DATA PROTECTION
Policy, Law, Regulations & Standards

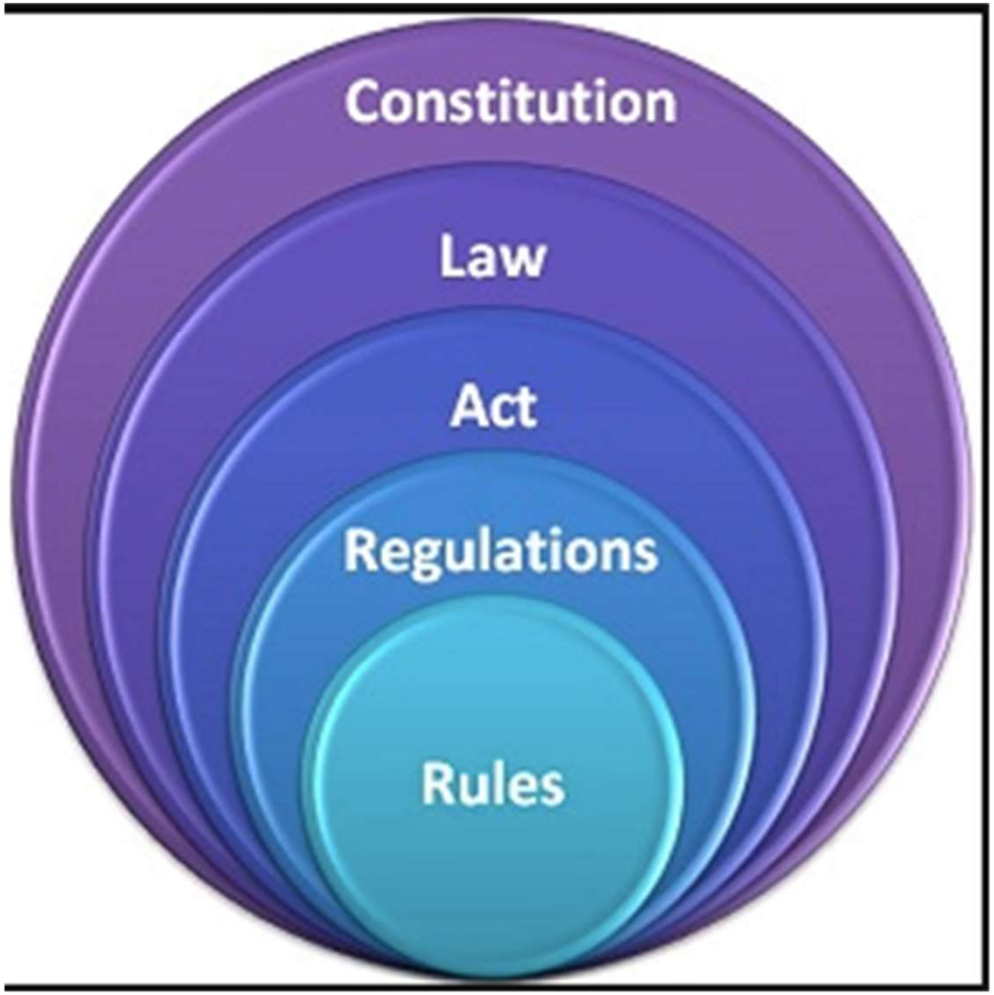
By: Mr. J. Walubengo, MSc, CISA
Lecturer, MMU /ICT Consultant,

Member: KE-Data Protection Taskforce
Walu.John@gmail.com

Summary

- The Privacy & Data Protection Policy
  - Rationale for the Policy/Bill
  - Key Principles & Influences
- The Law(Bill) & Regulations
  - Key Influences
  - Key Areas of the Bill
  - Key Implications for Enterprises
  - Potential Challenges
- The Standards (ISO, COSO, ITIL, COBIT)
- Conclusions
- Q&A

Laws, Act, Regulation, Standards:-Linkages



The Privacy & Data Protection Policy

Policy (Defns)

- A Policy is: A guiding principle designed to influence decisions, actions, etc. Typically, a policy designates a required process or procedure within an organization
- A Policy is: a deliberate system of principles to guide decisions and achieve rational outcomes
- A Policy is: a statement of management intent, implemented through procedures or protocols.

