INFO 6008

Week 2 –ISACA and COBIT

FANSHAWE

ISACA: https://www.isaca.org/About-ISACA/Press-room/Documents/ISACA_Fact-Sheet_0119.pdf

History

- ISACA was incorporated in 1969 by a small group of individuals who recognized a need for a centralized source of information and guidance in the growing field of auditing controls for computer systems. Today, ISACA serves 140,000 professionals in 180 countries.
- ISACA provides practical guidance, benchmarks and other effective tools for all enterprises that use information systems. Through its comprehensive guidance and services, ISACA defines the roles of information systems governance, security, audit and assurance professionals worldwide. The COBIT framework and the CISA, CISM, CGEIT and CRISC certifications are ISACA brands respected and used by these professionals for the benefit of their enterprises.

ISACA: https://www.isaca.org/About-ISACA/Press-room/Documents/ISACA_Fact-Sheet_0119.pdf

- ISACA® (isaca.org) is a global association helping individuals and enterprises achieve the positive potential of technology.
- Today's world is powered by information and technology, and ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organizations.

ISACA: https://www.isaca.org/About-ISACA/Press-room/Documents/ISACA_Fact-Sheet_0119.pdf

- ISACA leverages the expertise of its 460,000 engaged professionals in information and cybersecurity, governance, assurance, risk and innovation, as well as its enterprise performance subsidiary, CMMI® Institute, to help advance innovation through technology.
- ISACA has a presence in 188 countries, including more than 220 chapters worldwide and offices in both the United States and China.

ISACA: https://www.isaca.org/About-ISACA/Press-room/Documents/ISACA_Fact-Sheet_0119.pdf

- ISACA Facts and Figures:
- Established: 1969
- Engaged Professionals:460,000
- Members:140,000 in 188 countries
- Members and Certification-Holders:166,000+
- Chapters: More than 220
- Student Groups: 97

ISACA: https://www.isaca.org/About-ISACA/Press-room/Documents/ISACA_Fact-Sheet_0119.pdf

- ISACA Certifications
- ISACA developed and administers industry-leading certifications:
- Certified Information Systems Auditor® (CISA®). More than 146,000 CISAs have been certified since its inception in 1978.
- Certified in Risk and Information Systems Control™(CRISC™). More than 25,000 CRISCs have been certified since 2010.

ISACA: https://www.isaca.org/About-ISACA/Press-room/Documents/ISACA_Fact-Sheet_0119.pdf

- Certified Information Security Manager(CISM). More than 43,000 CISMs have been certified since 2002.
- Certified in the Governance of Enterprise IT (CGEIT). More than 8,000 CGEITs have been certified since 2007.
- CSX Practitioner Certification (CSXP™) is a performance-based certification allowing practitioners to validate their skills as a cybersecurity first-responder.
- The CSX Practitioner Certification (CSXP) exam was improved in 2018 to reflect current cybersecurity tasks and challenges and to support remote, flexible administration.

The CISA Certification

- The CISA exam was established in 1978 by the Information Systems Audit and Control Association (ISACA).
- More than 146,000 individuals (and counting) have obtained CISA certification worldwide, and more than 31,000 of them are audit directors, managers, consultants, or auditors.
- In North America, more than 33,000 individuals have CISA certification.

CISA EXAM

- The key mission of the CISA exam, as stated by ISACA, is as follows:
- *To develop and maintain a testing instrument that can be used to evaluate an individual's competency in conducting information systems audits.*

CISA EXAM

- The key mission of the CISA exam, as stated by ISACA, is as follows:
- *To develop and maintain a testing instrument that can be used to evaluate an individual’s competency in conducting information systems audits.*

CISA EXAM

- We all know how much the business world and technology have evolved in recent years.
- Globalization has broken down national barriers.
- Technology has evolved at lightning speeds—beyond the capability of the current laws to keep pace.
- Core issues related to personal privacy, electronic surveillance, and corporate ethics continue to challenge how personal rights are perceived in this digital age.

CISA EXAM

- We are all recipients of the benefits of the digital and technology explosion. Imagine life without the ability to instantly connect through smartphones or how narrow our perception of the world would be without the Internet.
- As businesses and governments continue to innovate through technology, they challenge the boundaries between personal and professional life. It often seems that every aspect of a person’s life has been digitized somewhere by someone—from health records and school records to personal emails and photos.

CISA EXAM

- The advent of social media has made it increasingly difficult for us to control our own personal data or to maintain privacy.
- As a result, businesses, governments, and individuals are on a constantly evolving journey, dealing with how to realize the benefits that technology provides while figuring out how to navigate the risks.

CISA EXAM

- On this journey, events and technology innovation continually redefine what is considered acceptable. Think about major cybersecurity breaches in which millions of customer credit card accounts or health care records are stolen. Or consider the evolution of autonomous vehicles: Driverless cars are more and more making life-and-death decisions on behalf of passengers and pedestrians.

CISA EXAM

- Top leadership in any organization needs the assurance that the organization is doing everything possible to follow a common set of accepted rules and principles. In this way, top leadership can be assured that they are managing these technology risks in an acceptable manner.

CISA EXAM

- Simply passing the CISA exam does not mean you are CISA certified. Remember that the CISA certification is intended to ensure that you are competent in your discipline related to the core set of commonly accepted rules and principles in information systems.

CISA EXAM

- Think of it this way: You can pass the written driver’s license test but you still need to practice behind the wheel.
- The CISA certification takes a similar approach, requiring a combination of passing a knowledge test and also demonstrating competence through actual work experience.
- To obtain CISA certification, you must meet four key requirements:

CISA EXAM

1. Pass the CISA exam
2. Demonstrate five years of professional work experience, which will be verified through your employer *.
3. Agree to adhere to the ISACA rules related to the ISACA Code of Professional Ethics, standards, and continuing education
4. Submit an application for CISA certification

***The requirement to have five years of professional work experience often creates anxiety for individuals. The good news is that ISACA has a waiver program that allows individuals to substitute up to three of the five years of work experience – check ISACA's website for details.**

CISA EXAM

- **CISA Exam Domains**
- The CISA exam is divided into five job practice areas, or domains.
- The CISA exam domains serve as the basis for the exam and the requirements to earn the certification. The exam domains consist of task and knowledge statements representing the work performed in information systems audit, assurance, and control.

CISA EXAM

- **The Five CISA Exam Domains**

- **Domain 1: The Process of Auditing Information Systems:**
- Planning and conducting information systems audits in accordance with IS standards and best practices, communicating results, and advising on risk management and control practices.

CISA EXAM

- **The Five CISA Exam Domains**

- **Domain 2: Governance and Management of IT:**
- Ensuring that adequate organizational structures and processes are in place to align and support the organization’s strategies and objectives.

CISA EXAM

- **The Five CISA Exam Domains**

- **Domain 3: Information Systems Acquisition, Development, and Implementation**
- Ensuring that appropriate processes and controls are in place for the acquisition, development, testing, and implementation of information systems in order to provide reasonable assurance that the organization’s strategies and objectives will be met.

CISA EXAM

- **The Five CISA Exam Domains**

- **Domain 4: Information Systems Operations and Business Resilience**

- Ensuring that systems and infrastructure have appropriate operations, maintenance, and service management processes and controls in place to support meeting the organization’s strategies and objectives..

CISA EXAM

- **The Five CISA Exam Domains**

- **Domain 5: Protection of Information Assets:**
- Ensuring that the organization’s security policies, standards, procedures, and controls protect the confidentiality, integrity, and availability of information assets.

CISA Certification

- The CISA exam codifies a core set of commonly accepted technology rules and principles. CISA certification ensures that individuals have the competency to provide leadership with the assurance that their organization complies with these industry norms.
- This assurance to top leadership is in many cases, the law. Top leaders of an organization can be personally liable for failure to put in place digital safeguards to protect customers and shareholders from technology risks.

