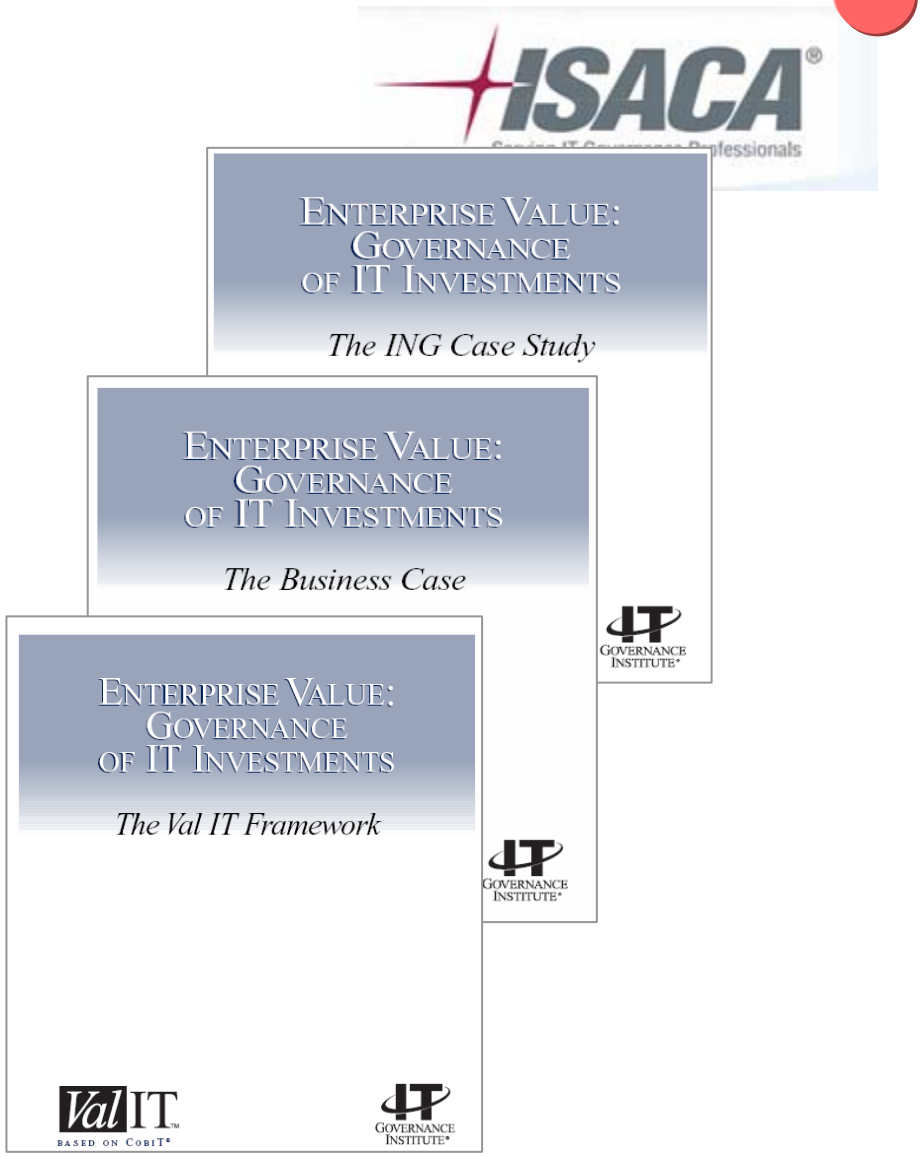
Val IT

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

IT Audit

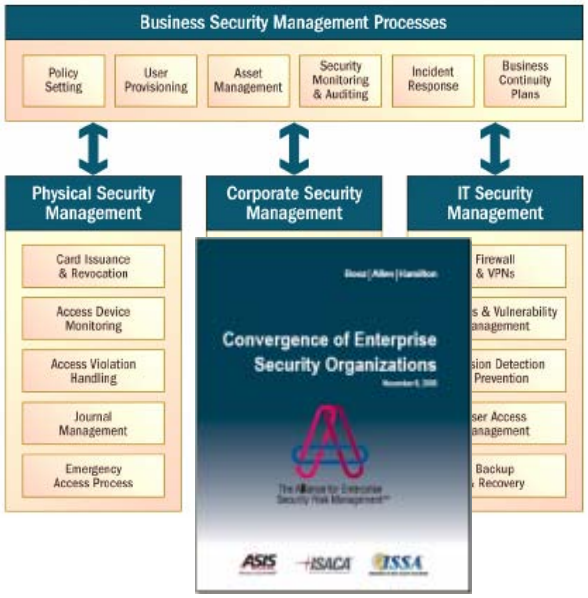
Background of IT Auditing

- 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 an Risk and on Internal Controls

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


Business Security Management Processes
Policy Setting
User Provisioning
Asset Management
Security Monitoring & Auditing
Incident Response
Business Continuity Plans
Physical Security Management
Corporate Security Management
IT Security Management
Card Issuance & Revocation
Access Device Monitoring
Access Violation Handling
Journal Management
Emergency Access Process
Firewall & VPNs
Backup & Recovery
Convergence of Enterprise Security Organizations
ASIS
ISACA
ISSA


Senior Management
Business Strategy
Organisation Objectives
Steering Committee and Executive Management
Risk Management/Information Security Strategy
Security Requirements
CISO/ Steering Committee
Security Action Plan, Policies, Standards
Security Programmes
Implementation
Security Objectives
Information Security Governance:
Guidance for Boards of Directors and Executive Management
2nd Edition