Target Levels /Scope

- Policies can have different levels of scope:
  - International (treaty, legal)
  - Regional (treaty, legal)
  - National (Policy, Legislative, Regulation)
  - Organizational (Policy, Procedure, Standard)

Rational for Privacy Policy & Bill

- The rational for the bill arises from the KE Constitutional requirement for privacy.
- Article 31 of the Constitution of Kenya 2010 recognizes the right to privacy.
- The Bill aims at giving effect the right to privacy and particularly Clauses 31 (c) and (d), by setting out the requirements for the protection of personal data processed by both public and private entities, as a facet to the right to privacy.

Rational for Privacy Policy & Bill

The 2010 KE Constitution provides that:-

- *"Every person has the right to privacy, which includes the right not to have—*
- *a) Their person, home or property searched;*
- *b) Their possessions seized;*
- *c) Information relating to their family or private affairs unnecessarily required or revealed; or,*
- d*The privacy of their communications infringed*

The Data Subject(Citizen) Rights

- Right to access to personal information;
- Right to information as to whether personal data is being processed;
- The right to rectification if the information held is inaccurate or incomplete or requires to be updated;
- The right to restrict processing of their personal data;

The Data Subject(Citizen) Rights

- The right to object decisions solely based on automated processing circumstances (AI) which produces legal effects or significantly affects data subject;
- The right to complain (as would be appropriate to the controller, processor or regulator).
- The right to object the processing of their data for direct-marketing purposes;
- The right to data portability;

The Data Subject(Citizen) Rights

- The right to object decisions solely based on automated processing circumstances (AI) which produces legal effects or significantly affects data subject;
- The right to complain (as would be appropriate to the controller, processor or regulator).
- The right to object the processing of their data for direct-marketing purposes;
- The right to data portability;

The Data Subject (Citizen) Rights

- The right to be forgotten/ the right to erasure will require mechanisms to be put in place to ensure this right;
- The Right to appropriate security safeguards where personal data is being archived for various purposes;
- The right to appropriate security safeguards in cross border transfer of personal data; and
- The right of the data subject can withdraw their consent at any time without detriment to their interests

The Data Controller/Processor Obligations

- Inform the data subject about the data processing activities and the rights of data subject under the law;
- Specify the purposes for which data is to be used;
- Should only collect and use personal data in accordance with lawful conditions;
- Should keep updated Records of Processing activities, making them available to the Office of the Data Protection Regulator and to the data subject on request;

The Data Controller/Processor Obligations

- Rely on consent as a condition for processing personal data only where: The data controller first obtain the data subject's specific, informed and freely given consent;
- Notify the regulator and data subject of any data breach;
- Register with the data protection regulator ;
- Designate a Data Protection Officer to handle all matters of data protection;

The Data Controller/Processor Obligations

- Conduct data protection impact assessment
- Develop internal data protection policies and procedures;
- Provide privacy notices/notifications to data subject before personal data is collected or used
- Ensure that the processor or any person acting under the authority of the controller or of the processor, shall not process personal data except on instructions from the controller

The Key Principles

- a) Fairness and lawfulness
- b) Restriction to a specific purpose
- c) Transparency
- d) Data minimization
- e) Storage Limitation
- f) Factual accuracy; up-to-date data
- g) Confidentiality and data security
- h) Accountability

The Key Principles

- Fairness and lawfulness
  - When processing personal data, the individual rights of the data subjects must be protected.
  - Personal data must be collected and processed in a legal and fair manner and have a legal or legitimate basis for the processing.
- Restriction to a specific purpose
  - Personal data can be processed only for the purpose that was defined before the data was collected. Subsequent changes to the purpose are only possible to a limited extent and require substantiation

The Key Principles

- Transparency
  - The data subject must be informed of how their data is being handled. In general, personal data must be collected directly from the individual concerned. When the data is collected, the data subject must either be aware of, or informed of:
  - The identity of the data controller
  - The purpose of data processing
  - Third parties or categories of third parties to whom the data might be transmitted

The Key Principles

- Data minimization
  - Before processing personal data, you must determine whether and to what extent the processing of personal data is necessary in order to achieve the purpose for which it is undertaken.
  - Where the purpose allows and where the expense involved is in proportion with the goal being pursued, anonymized or statistical data must be used.
  - Personal data may not be collected in advance and stored for potential future purposes unless required or permitted by law.