CISA Certification

- When the U.S. Congress passed the Sarbanes-Oxley Act of 2002, it wanted to restore the confidence of investors by improving the reliability of financial reporting and strengthening the control environment, such as information systems controls.

CISA Certification

- The law calls out specific obligations for officers of a company, such as the CEO and CFO who must certify compliance with the law and ensure that the related control environment is in place and working.
- If this certification is found to be materially flawed or fraudulent, the officers can be held personally accountable and subject to heavy fines and potentially even prison time.

CISA Certification

- Senior executives need to know whether their organization is compliant with the Sarbanes-Oxley Act, but this can be a daunting task, especially in a large organization where operations and technical knowledge are siloed.
- Senior executives, therefore, need to have competent individuals to build, maintain, and audit their technology.

CISA Certification

- We have only looked briefly at SOX and a single company.
- Take more companies and more laws and you can see the need for a core set of commonly accepted rules and principles.
- The CISA exam addresses this important need, and that’s why it continues to gain popularity.

CISA Certification

- We have only looked briefly at SOX and a single company.
- Take more companies and more laws and you can see the need for a core set of commonly accepted rules and principles.
- The CISA exam addresses this important need, and that’s why it continues to gain popularity.

CISA Certification

- The CISA certification's growth in popularity has made it the gold standard in the industry for many professionals. The certification is often seen as being key to advancement in information systems auditing and a growing number of other information systems roles.

CISA Certification

- As part of the CISA application, you must sign off on three agreements. You must agree to the following:
- To conduct yourself honestly and ethically and abide by the Code of Professional Ethics (see www.isaca.org/ethics)
- To abide by the information systems standards, as adopted by ISACA (see www.isaca.org/standards)
- To maintain your competency through continuing professional education (CPE)
  (see www.isaca.org/cisacpepolicy)

CISA Certification

- The three agreements are part of the CISA application form, and ISACA takes them very seriously. Violations are rarely found, but when a clear violation is identified, the penalty may include revocation of CISA certification.

ENTERPRISE AND GOVERNANCE

- *Enterprise* is the term used to describe a range of different organisations:
- a commercial business (often called a corporation) that may, or may not, be quoted on a stock exchange;
- a public sector organisation such as a local or national government department,
- or a not-for-profit organisation such as a non-governmental organisation (NGO) or a charity.

ENTERPRISE AND GOVERNANCE

- Enterprise is a more generic term than business since business often implies there is commercial interest. As such, enterprise has become the term frequently used in the 21st century when discussing governance of organisations: that is, enterprise governance.

ENTERPRISE AND GOVERNANCE

- *Governance* is defined as per the Cambridge Dictionary as*:*

“the way that organizations or countries are managed at the highest level, and the systems for doing this” (https://dictionary.cambridge.org/dictionary/english/governance).

- Another way to look at it is: the action, manner or fact of governing; controlling or regulating influence or good order.

ENTERPRISE AND GOVERNANCE

- Clearly, governance applied to enterprises is expressing the view that directors (or top management) of enterprises are tasked with governing, controlling and regulating their enterprise using best practices.

ENTERPRISE AND GOVERNANCE

- Clearly, governance applied to enterprises is expressing the view that directors (or top management) of enterprises are tasked with governing, controlling and regulating their enterprise using best practices.

Corporate Governance

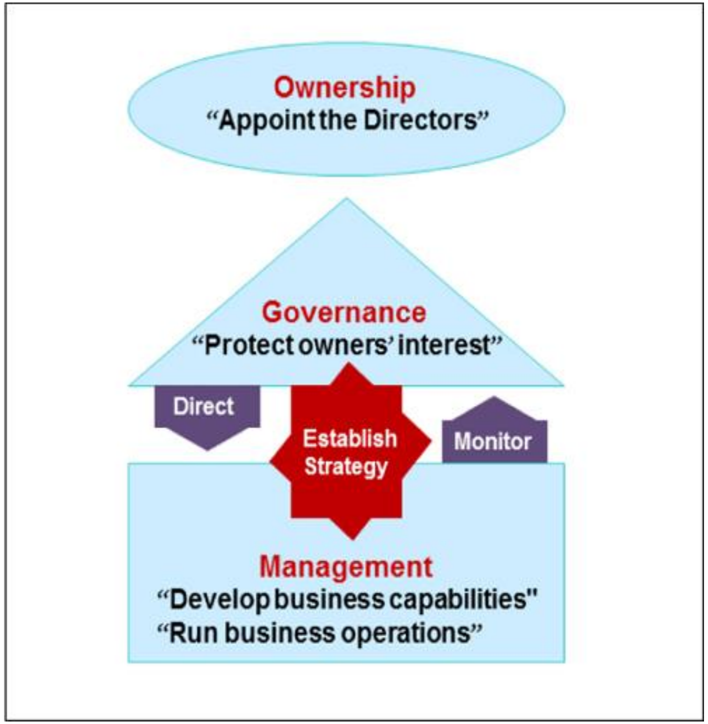
- Teresa Barger* explains corporate governance very succinctly. She states there are three parts:
- ownership
- governance
- management

* Ms. Barger serves on the Advisory Council for the Global Corporate Governance Forum among others.

Corporate Governance

- Her view is that shareholders have an ownership of a corporation and appointed directors govern the corporation. The directors’ duty is to protect the shareholders’ investment in the corporation by working with management to develop a corporate strategy and by directing management to run the corporation.
- Management’s job is ‘to develop business capabilities’ and ‘run business operations’. The directors would also request the management to provide reports so they could monitor whether their management was meeting directives.
- *Barger, T. (2004) Corporate Governance – A Working Definition, International Corporate Governance Meeting, Hanoi: IFC/World Bank Corporate Governance Department.*

Corporate Governance



IT Governance

- IT governance took off as a discipline once the COBIT framework evolved from an IT audit to an IT governance framework with the release of COBIT®3.0 in 2000.
- COBIT was, and still is, widely adopted as the *de facto* framework to meet the IT governance requirements of Section 404 of the Sarbanes-Oxley Act of 2002.
- COBIT recognised that IT governance was concerned with ensuring both conformance and performance, that is, compliance and value delivery to the business.

IT Governance

- IT governance should be the wellspring from which all other IT activities flow.
- Properly implemented, *governance* is a process whereby senior management exerts strategic control over business functions through policies, objectives, delegation of authority, and monitoring.

IT Governance

- Governance is management’s control over all other IT processes to ensure that IT processes continue to meet the organization’s business objectives effectively.
- Business alignment is a critical characteristic of IT governance. IT’s primary mission should be the support of the overall business mission, goals, and objectives. The alignment of IT to the business must be intentional and deliberate for IT and the organization to succeed.

IT Governance

- Organizations usually establish governance through an IT steering committee that is responsible for setting long-term IT strategy and by making changes to ensure that IT processes continue to support IT strategy and the organization’s needs. This is accomplished through the development and enforcement of IT policies, requirements, and standards.

IT Governance

- IT governance typically focuses on several key processes, such as personnel management, sourcing, change management, financial management, quality management, security management, and performance optimization.
- Another key component is the establishment of an effective organization structure and clear statements of roles and responsibilities. An effective governance program will use a balanced scorecard (BSC) or other means to monitor these and other key processes, and through a process of continuous improvement, IT processes will be changed to remain effective and to support ongoing business needs.

COBIT 5

- COBIT 5 was released in April 2012.
- COBIT 5 is a business framework for the governance and management of enterprise IT.
- Governance of enterprise IT is concerned with both governance and management and requires a broad range of practices to be included.
- IT governance is the responsibility of the board of directors and executive management.

