ISACA Roma – Resources for IT Governance

Prof. Ing. Claudio CILLI
CIA, CISA, CISM, CGEIT, CRISC, CISSP, CSSLP, M.Inst.ISP

University of Rome "Sapienza"
ISACA Rome Chapter President

cilli@di.uniroma1.it
c.cilli@isacaroma.it
www.dsi.uniroma1.it/~cilli

OWASP-Italy Day2012
Rome, 23° November 2012

The OWASP Foundation
http://www.owasp.org

ISACA Facts

- Founded in 1969 as the EDP Auditors Association
- Since 1978, CISA has been a globally accepted standard of competency among IS audit, control, assurance and security professionals
- More than 95,000 members in over 160 countries
- More than 190 chapters worldwide

ISACA Roma Facts

- Founded in 2002
- Awarded as the best growing Chapter in the World
- Current Members: 312 (CGEIT: 26 - CRISC: 60 - CISA: 163 - CISM: 74)
- Provides certification preparation courses
- Free monthly seminars on IT Security and Audit
- Research activities

www.isacaroma.it

IT Governance

- Methodology and research

- Certification: CISA/CISM/CGEIT/CRISC

www.isaca.org/certification

Information!

- Information is a key resource for all enterprises
- Information is created, used, retained, disclosed and destroyed
- Technology plays a key role in these actions
- Technology is becoming pervasive in all aspects of business and personal life

- **What benefits does information and technology bring to enterprises?**

Enterprise benefits?

Enterprises and their executives strive to:

- Maintain quality information to support business decisions
- Generate business value from IT-enabled investments, i.e. achieve strategic goals and realise business benefits through effective and innovative use of IT
- Achieve operational excellence through reliable and efficient application of technology
- Maintain IT-related risk at an acceptable level
- Optimise the cost of IT services and technology

How can these benefits be realized to create enterprise stakeholder value?

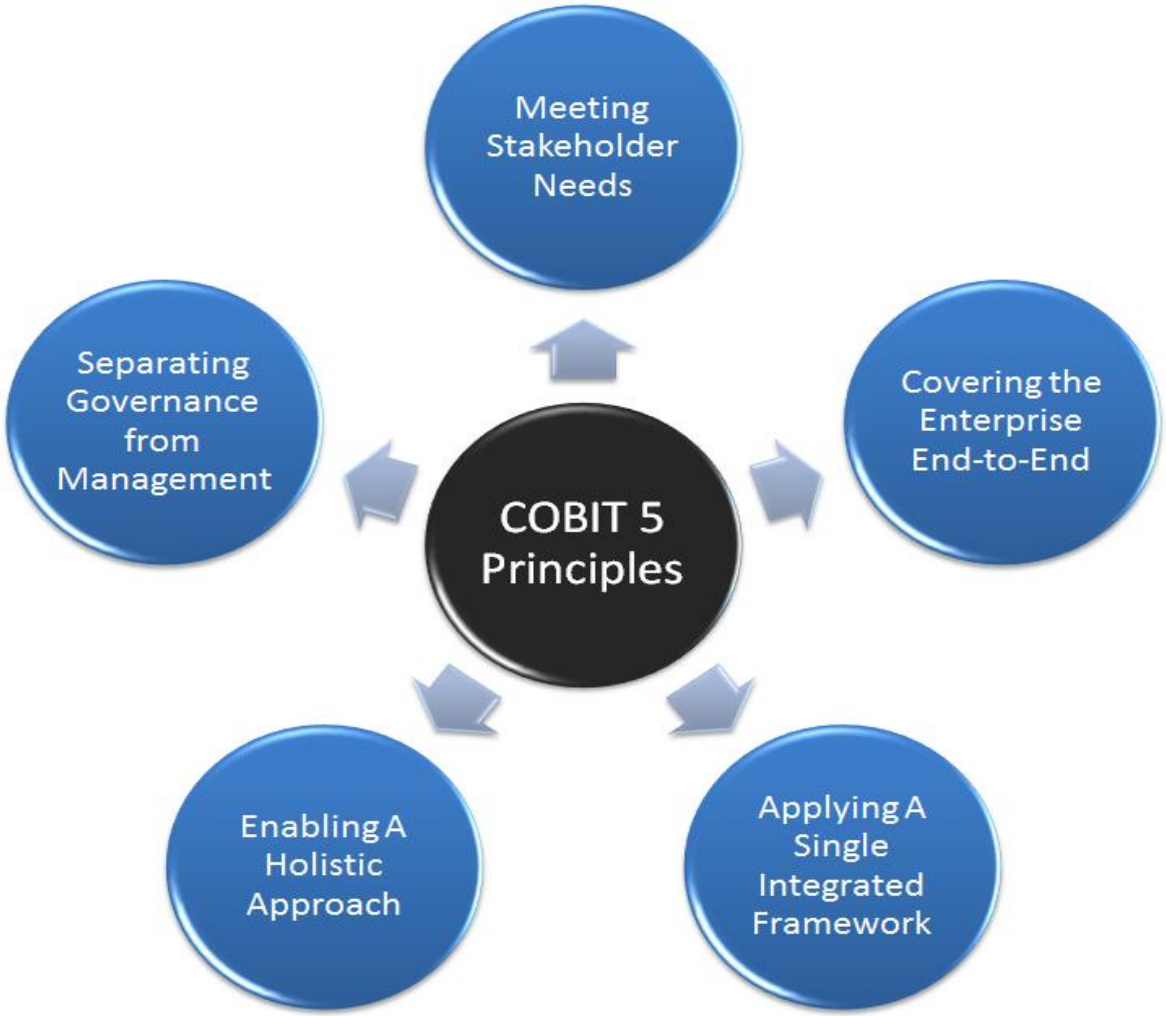
Stakeholder value!