The Key Principles

- Storage Limitation
  - Personal data that is no longer needed after the expiration of legal or business process-related periods must be deleted.
  - There may be an indication of interests that merit protection or historical significance of this data in individual cases.
  - If so, the data must remain on file until the interests that merit protection have been clarified legally, or the corporate archive has evaluated the data to determine whether it must be retained for historical purposes.
- Factual accuracy; up-to-date data
  - Personal data on file must be correct, complete, and if necessary, kept up to date. Suitable steps must be taken to ensure that inaccurate or incomplete data are deleted, corrected, supplemented or updated.

The Key Principles

- Confidentiality and data security
  - Personal data is subject to data secrecy.
  - It must be treated as confidential on a personal level and secured with suitable organizational and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification or destruction.
- Accountability
  - All data controllers or data processors shall be responsible for personal data protection, and be able to demonstrate compliance to the data protection principles.

The Law(Bill) & Regulations

Key Influences

- The National Assembly Bill largely influenced by other similar legislative and regulatory frameworks including
- EU Convention 108+
- GDPR
- African Countries with similar legislation (Ghana, Mauritius, SA,etc)

Location of Bill(s)

- The Bill (National Assembly) can be found at
  - https://drive.google.com/file/d/1jJLX4IQYbmJxG4TH3tk3YutYl91q-ljG/view

- Another similar bill by Senate can be found at
  - http://www.parliament.go.ke/sites/default/files/2017-05/Data_Protection_Bill_2018.pdf

Data Protection Bill

- **PART I** of the Bill provide for preliminaries and sets out the objects and purposes of the Bill.

- **PART II** establishes the Office of the Data Commissioner, provides for the appointment, qualifications, functions, powers, removal of the Data Commissioner.

Data Protection Bill

- **PART III** provides for the registration of both data controllers and data processors.
  - It outlines the application procedure including necessary thresholds and exemptions,
  - duration of the license, cancellation of the registration, periodic audits by the Data Commissioner and
  - possibilities for the designation of the data protection officer.

Data Protection Bill

- **PART IV** outlines the principles for the processing of personal data.
  - the rights of data subjects and exercise of such rights, conditions for consent,
  - principle of data portability, retention and rectification of personal data,
  - data protection assessments, processing of data belonging to children and notification procedures in instances of breaches.

Data Protection Bill

- **PART V** outlines the grounds for processing of sensitive personal data including further categorization of sensitive personal data.
- **PART VI** provides for the conditions for the transfer of personal data outside Kenya and provision of safeguards prior to transfer of personal data out of Kenya.
- **PART VII** provides for the exemptions to processing of personal data & the development of a data sharing code.

Data Protection Bill

- **PART VIII** sets out enforcement provisions of how the Data Commissioner may exercise the powers granted to them under the Act.
- **PART IX** provides for financial provisions, reporting mechanism, and management of funds by the Office of the Data Commissioner.
- **PART X** provides for offences including the unlawful disclosure of personal data, general penalties and the development of codes, guidelines and regulations.