COBIT 5

- It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives."
- The growing need for IT governance tools and techniques was fueled by the following factors:
- Growing complexity of IT environments
- Fragmented or poorly performing IT infrastructures
- User frustration leading to ad hoc solutions

COBIT 5

- IT costs perceived to be out of control
- IT managers operating in a reactive, rather than proactive, manner
- Communication gaps between business and IT managers
- Increasing pressure to leverage technology in business strategies
- Need to comply with increasing laws, standards, and regulations
- Scarcity of skilled staff

COBIT 5

- Lack of application ownership
- Resource conflicts/shifting priorities
- Impaired organizational flexibility and nimbleness to change
- Concern for risk exposures
- Volatile organizational, political, or economic environment

COBIT 5

- ISACA has always been very good at recognising such practices and has always used well-known frameworks and international standards as the basis for the development of COBIT. For example, COBIT4.1 was quoted by ISACA as being based on more than 40 other frameworks and standards and COBIT 5 is claimed to be based on more than 80 frameworks and standards.
- Some of the key frameworks and international standards which are the basis for COBIT 5 follow.

COBIT 5

- **ISO/IEC 38500: 2008 Corporate Governance Of Information Technology** is an International Standard based on an Australian Standard, AS 8015-2005, that specifies the three activities to be conducted by board members and senior executives who are accountable and responsible for corporate governance of IT.
- 1. Evaluate
- 2. Direct
- 3. Monitor

COBIT 5

IT SERVICE MANAGEMENT

- ITIL 2011 Edition
- ISO/IEC 20000: 2011

COBIT 5

- **IT INFRASTRUCTURE LIBRARY (ITIL) 2011 EDITION**
- ITIL was first published in 1989 and is almost certainly the most deployed framework in the world for IT.
- ITIL is concerned with best practices for the delivery of IT services to businesses and is based on three key areas:
- Services – IT applications that support business processes and activities
- Processes – these processes are used to control and manage IT services
- Functions – organisational units in the IT department

COBIT 5

- **ISO/IEC 20000: 2011 Information Technology Service Management System**
- ISO/IEC 20000 was originally developed in 2000 as British Standard BS 15000 using ITIL V2 as its main source of ITSM practices. It was developed as the basis for certification of organisations for IT service management.

COBIT 5

- **ISO/IEC 20000: 2011 Information Technology Service Management System**
- To gain certification an organisation has to be externally audited for compliance with the Standard, which confirms that the organisation is using recognised ITSM practices for the delivery of IT service management. BS 15000 was internationalised as ISO/IEC 20000 in 2005 and was upgraded in 2011.

COBIT 5

- **PROJECT MANAGEMENT**
- In this section the following will be discussed:
- • PRINCE2® 2009 Edition
- • PMBOK® 5th Edition (2013)

COBIT 5

- **PRINCE2 2009 EDITION**
- PRINCE2, an acronym for **PR**ojects **IN** **C**ontrolled **E**nvironments, was first published in 1996 and is a process-based method for managing projects of any kind. In 2009, it was upgraded to PRINCE2 2009 Edition to reflect developments in approaches to project management practices.
- PRINCE2 is adopted worldwide as a project management framework and is the framework of choice for most organisations in Europe.

COBIT 5

- **PMBOK®**
- PMBOK®, the **P**roject **M**anagement **B**ody of **K**nowledge, was first published in 1987 but in 2013 was updated to PMBOK® – 5
- PMBOK® is adopted worldwide as a project management framework and it is the framework of choice in North America.

COBIT 5

- **RISK MANAGEMENT**
- From an IT governance perspective, risk management frameworks are designed to identify and analyse IT-related risks; and determine how to mitigate, manage and monitor them while ensuring there is alignment with enterprise risk management.
- There are many standards and frameworks covering risk management including:

COBIT 5

RISK MANAGEMENT

- COSO ERM (Enterprise Risk Management (2004)) Commission.
- Risk IT™(2009) from ISACA. One of the ISACA frameworks used to build COBIT 5.
- Management of Risk (M_o_R)
- OCTAVE® (2001 and onwards) (Operationally Critical Threat, Asset and Vulnerability Evaluation) from the Software Engineering Institute at Carnegie Mellon University.
- ISO 31000:2009 Risk Management

COBIT 5

VALUE DELIVERY

- Value delivery enables business benefits to be realised from IT investments.
- Value delivery frameworks are:
- Val IT V2.0 (2008) from ISACA.
- Management of Value (MoV) (2010) from the UK Cabinet Office.

COBIT 5

INFORMATION SECURITY

- Information security is principally covered by the ISO/IEC 27000 series of standards.
- Two other frameworks that are related to ISO27000:
- MEHARI and The Standard of Good Practice for Information Security.

COBIT 5

INFORMATION SECURITY

- MEHARI was developed originally in 1996 for chief information security officers, CIOs, risk managers and auditors by CLUSIF (Club de la securité de l’information français), based in Paris, France. The latest version (2010) is aligned with ISO27002.
- The Standard of Good Practice for Information Security (2013) from the Information Security Forum (ISF), founded in 1989, is a practical 372-page book that addresses information security from a business perspective.

COBIT 5

INFORMATION SECURITY

- The ISO 27000 series consists of a large number of standards of which two: ISO/IEC 27001 and ISO27002 are the main parts.
- ISO/IEC 27000: 2012. Information technology. Security techniques. Information security management systems. Overview and vocabulary.
- ISO/IEC 27001: 2013. Information technology. Security techniques. Information security management systems. Requirements.

COBIT 5

INFORMATION SECURITY

- ISO/IEC 27002: 2013. Information technology. Security techniques. Code of practice for information security management.
- ISO/IEC 27003: 2010. Information technology. Security techniques. Information security management system implementation guidance.
- ISO/IEC 27004: 2009. Information technology. Security techniques. Information security management. Measurement.

COBIT 5

INFORMATION SECURITY

- ISO/IEC 27005: 2008. Information technology. Security techniques. Information security risk management.
- ISO/IEC 27006: 2011. Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems.
- ISO/IEC 27011: 2008. Information technology. Security techniques. Information security management guidelines for telecommunications organisations based on ISO/IEC 27002.

COBIT 5

INFORMATION SECURITY

- ISO/IEC 27013: 2012. Information technology. Security techniques. Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1.
- ISO/IEC 27031: 2011. Information technology. Security techniques. Guidelines for information and communication technology readiness for business continuity.
- ISO/IEC 27032: 2012. Information technology. Security techniques. Guidelines for cybersecurity.

COBIT 5

INFORMATION SECURITY

- ISO/IEC 27033-5: 2013. Information technology. Security techniques. Network security. Securing communications across networks using Virtual Private Networks (VPNs).
- ISO/IEC 27034-1: 2011. Information technology. Security techniques. Application security. Overview and concepts.
- ISO/IEC 27035: 2011. Information technology. Security techniques. Information security incident management.

COBIT 5

INFORMATION SECURITY

- ISO/IEC 27037: 2012. Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence.
- ISO/IEC 27001 is referenced by COBIT 5 as being guidance for five of the COBIT 5 processes.

COBIT 5

ENTERPRISE ARCHITECTURE (EA)

- EA is a framework that enables business strategy to be achieved using information systems and information technology by specifying how business processes across the enterprise will be developed and standardised to use information systems and information technology.
- EA can be viewed as a set of domains. There are several enterprise architecture frameworks and each has a slightly different view of the domains, but the general principles are similar.

COBIT 5

ENTERPRISE ARCHITECTURE (EA)

Enterprise Architecture Domain	Description
Business architecture	Processes used by the business to meet its business strategy, governance and business outcomes
Application architecture	How specific applications are designed to conduct business processes and how they interact with one another
Data architecture	How the enterprise databases (or data warehouse) are organized and accessed by applications
Technical architecture	Hardware and software infrastructure including networks that supports applications and their interactions

COBIT 5

ENTERPRISE ARCHITECTURE (EA)

- Enterprise architectures commonly used are:
- TOGAF® – **T**he **O**pen **G**roup **A**rchitecture **F**ramework
- Zachman Framework for Enterprise Architecture
- CEAF – **C**ommission **E**nterprise **A**rchitecture **F**ramework
- FEA – **F**ederal **E**nterprise **A**rchitecture

COBIT 5

ENTERPRISE ARCHITECTURE (EA)

- Enterprise architectures commonly used are:
- TOGAF® – **T**he **O**pen **G**roup **A**rchitecture **F**ramework
- Zachman Framework for Enterprise Architecture
- CEAF – **C**ommission **E**nterprise **A**rchitecture **F**ramework
- FEA – **F**ederal **E**nterprise **A**rchitecture

COBIT 5

- **MATURITY ASSESSMENT**
- CMM®
- CMMI®
- ISO/IEC 15504

COBIT 5

MATURITY ASSESSMENT

- **CMM®**
- The Software Engineering Institute (SEI) at Carnegie Mellon University, having initially devised a capability maturity model in 1986 to assess software development projects for the US Department of Defense, then published in 1993 the full Capability Maturity Model (CMM®), a maturity assessment framework for assessment of software development projects.