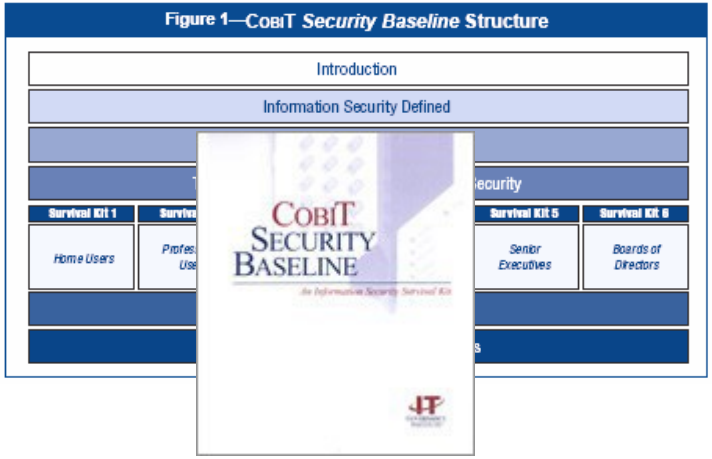
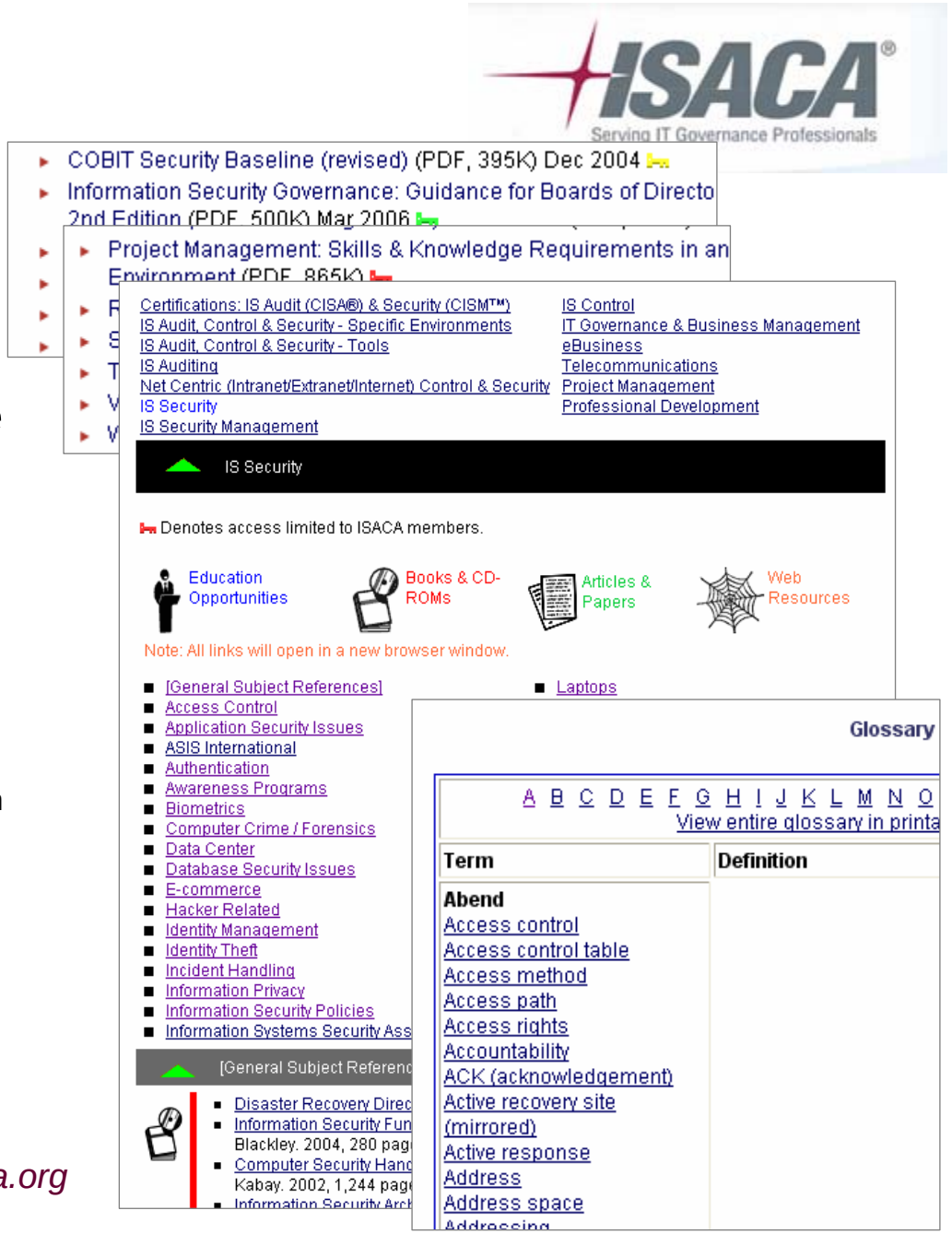


Figure 1—CobiT Security Baseline Structure
Introduction
Information Security Defined
Survival Kit 1
Survival Kit 5
Survival Kit 6
Home Users
Senior Executives
Boards of Directors
CobiT Security Baseline