- Delivering enterprise stakeholder value requires good **governance and management** of information and technology (IT) assets
- Enterprise Boards, Executives and management have to **embrace IT** like any other significant part of their business
- External **legal, regulatory and contractual compliance** requirements related to enterprise use of information and technology are increasing, threatening value if breached
- **COBIT 5 provides a comprehensive framework that assists enterprises to achieve their goals and deliver value through effective governance and management of enterprise IT**

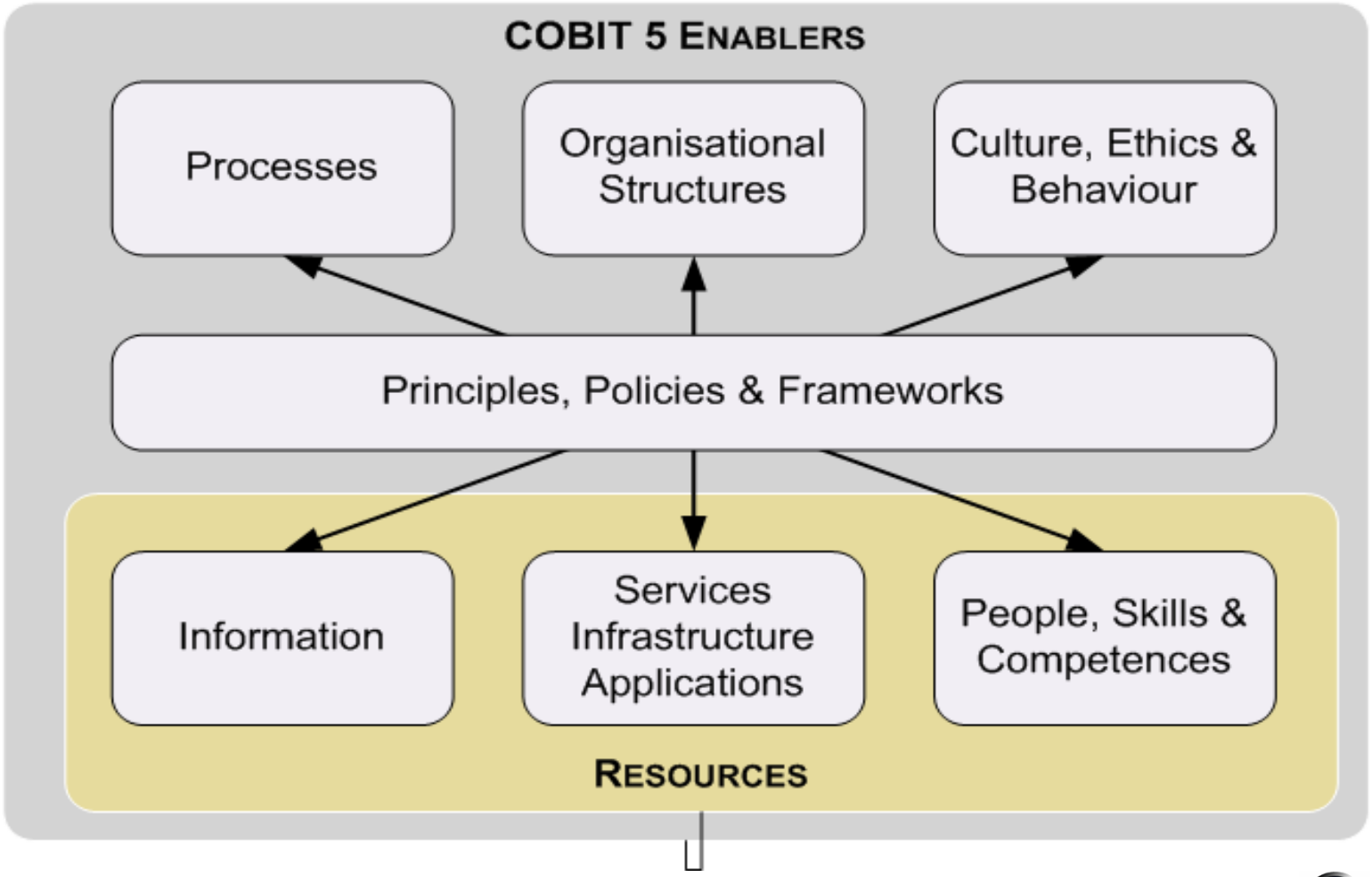
The COBIT 5 Framework

- Simply stated, COBIT 5 helps enterprises to create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use
- COBIT 5 enables information and related technology to be governed and managed in a holistic manner for the whole enterprise, taking in the full end-to-end business and functional areas of responsibility, considering the IT-related interests of internal and external stakeholders