COBIT 5

MATURITY ASSESSMENT

CMM®

- It was soon recognised by many people that the CMM® approach could be used for general business and IT process assessment and this was the approach used by ISACA to create the COBIT Maturity Model that was used for all COBIT processes up to and including COBIT 4.1.

COBIT 5

MATURITY ASSESSMENT

CMMI®

- In 2002, SEI superseded CMM® with Capability Maturity Model Integration (CMMI®) to extend to other activities, not only software development.

COBIT 5

INTERNAL CONTROLS

- Internal controls are put in place by enterprises to transmit governance policies throughout the enterprise to ensure fiduciary control of financial and accounting information, with the aim of meeting operational and profitability targets while complying with regulations.

COBIT 5

INTERNAL CONTROLS

COSO

- A framework for internal control was established in 1992 by the Committee of the Sponsoring Organisation of the Treadway Commission (COSO). The latest version is *Internal Control–Integrated Framework* (2013).
- COSO was seen as an important framework to include in COBIT when the first version of COBIT was being developed between 1991 and 1996.

COBIT 5

INTERNAL CONTROLS

SARBANES-OXLEY ACT

- The Sarbanes-Oxley Act (2002), known colloquially as SOX, was introduced in the US to control enterprise board activity following Enron and Worldcom frauds. It applies to enterprises registered on the New York Stock Exchange (NYSE) and NASDAQ Stock Market.
- Section 404 of SOX is important because it covers the assessment of internal controls on financial reporting. IT services are fundamental to the creation of financial reports and hence must have appropriate internal controls and be assessed.

COBIT 5

INTERNAL CONTROLS

- After SOX was published, ISACA produced a guide, *IT Control Objectives for Sarbanes-Oxley*, and COBIT has been recognised as the framework to use to meet SOX requirements and pass Public Company Accounting Oversight Board (PCAOB) assessment.
- **BASEL III FRAMEWORK**
- Basel III, the 2010-11 update to Basel II, is a framework for internal control systems in banking organisations. It has to be implemented between 2013 and 2018 and has banks worldwide complying with it.

COBIT 5

- **CULTURAL CHANGE ENABLEMENT**
- Cultural change enablement is a process to ensure stakeholders recognise and are committed to the need to change their culture, ethics and behaviour in order to be able to change the way the enterprise operates.
- Cultural change enablement is vital in order to successfully implement any changes to an enterprise’s business activities including changes to IT such as the desire to implement governance of enterprise IT (GEIT).

COBIT 5

CULTURAL CHANGE ENABLEMENT

The most commonly adopted approach to cultural change enablement is Kotter’s 8 Steps to Transformation:

1. Establish a sense of urgency of the need for change
2. Form a guiding coalition of stakeholders
3. Create a vision of where the enterprise wants to be
4. Communicate the vision to everyone
5. Empower people to act
6. Plan and implement quick wins
7. Consolidate improvements and make further changes
8. Institutionalise the changes

COBIT 5

- **BUSINESS CONTINUITY MANAGEMENT**
- The International Standard ISO22301:2012 (formerly a British Standard BS25999-2 published in 2007) specifies the requirements for a Business Continuity Management System (BCMS) to protect a business from disruptive incidents in addition to reducing the likelihood that such incidents might occur.
- Like other management system standards, ISO22301 uses Plan, Do, Check, Act (PDCA) as its core approach with key activities that cover business impact analysis (BIA), strategy, planning, exercising and improvement.

COBIT 5 – How they map

COBIT® Process No.	COBIT® Process Name	Related Guidance Frameworks and Standards
EDM01	Ensure Governance Framework Setting and Maintenance	COSO, ISO/IEC 38500, King III, OECD
EDM02	Ensure Benefits Delivery	COSO, ISO/IEC 38500, King III
EDM03	Ensure Risk Optimisation	COSO/ERM, ISO/IEC 31000, ISO/IEC 38500, King III
EDM04	Ensure Resource Optimisation	ISO/IEC 38500, King III, TOGAF® 9
EDM05	Ensure Stakeholder Transparency	COSO, ISO/IEC 38500, King III

COBIT 5 – How they map

COBIT® Process No.	COBIT® Process Name	Related Guidance Frameworks and Standards
APO01	Manage the IT Management Framework	ISO/IEC 20000, ISO/IEC 27002
APO02	Manage Strategy	ITIL 2011
APO03	Manage Enterprise Architecture	TOGAF® 9
APO04	Manage Innovation	None
APO05	Manage Portfolio	ISO/IEC 20000, ITIL 2011, SFIA
APO06	Manage Budget and Costs	ISO/IEC 20000, ITIL 2011
APO07	Manage Human Resources	ISO27002, SFIA
APO08	Manage Relationships	ISO/IEC 20000, ITIL 2011
APO09	Manage Service Agreements	ISO/IEC 20000, ITIL 2011
APO10	Manage Suppliers	ISO/IEC 20000, ITIL 2011, PMBOK®
APO11	Manage Quality	ISO 9001:2008
APO12	Manage Risk	ISO27001:2005, ISO/IEC 27002:2011, ISO/IEC 31000
APO13	Manage Security	ISO/IEC 27001:2005, ISO27002:2011, NIST SP800-53 Rev 1

COBIT 5 – How they map

COBIT® Process No.	COBIT® Process Name	Related Guidance Frameworks and Standards
BAI01	Manage Programmes and Projects	PMBOK®, PRINCE2
BAI02	Manage Requirements Definitions	ITIL 2011
BAI03	Manage Solutions Identification and Build	None
BAI04	Manage Availability and Capacity	ISO/IEC 20000, ITIL 2011
BAI05	Manage Organisational Change Enablement	Kotter (1996), Leading Change, Boston, Harvard Business School Press
BAI06	Manage Changes	ISO/IEC 20000, ITIL 2011
BAI07	Manage Change Acceptance and Transitioning	ISO/IEC 20000, ITIL 2011, PMBOK®, PRINCE2
BAI08	Manage Knowledge	ITIL 2011
BAI09	Manage Assets	ITIL 2011
BAI10	Manage Configuration	ISO/IEC 20000, ITIL 2011