Key Areas of Bill

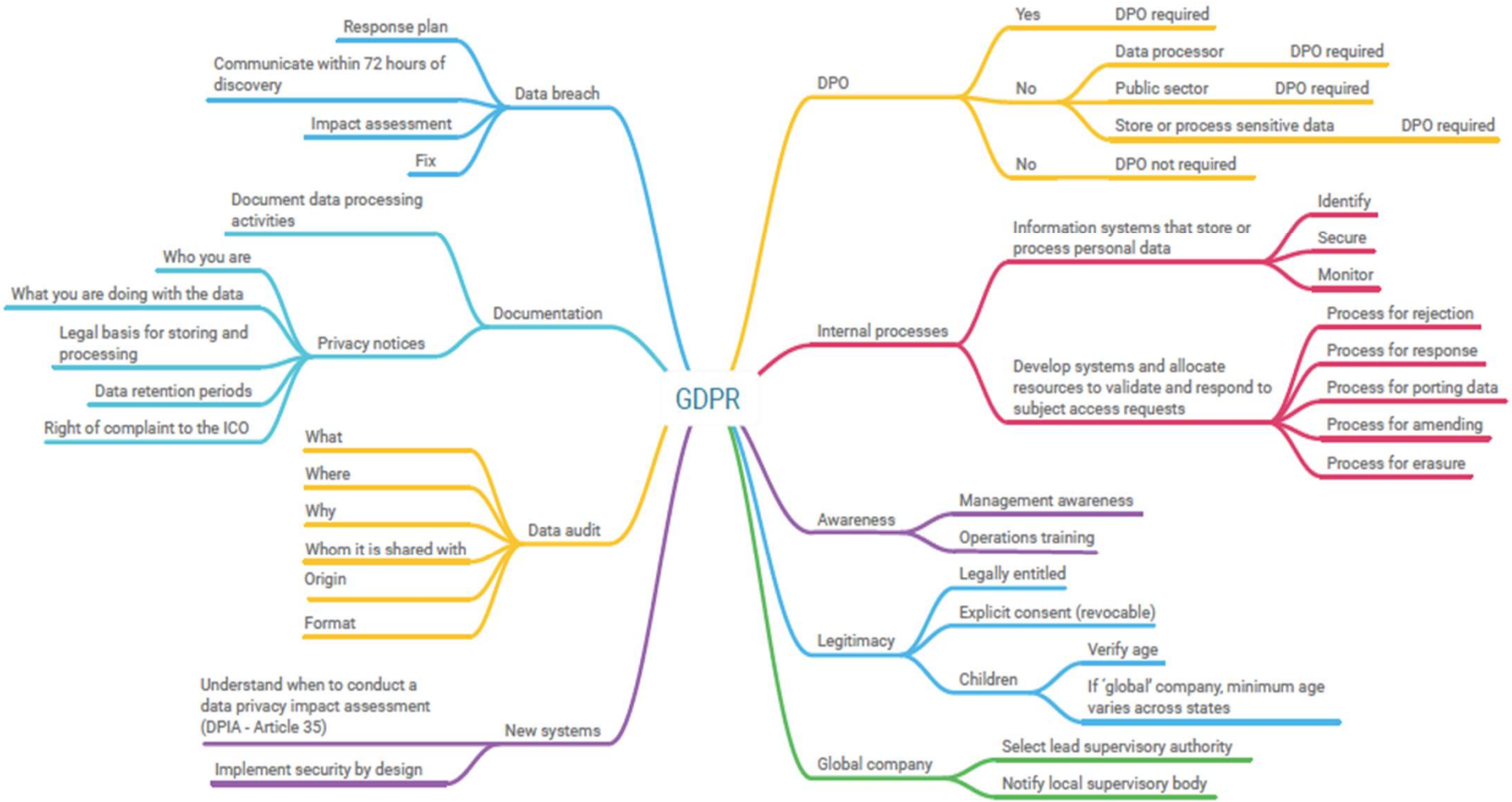
- The Principles of Data Protection
- The Rights of Data Subjects (consent, right to be forgotten, right to human review to AI logic, etc)
- The Obligations of Data Controllers and Processors (Security, Privacy, Reporting)
- Crossborder Transfers
- The Institutional /Establishment/Regulatory Framework
- Implementation Schedules

Key Implications for Enterprises

- Data Privacy & Protection By Design
  - Create inventory of Processes & their Data Life Cycle
  - Evaluate existing data processing system and establish the extent (or not) that they meet the Key Principles (Consent, Purpose, Data Minimization etc)
  - Undertake Data Protection Impact Assessments
- Appoint Data Protection Officers/Function
- Take note of Clause on Automated Processing & Data Transfers
- Take note of Breach Notifications (within 72hrs)
- General Penalties (Ksh 3M; 2yrs Imprisonment)
- Administrative Fines (Ksh 5M; 2% Annual Turnover)