- The COBIT 5 **principles** and **enablers** are generic and useful for enterprises of all sizes, whether commercial, not-for -profit or in the public sector

COBIT 5 Principles



COBIT 5 enablers



Governance & Management

Governance

- Governance ensures that enterprise objectives are achieved by **evaluating** stakeholder needs, conditions and options; setting **direction** through prioritisation and decision making; and **monitoring** performance, compliance and progress against agreed direction and objectives **[EDM]**

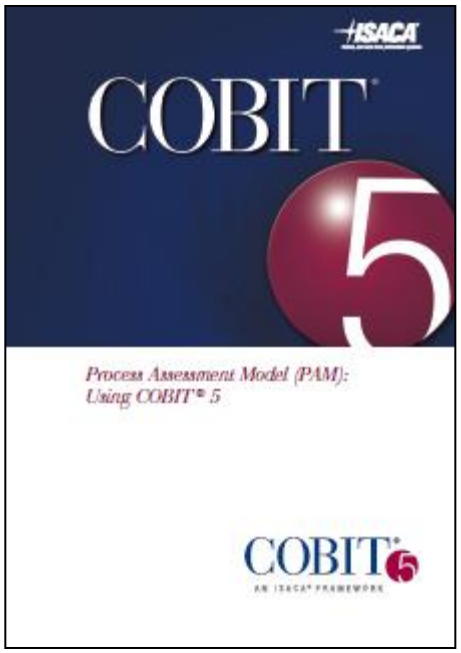
Management

- Management **plans, builds, runs** and **monitors** activities in alignment with the direction set by the governance body to achieve the enterprise objectives **[PBRM]**

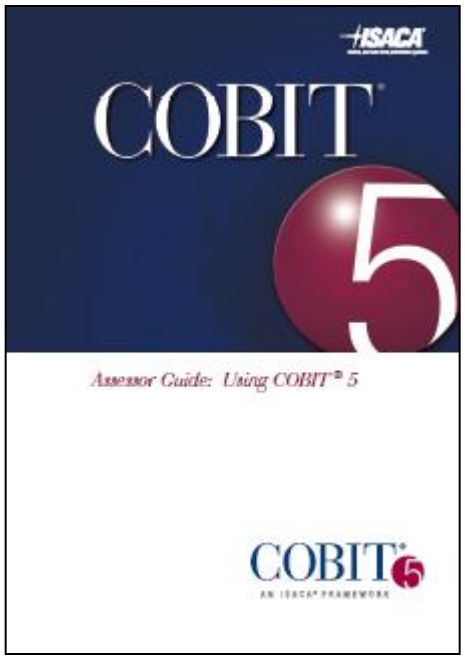
In summary ….