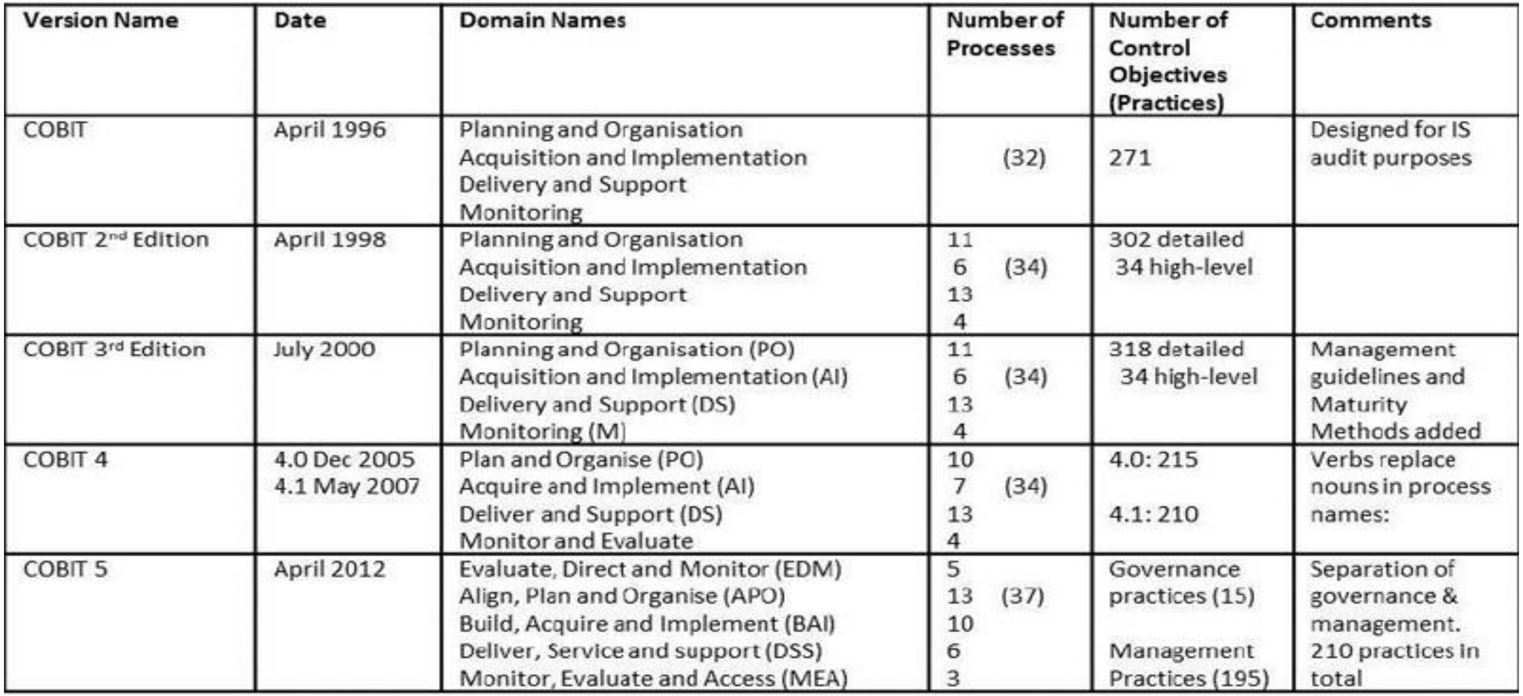
COBIT 5 – How they map

COBIT® Process No.	COBIT® Process Name	Related Guidance Frameworks and Standards
DSS01	Manage Operations	ITIL 2011
DSS02	Manage Service Requests and Incidents	ISO/IEC 20000, ISO27002, ITIL 2011
DSS03	Manage Problems	ISO/IEC 20000, ITIL 2011
DSS04	Manage Continuity	BS 25999-2007 (now ISO22301:2012), ISO/IEC 27002:2011, ITIL 2011
DSS05	Manage Security Services	ISO/IEC 27002:2011, NIST SP800-53 Rev 1, ITIL 2011
DSS06	Manage Business Process Controls	None
MEA01	Monitor, Evaluate and Assess Performance and Conformance	ISO/IEC 20000, ITIL 2011
MEA02	Monitor, Evaluate and Assess the System of Internal Controls	None
MEA03	Monitor, Evaluate and Assess Compliance with External Requirements	None

COBIT 5

- COBIT was initially developed as an IT audit framework and in today’s view of history is seen as moving over 16 years from IT audit (COBIT 1) to IT control (COBIT 2) to IT management (COBIT 3) to IT governance (COBIT 4.0/4.1) to governance of enterprise IT (GEIT) (COBIT 5). The table in the next slide is a comparison of the versions of COBIT since 1996.

Comparisons of Versions of COBIT® Since 1996



Version Name	Date	Domain Names	Number of Processes	Number of Control Objectives (Practices)	Comments
COBIT	April 1996	Planning and Organisation Acquisition and Implementation Delivery and Support Monitoring	(32)	271	Designed for IS audit purposes
COBIT 2nd Edition	April 1998	Planning and Organisation Acquisition and Implementation Delivery and Support Monitoring	11 6 (34) 13 4	302 detailed 34 high-level	
COBIT 3rd Edition	July 2000	Planning and Organisation (PO) Acquisition and Implementation (AI) Delivery and Support (DS) Monitoring (M)	11 6 (34) 13 4	318 detailed 34 high-level	Management guidelines and Maturity Methods added
COBIT 4	4.0 Dec 2005 4.1 May 2007	Plan and Organise (PO) Acquire and Implement (AI) Deliver and Support (DS) Monitor and Evaluate	10 7 (34) 13 4	4.0: 215 4.1: 210	Verbs replace nouns in process names:
COBIT 5	April 2012	Evaluate, Direct and Monitor (EDM) Align, Plan and Organise (APO) Build, Acquire and Implement (BAI) Deliver, Service and support (DSS) Monitor, Evaluate and Access (MEA)	5 13 (37) 10 6 3	Governance practices (15) Management Practices (195)	Separation of governance & management. 210 practices in total

COBIT 5

- A major factor that all committees responsible for international standards and frameworks recognise is that about every five years, they need to review their international standard or framework to take into account developments in the world.
- **WHAT COBIT 5 ADDRESSES**
- ISACA decided its next generation of guidance covered by COBIT 5 should cover the governance and management of enterprise IT.

COBIT 5

- To ensure the delivery of enterprise IT is fully engaged with the business to ensure core business expectations are achieved:
- Value creation
- Business user satisfaction
- Regulatory and contractual compliance

COBIT 5

- **KEY IDEAS OF COBIT 5**
- COBIT 5 is based simply on two concepts:
- Five principles
- Seven enablers

COBIT 5 -THE FIVE PRINCIPLES

- The five principles explain exactly what COBIT 5 has been designed to achieve:
- 1. Meeting stakeholder needs
- 2. Covering the enterprise end-to-end
- 3. Applying a single integrated framework
- 4. Enabling a holistic approach
- 5. Separating governance from management

COBIT 5 -THE FIVE PRINCIPLES

Meeting stakeholder needs

- Stakeholders are both internal and external.
- Internal stakeholders are roles given to members of the enterprise and range across the levels of the enterprise and include:
- the board; CEO; CFO; business executives and managers; risk, security and audit managers; IT managers; and users.

COBIT 5 -THE FIVE PRINCIPLES

1. ***Meeting stakeholder needs***

- External stakeholders are not members of the enterprise and roles include, but are not limited to:
- shareholders, business partners, suppliers, regulatory officials, external auditors and customers.

COBIT 5 -THE FIVE PRINCIPLES

1. ***Meeting stakeholder needs***

- Enterprises are expected to create value for their stakeholders and that is the reason why the key governance objective of an enterprise is value creation. Value creation is perceived as realising benefits at optimal resource costs while optimising risks.

COBIT 5 -THE FIVE PRINCIPLES

1. ***Meeting stakeholder needs***

- It is the stakeholder needs that determine what the value should be and different stakeholders have different needs. Therefore, the governance system should take into account all stakeholder needs when making decisions.

COBIT 5 -THE FIVE PRINCIPLES
2. ***Covering the enterprise end-to-end***

- It is universally recognised that IT is a fundamental part of running an enterprise and realising benefits. It has always been recognised that the board and executive management are responsible for finance and human resource governance and now enterprise governance of IT.

COBIT 5 -THE FIVE PRINCIPLES
2. ***Covering the enterprise end-to-end***

- The Board determines strategy, ROI, value and solvency and the Board directs by allocation of responsibility and targets to management teams in the enterprise. The CIO is responsible for controlling IT and provides policies and objectives on IT to management teams in the enterprises. Management teams in the enterprise are responsible for the delivery of performance by their business unit and IT is essential for delivery. They request new IT services to be provided and they use existing IT services, and the enabler is the IT department.