How to be Ready-Key domains

FIGURE 1: Key GDPR Domains and Requirements



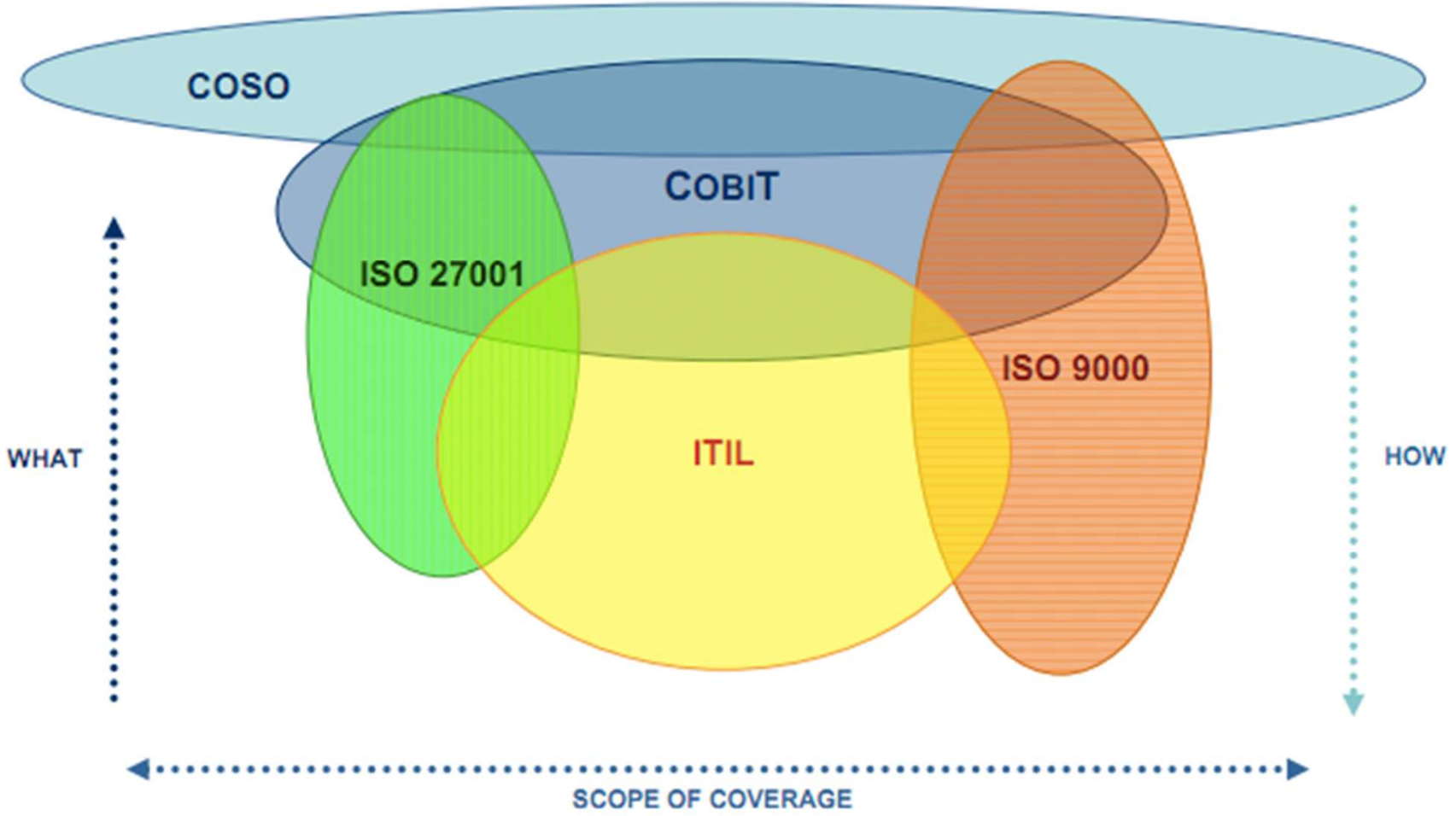
Potential Risks/Challenges

- Compliance Costs in terms of Readiness & Re-engineering processes maybe high to most SME
- Poor understanding of Data Protection Regime
  - Need for Capacity Building Required for both Data Commissioner office, Enterprises and Citizens in General
- Consider reviewing your AI/Business Intelligence modules in light of Data Protection
- Clause 50: The Cabinet Secretary may prescribe, based on grounds of strategic interests of the state or protection of revenue, certain nature of processing that shall only be effected through a server or a data centre located in Kenya.