COBIT 5

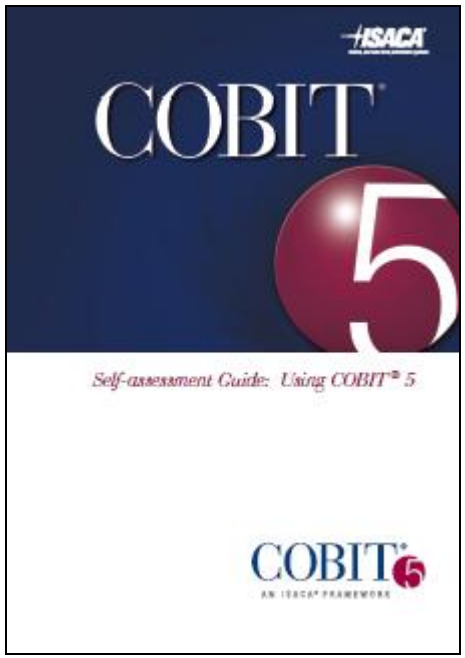
- brings together the **five principles** that
- allow the enterprise to build an effective **governance** and **management** framework based on
- an holistic set of **seven enablers** that
- optimises **information** and **technology** investment and use for the benefit of stakeholders



Process Assessment Model (PAM) : Using COBIT® 5



Assessor Guide : Using COBIT® 5



Self-assessment Guide : Using COBIT® 5

COBIT® 5

AN ISACA® FRAMEWORK

www.isaca.org/cobit

CISA Certification Details

www.isaca.org/cisa

CISA Job Practice Areas (Effective 2011)

- The Process of Auditing Information Systems – 14%
  - Provide audit services in accordance with IT audit standards to assist the organization in protecting and controlling information systems.
- Governance and Management of IT – 14%
  - Provide assurance that the necessary leadership and organization structure and processes are in place to achieve objectives and to support the organization's strategy.
- Information Systems Acquisition, Development and Implementation – 19%
  - Provide assurance that the practices for the acquisition, testing and implementation of information systems meet the organization's strategies and objectives.

CISA Job Practice Areas (Effective 2011) (continued)

- Information Systems Operations, Maintenance and Support – 23%
  - Provide assurance that the processes for information systems operations, maintenance and support meet the organization's strategies and objectives.
- Protection of Information Assets – 30%
  - Provide assurance that the organization's security policies, standards, procedures, and controls ensure the confidentiality, integrity, and availability of information assets.

For complete details, visit www.isaca.org/cisajobpractice

CISA Certification Requirements

- Earn a passing score on the CISA Exam. (CISA exam is offered in 11 languages.)
- Have a minimum of five years of verifiable IS audit, control or security experience (substitutions available)
- Submit the CISA application and receive approval
- Adhere to ISACA's Code of Professional Ethics
- Abide by IS Auditing Standards as adopted by ISACA
- Comply with CISA Continuing Professional Education Policy

CISM Certification Details

www.isaca.org/cism

CISM Certification Current Facts

- More than 16,000 CISMs worldwide
- The CISM exam is offered in 4 languages (English, Japanese, Korean and Spanish) in over 240 locations
- What makes CISM Unique?
  - Designed for information security managers exclusively
  - Criteria and exam developed from job practice analysis validated by information security managers
  - Experience requirement includes information security management

CISM Job Practice (Effective June 2012)

- Information Security Governance (24%)
  - Establish and maintain an information security governance framework and supporting processes to ensure that the information security strategy is aligned with organizational goals and objectives, information risk is managed appropriately and program resources are managed responsibly.
- Information Risk Management and Compliance (33%)
  - Manage information risk to an acceptable level to meet the business and compliance requirements of the organization.
- Information Security Program Development and Management (25%)
  - Establish and manage the information security program in alignment with the information security strategy.
- Information Security Incident Management (18%)
  - Plan, establish and manage the capability to detect, investigate, respond to and recover from information security incidents to minimize business impact