Security

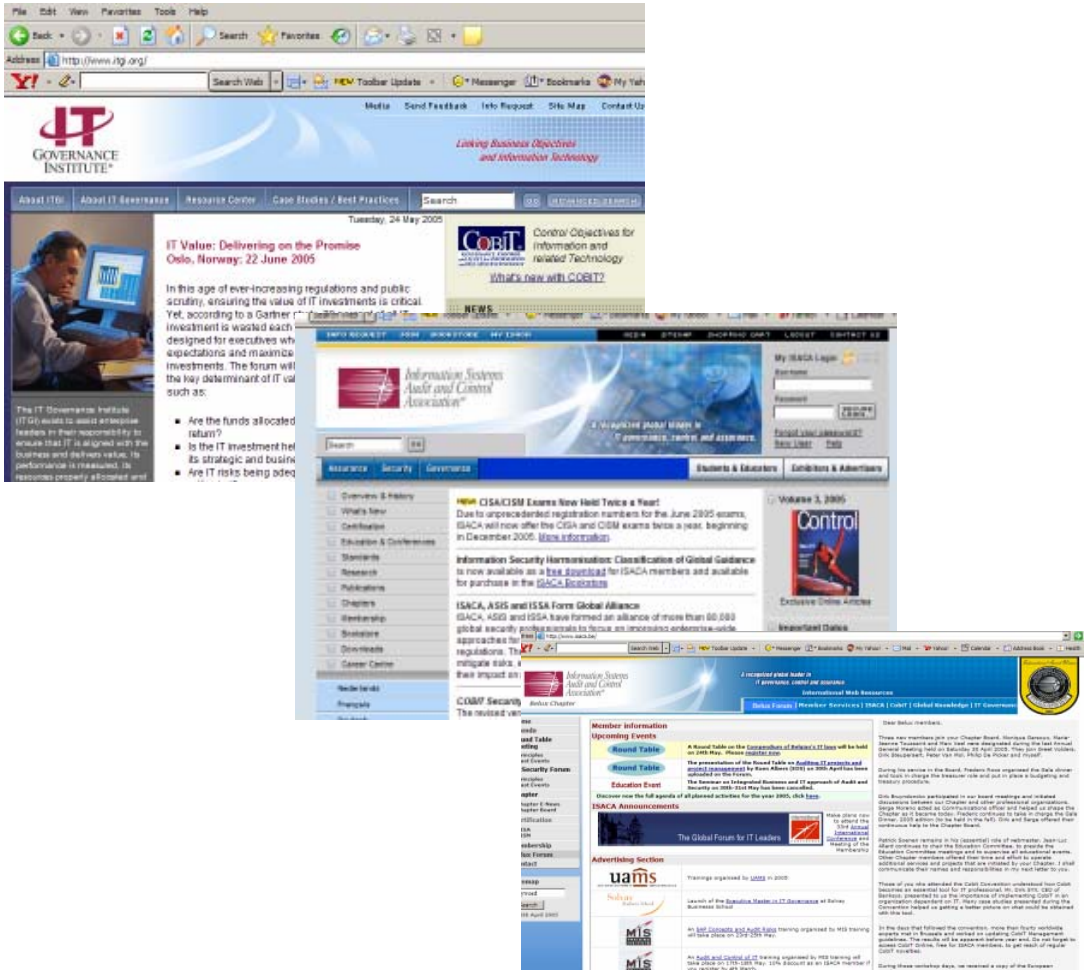
- Research and publications
  - Security Governance
  - Security technology
- Security Knowledge Centre
  - K-NET contains over 6,000 peer-reviewed web site resources
  - Pertaining to knowledge covering IT Governance, Assurance, Security and Control.
- Glossary
- Security Management Committee
  - Establishes 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



Further references

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



Jean-Luc Allard

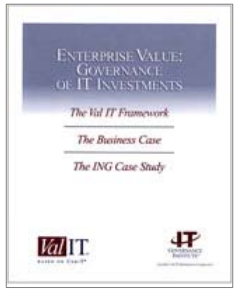
- Chairman of the Education Committee at ISACA Belux Chapter
- Managed telecommunication and Information Systems at the Belgian Air Force
- Active involvement with the Belgian Shadow Committee for developing standards such as ISO/IEC 13335, 27005, 2700x
- Member of the Belgian Chamber of IT Expert Witnesses (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

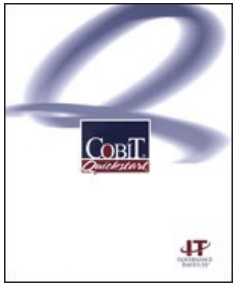
- Past Senior Security Consultant at Cybertrust (Ubizen) where he was involved with the development of a process and method for information security risk management (based on EBIOS) and application with a dozen of clients in countries such as Belgium, United States, Saudi Arabia, The Grand Duchy of Luxembourg, 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).

Georges Ataya MSCS, PBA, CISA, CISM, CISSP

- 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 ?