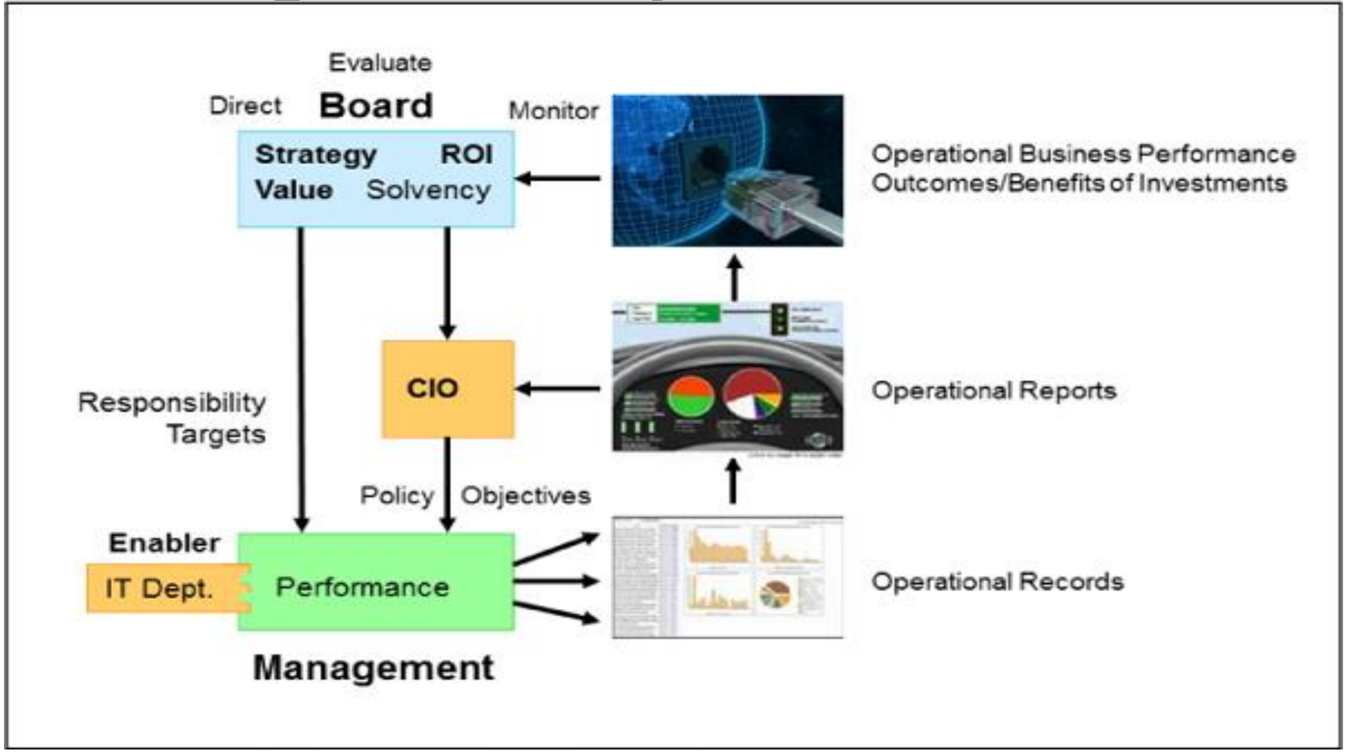
COBIT 5 -THE FIVE PRINCIPLES

2. ***Covering the enterprise end-to-end***

- Reports from management teams in the enterprise to the CIO are reports on IT services and its impact on business performance (operational records), which comes directly from IT departments as well as from management teams. The CIO then provides operational reports to the Board that indicate operational business performance and the outcome benefits of investments (i.e. from IT projects). The Board monitors these reports and evaluates and directs the management teams as necessary.

COBIT 5 -THE FIVE PRINCIPLES

2. ***Covering the enterprise end-to-end***



COBIT 5 -THE FIVE PRINCIPLES
3. ***Applying a single integrated framework***

- COBIT 5 has integrated the existing ISACA frameworks and the wide range of other standards and frameworks that are relevant to the governance of enterprise IT such as COSO, ISO etc. In that sense ISACA sees COBIT 5 as a single integrated framework that is a ‘consistent and integrated source of guidance in a non-technical, technology-agnostic common language

COBIT 5 -THE FIVE PRINCIPLES

4. ***Enabling a holistic approach***

- The holistic approach to delivering governance and management of enterprise IT is to implement enablers. COBIT 5 recognises the need for seven categories of enablers:

COBIT 5 -
4. ***Enabling a holistic approach***

The Seven Enablers:

- 1. Principles, policies and frameworks
- 2. Processes
- 3. Organisational structures
- 4. Culture, ethics and behaviour
- 5. Information
- 6. Services, infrastructure and applications
- 7. People, skills and competencies

Collectively, the final three enablers (5, 6 and 7) are enterprise resources.

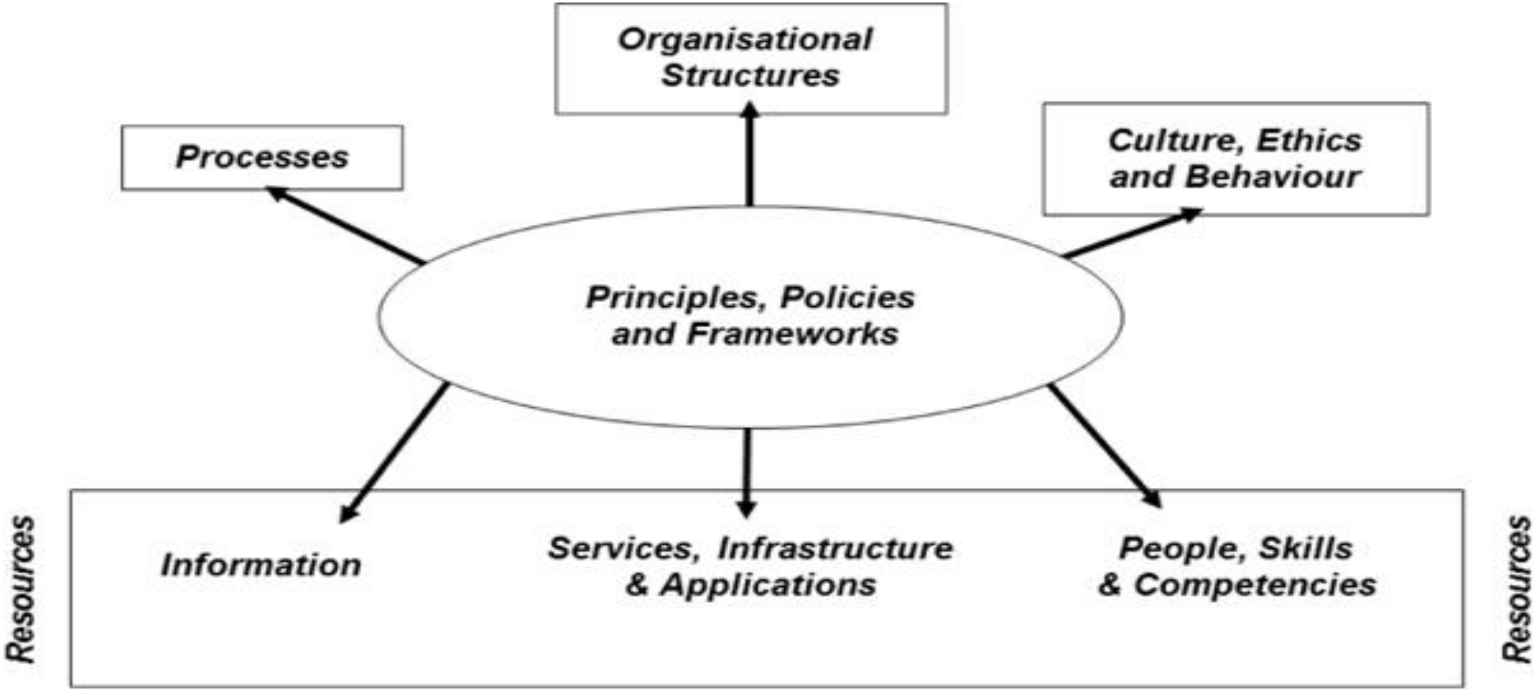
COBIT 5 – THE SEVEN ENABLERS

4. ***Enabling a holistic approach***

- The illustration on the next slide shows the 7 Enablers and is derived from *COBIT 5: A business framework for the governance and management of enterprise IT.*

COBIT 5 -THE FIVE PRINCIPLES

4. ***Enabling a holistic approach***


Organisational Structures
Processes
Culture, Ethics and Behaviour
Principles, Policies and Frameworks
Resources
Information
Services, Infrastructure & Applications
People, Skills & Competencies
Resources

COBIT 5 -THE SEVEN ENABLERS

5: Separating governance from management

- The COBIT 5 framework adheres to the principle of corporate governance that governance and management are separate, or put more specifically they are distinct but communicate.