The Standards

ISO, COSO, COBIT

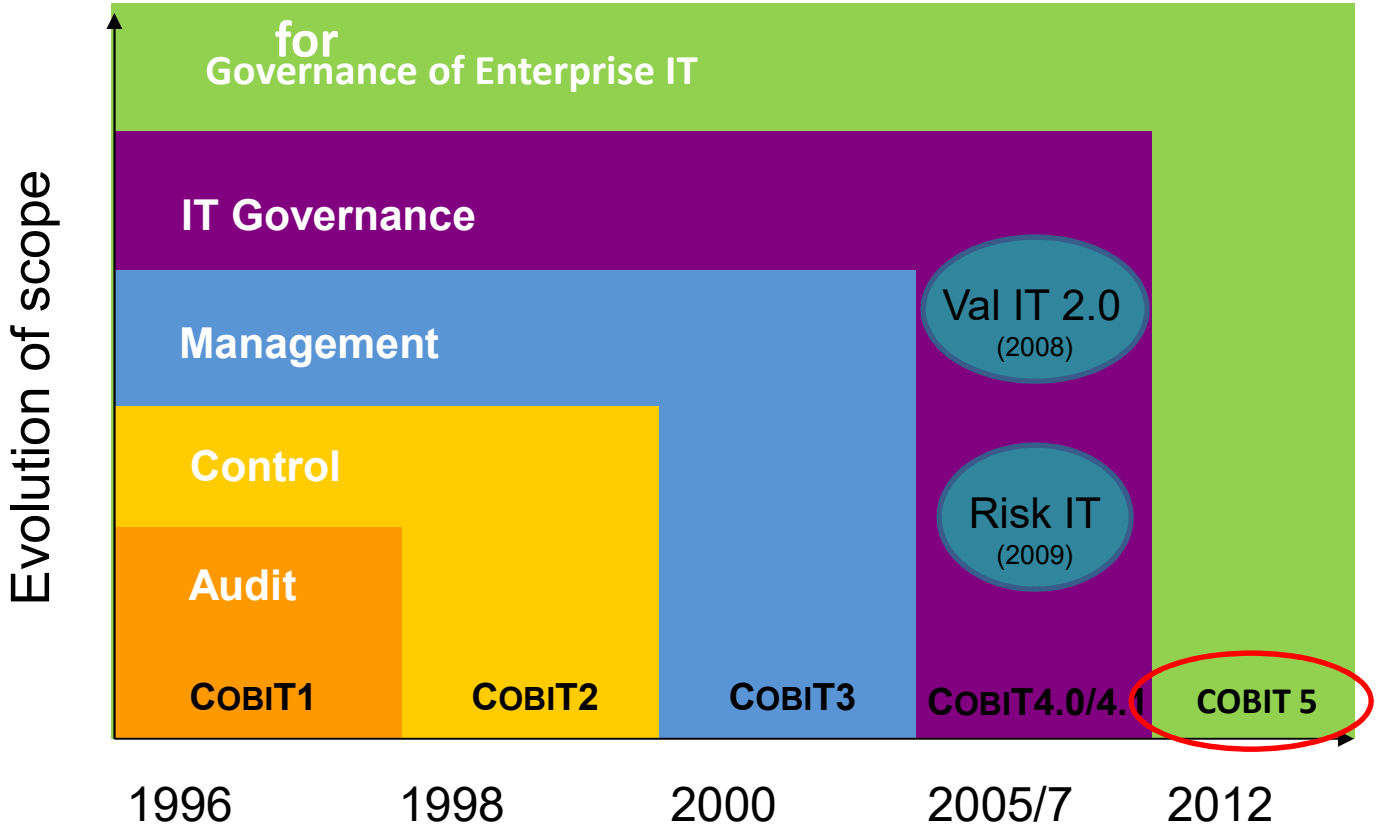
Various ICT Frameworks/Standards



COBIT® is a Road Map to Good ICT Governance

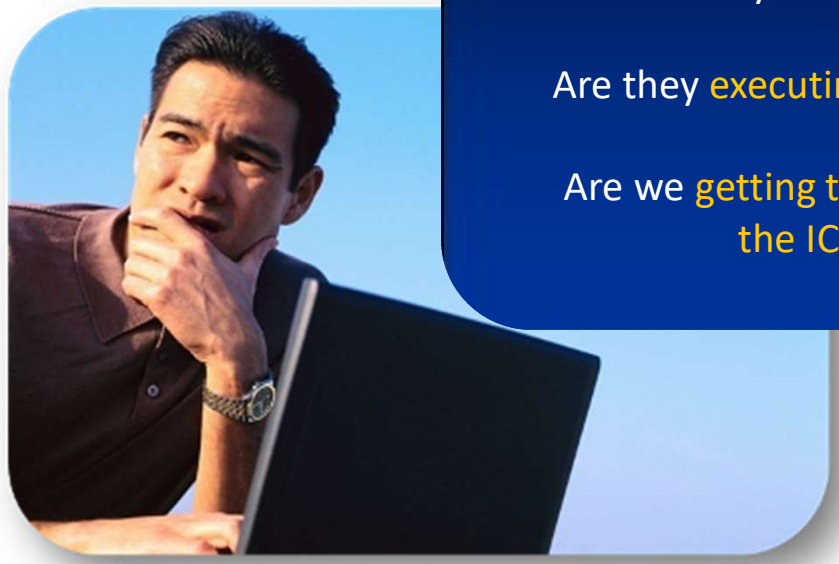
- Accepted globally as a set of tools that ensures IT is working effectively
- Functions as an overarching framework
- Provides common language to communicate goals, objectives and expected results to all stakeholders
- Based on, and integrates, industry standards and good practices in:
  - Strategic alignment of IT with business goals
  - Value delivery of services and new projects
  - Risk management
  - Resource management
  - Performance measurement

COBIT v5: Now One Complete Governance Framework



An business framework from ISACA, at www.isaca.org/cobit

COBIT® /ICT Governance provides Answers to Key Business Questions



Is the ICT Function
Dept / doing the right things?

Are they doing them the right way?

Are they executing getting them done well?

Are we getting the expected benefits from the ICT investments? *

* Based on the "Four Areas" as described by John Thorp in his book *The Information Paradox,* written jointly with Fujitsu, first published in 1998 and revised in 2003

ICT Governance Benefits

[redacted] work provides guidance for Board/ executive management to govern ICT within the enterprise

- More effective tools for ICT to support business goals
- More transparent and predictable full life-cycle ICT costs
- More timely and reliable information from ICTs
- Higher quality ICT services and more successful projects
- More effective management of ICT-related risks

Delivering Stakeholder Value

- Delivering enterprise stakeholder value requires good **governance and management** of information and technology (IT) assets.
- Organization/Enterprise Boards, executives and management have to **embrace ICTs** like any other significant part of the business.
- External **legal, regulatory and contractual compliance** requirements related to enterprise use of information and technology are increasing, threatening value if breached.
- ***An ICT Governance framework (COBIT) provides a can assist enterprises to achieve their goals and deliver value through effective governance and management of enterprise IT*.**

Conclusion

- Digitization/Automation will continue to increase at a faster pace than the rate of available protection.
- Corporates must however have ICT corporate governance mechanisms that address due diligence/ risk mitigations strategies from ICT professionals (Privacy Impact Ass.)
- Corporates must have regular and continuous Privacy, Cybersecurity trainings for employees: your corporate e-Security is only as strong as the weakest employee.

Conclusions

- At a national level, the laws may not be enough; there will be need to increase Data Protection capacities at judicial, prosecutorial and Data Commissioner levels
- There will be implementation challenges as the local data controllers, data processors and the data commissioners come to terms with the reality.

- ENDs
- Q&A