For more details visit www.isaca.org/cismjobpractice

CISM Certification Requirements

- Earn a passing score on the CISM exam
- Submit verified evidence of a minimum of five years of information security management work experience (covering 3 of the 4 job practice domains)
- Submit completed CISM application within 5 years of passing exam and receive approval
- Adhere to the ISACA Code of Professional Ethics
- Comply with the CISM Continuing Professional Education Policy

CGEIT Certification Details

www.isaca.org/cgeit

CGEIT: Who is it for?

The CGEIT certification is intended to recognize a wide range of professionals for their knowledge and application of IT governance principles and practices.

It is designed for professionals who have management, advisory, or assurance responsibilities as defined by the CGEIT Job Practice consisting of IT governance related task and knowledge statements.

CGEIT Job Practice

- IT Governance Framework (25%)
  - Define, establish and maintain an IT governance framework (leadership, organizational structures and processes) to: ensure alignment with enterprise governance; control the business information and information technology environment through the implementation of good practices; and assure compliance with external requirements.
- Strategic Alignment (15%)
  - Ensure that IT enables and supports the achievement of business objectives through the integration of IT strategic plans with business strategic plans and the alignment of IT services with enterprise operations to optimize business processes.
- Value Delivery (15%)
  - Ensure that IT and the business fulfill their value management responsibilities: IT-enabled business investments achieve the benefits as promised and deliver measurable business value both individually and collectively, that required capabilities (solutions and services) are delivered on-time and within budget, and that IT services and other IT assets continue to contribute to business value.
- Risk Management (20%)
  - Ensure that appropriate frameworks exist and are aligned with relevant standards to identify, assess, mitigate, manage, communicate and monitor IT-related business risks as an integral part of an enterprise's governance environment.
- Resource Management (13%)
  - Ensure that IT has sufficient, competent and capable resources to execute current and future strategic objectives and keep up with business demands by optimizing the investment, use and allocation of IT assets.
- Performance Measurement (12%)
  - Ensure that business-supporting IT goals/objectives and measures are established in collaboration with key stakeholders and that measurable targets are set, monitored and evaluated.

For more details visit www.isaca.org/cgeitjobpractice

CGEIT Experience Requirements

- Earn a passing score on the CGEIT exam
- Submit verified evidence of the five year experience requirement as defined by the CGEIT Job Practice
- Submit the CGEIT application and receive approval
- Adhere to the ISACA Code of Professional Ethics
- Comply with the CGEIT Continuing Education Policy

Certified in Risk and Information Systems Control™

www.isaca.org/crisc

CRISC Target Market

- Designed exclusively for risk and information controls personnel who:
  - Identify, assess and analyze risk
  - Design, implement and maintain controls to mitigate risk
  - Respond to risk events

CRISC Job Practice (Effective June 2010)

- Risk Identification, Assessment and Evaluation (31%)
  - Identify, assess and evaluate risk to enable the execution of the enterprise risk management strategy.
- Risk Response (17%)
  - Develop and implement risk responses to ensure that risk issues, opportunities and events are addressed in a cost-effective manner and in line with business objectives.
- Risk Monitoring (17%)
  - Monitor risk and communicate information to the relevant stakeholders to ensure the continued effectiveness of the enterprise‘s risk management strategy.
- IS Control Desing and Implementation (17%)
  - Design and implement IS controls in alignment with the organisation‘s risk appetite and tolerance levels to support business objectives.
- IS Control Monitoring and Maintenance (18%)
  - Monitor and maintain IS controls to ensure they function effectively and efficiently.

For more details visit www.isaca.org/criscjobpractice

CRISC Certification Requirements

- Earn a passing score on the CRISC exam
- Submit verified evidence of a minimum of 3 years of risk and information systems controls experience (covering 3 of the 5 job practice domains)
- Submit completed CRISC application within 5 years of passing exam and receive approval
- Adhere to the ISACA Code of Professional Ethics
- Comply with the CRISC Continuing Professional Education Policy