COBIT 5 -THE SEVEN ENABLERS

5: Separating governance from management

COBIT 5 defines governance as:

‘**Governance** ensures that stakeholder needs, conditions and options are evaluated to determine:

- balanced, agreed-on enterprise objectives to be achieved;
- setting direction through prioritisation and decision making;
- and monitoring performance and compliance against agreed-on direction and objectives.’

COBIT 5 -THE SEVEN ENABLERS

5: Separating governance from management

COBIT 5’s view is that governance is the responsibility of the board of directors with leadership from the chairperson. In reality, the board of directors is accountable for governance.

Note that although the board of directors retains accountability for governance it is perfectly acceptable for them to appoint an IT Strategy Committee (sometimes called IT Steering Committee) to be responsible for governance.

COBIT 5 -THE SEVEN ENABLERS
5: Separating governance from management

COBIT 5 defines management as:

- ‘**Management** plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.’

COBIT 5 -THE SEVEN ENABLERS
5: Separating governance from management

COBIT 5’s view is that management is the responsibility of executive management under the leadership of the CEO.

Executive management (*aka* senior management) is immediately beneath the board of directors and is responsible for the day-to-day activities of the enterprise and is usually led by the CEO who is often also an internal member of the board of directors.

COBIT 5 -THE SEVEN ENABLERS
5: Separating governance from management

To recap governance is about evaluation, direction and monitoring and this requires interaction with management that plans, builds, runs and monitors the enterprise activities.

The processes that cover governance and management are described in the COBIT 5 Process Reference Model (PRM) –.

The PRM provides 37 processes and separates these into governance and management areas.

COBIT 5 -THE SEVEN ENABLERS

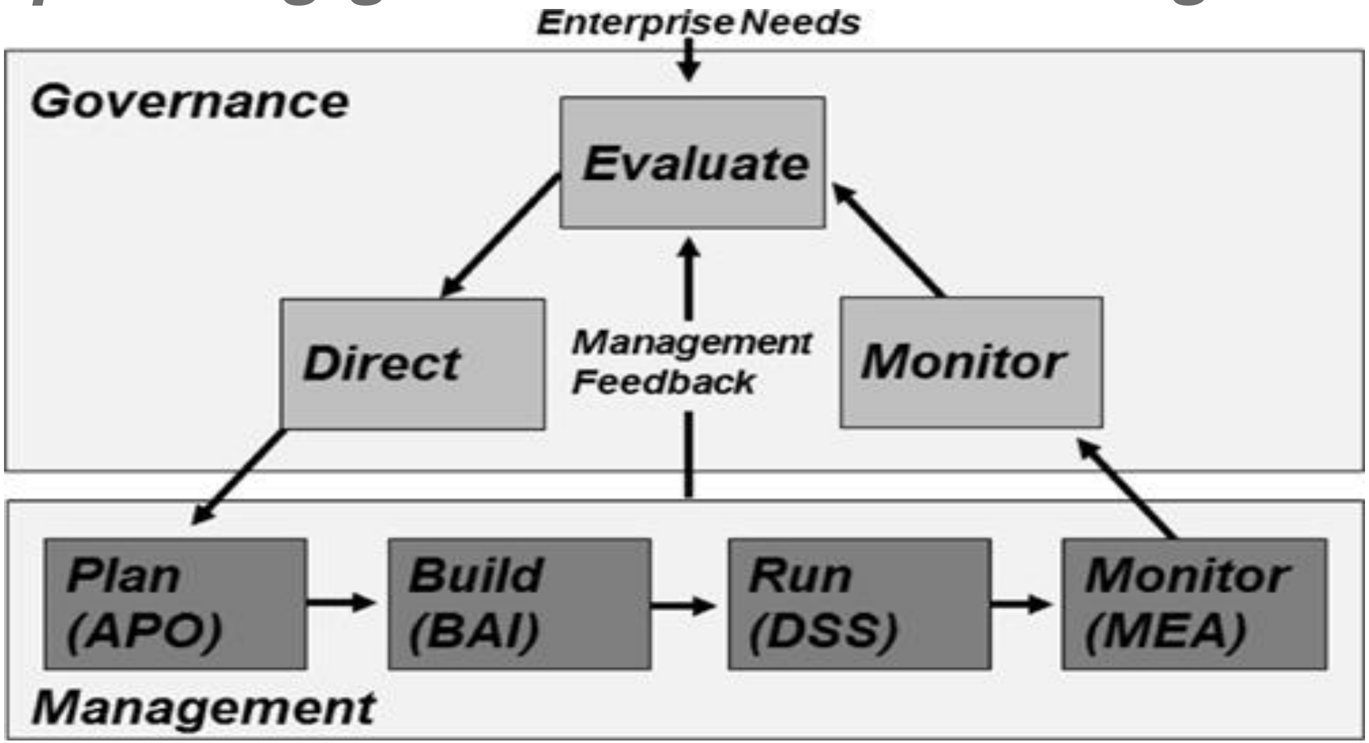
5: Separating governance from management

Overall there are five domains:

- **Governance**: the single domain Evaluate, Direct and Monitor (EDM) consisting of five processes.
- **Management**: four domains
- Align, Plan and Organise (APO) consisting of 13 processes
- Build, Acquire and Implement (BAI) consisting of 10 processes
- Deliver, Service and Support consisting of 6 processes
- Monitor, Evaluate and Assess (MEA) consisting of 3 processes

COBIT 5 -THE SEVEN ENABLERS

5: Separating governance from management

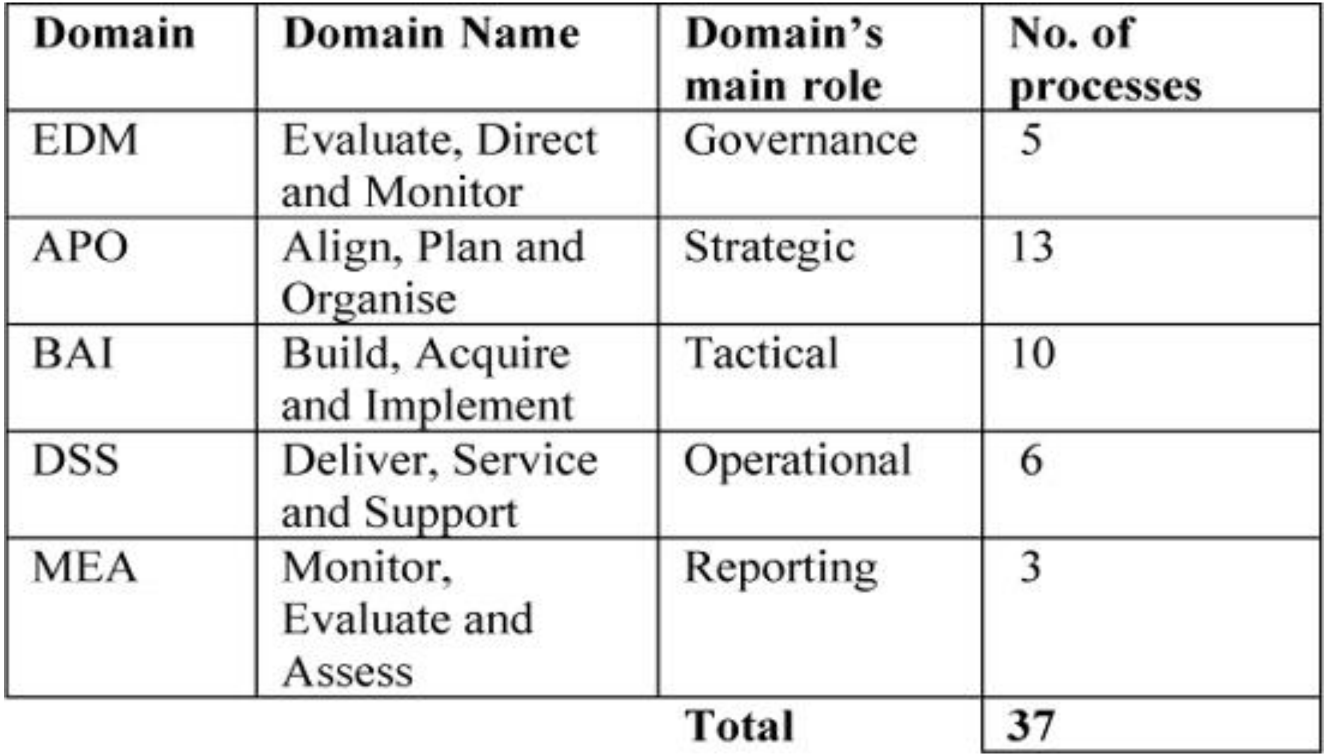


COBIT 5 - Process Reference Model (PRM)

COBIT 5 has 37 processes in five domains.

- The governance domain: Evaluate, Direct and Monitor (EDM), has five processes.
- The four management domains:
- Align, Plan and Organise (APO);
- Build, Acquire and Implement (BAI);
- Deliver, Service and Support (DSS); and
- Monitor, Evaluate and Assess (MEA), have the remaining 32 processes.

COBIT 5 - Process Reference Model (PRM)



Domain	Domain Name	Domain's main role	No. of processes
EDM	Evaluate, Direct and Monitor	Governance	5
APO	Align, Plan and Organise	Strategic	13
BAI	Build, Acquire and Implement	Tactical	10
DSS	Deliver, Service and Support	Operational	6
MEA	Monitor, Evaluate and Assess	Reporting	3
		Total	**37**

COBIT 5 - **AN EXAMPLE OF A GOVERNANCE PROCESS**

- **Process Number:** *EDM01*
- **Process Name:** *Ensure Governance Framework Setting and Maintenance*
- **Area:** *Governance*
- **Domain:** *Evaluate, Direct and Monitor*

COBIT 5 - **AN EXAMPLE OF A GOVERNANCE PROCESS**

- **Process Description:** *Analyse and articulate the governance of enterprise IT, and put in place and maintaineffective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission goals and objectives.*

COBIT 5 - **AN EXAMPLE OF A GOVERNANCE PROCESS**

- **Process Purpose Statement:** *Provide a consistent approach integrated and aligned with the enterprise governance approach. To ensure that IT-related decisions are made in line with the enterprises' strategies and objectives, ensure the IT-related processes are overseen effectively and transparently, compliance with legal and regulatory requirements is confirmed and the governance requirements for board members are met.*

COBIT 5 - **AN EXAMPLE OF A GOVERNANCE PROCESS**

- **IT-related Goals:** Appropriate IT-related goals
- **Related Metrics:** Three or four metrics for measuring achievement of each IT-related goal.
- **Process Goals:** Called process goals (three), but effectively these are the process outcomes.
- **Related Metrics:** Two or three metrics for measuring achievement of each process goal.
- **RACI Chart:** The governance practices are defined and numbered using decimal points:

COBIT 5 - **AN EXAMPLE OF A GOVERNANCE PROCESS**

- *EDM01.01 Evaluate the governance system*
- *EDM01.02 Direct the governance system*
- *EDM01.03 Monitor the governance system.*
- A RACI chart is provided that shows for each of these governance practices who is responsible, accountable, consulted or informed. Only one role is accountable for each governance practice. (Roles would be CEO, CIO CFO, VPs Directors etc.).

COBIT 5 - **AN EXAMPLE OF A MANAGEMENT PROCESS**

- **Process Number:** *DSS02*
- **Process Name:** *Manage Service Requests and Incidents*
- **Area:** *Management*
- **Domain:** *Deliver, Service and Support*

COBIT 5 - **AN EXAMPLE OF A MANAGEMENT PROCESS**

- **Process Description:** *Provide timely and effective response to user requests and resolution of all types of incidents. Restore normal service, record and fulfil user requests; and record, investigate, diagnose, escalate and resolve incidents.*
- **Process Purpose Statement:** *Achieve increased productivity and minimise disruptions through quick resolutions of user queries and incidents.*

COBIT 5 - **AN EXAMPLE OF A MANAGEMENT PROCESS**

- **IT-related Goals:** Appropriate IT-related goals.
- **Related Metrics:** Three or four metrics for measuring achievement of each IT-related goal.
- **Process Goals:** Called process goals (three), but effectively these are the process outcomes.
- **Related Metrics:** One or two metrics for measuring achievement of each process goal.
- **RACI Chart:** The management practices are defined and numbered.

COBIT 5 - **AN EXAMPLE OF A MANAGEMENT PROCESS**

- DSS02.01 Define incident and service request classification schemes
- DSS02.02 Record, classify and prioritise requests and incidents
- DSS02.03 Verify, approve and fulfil service requests
- DSS02.04 Investigate, diagnose and allocate incidents
- DSS02.05 Resolve and recover from incidents
- DSS02.06Close service requests and incidents
- DSS02.07Track status and produce reports

COBIT 5 - **AN EXAMPLE OF A MANAGEMENT PROCESS**

- **IT-related Goals:** Appropriate IT-related goals.
- **Related Metrics:** Three or four metrics for measuring achievement of each IT-related goal.
- **Process Goals:** Called process goals (three), but effectively these are the process outcomes.
- **Related Metrics:** One or two metrics for measuring achievement of each process goal.
- **RACI Chart:** The management practices are defined and numbered.

FRAMEWORKS AND STANDARDS TRENDS

- Business requirements and practices vary significantly around the world, as do the political interests of many of the organizations creating standards.
- It is not likely that a single set of frameworks and standards will appear in the near future to cover everyone’s needs.
- The complexity of mapping hundreds of authority documents from regulations (international, national, local/state, and so on) and standards (ISO, industry-specific, vendor, and so on) created an opportunity and market niche.

FRAMEWORKS AND STANDARDS TRENDS

- Technology vendors rightfully identified this important market niche, or differentiator, to boost product sales by identifying how to get their products to address authority requirements. Vendors jumped at the opportunity to map their capabilities to address specific controls from multiple regulations and standards.
- Network Frontiers is perhaps the best-known company that attempted the impossible: to create a common mapping of IT controls across every known regulation, standard, and best practice available. The result is called the IT Unified Compliance Framework, and it can be found at www.unifiedcompliance.com.
- .

FRAMEWORKS AND STANDARDS TRENDS

- Subsequently, these mappings were adopted by Archer Technologies, Microsoft, Computer Associates, McAfee, and several other vendors to help bridge the alignment of the controls managed or tracked by the vendors with the requirements of individual authority documents.
- One viewpoint suggests a single adopted framework would simplify technology product development, organizational structures, and control objectives. The other viewpoint suggests that the complexity of disparate regional, political, business, cultural, and other interests ensures a universally accepted control framework will never be created.

FRAMEWORKS AND STANDARDS TRENDS

- The truth probably rests somewhere in the middle. Although a single set of international standards isn’t imminent, the tools described in this chapter are nonetheless serving to create reliable, secure, and sustainable technology infrastructures that ultimately benefit the participants.