ISACA Privacy Principles and Program Management Guide Preview

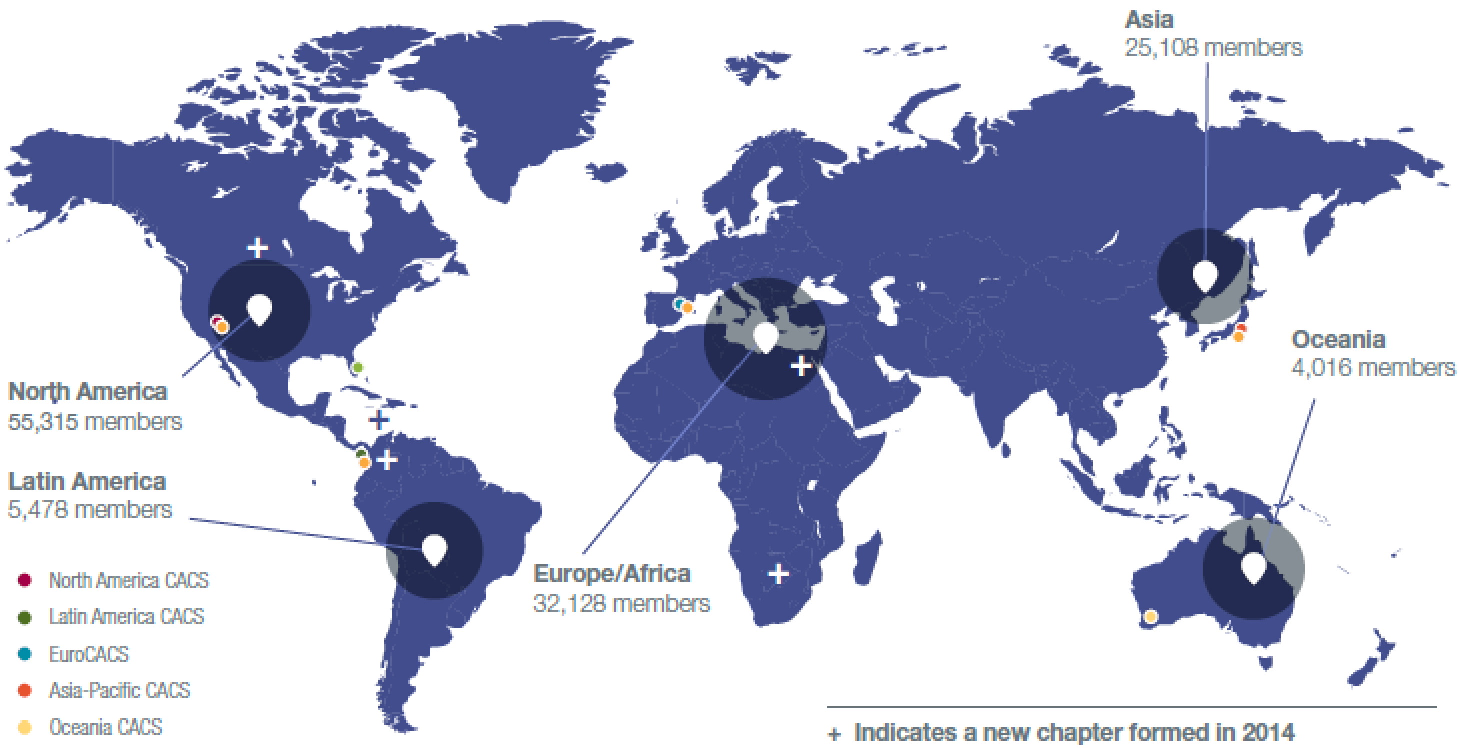
Yves LE ROUX
Principal consultant
Yves.leroux@ca.com

BUILDING TRUST
IN A HYPERCONNECTED
WORLD

Ditton Manor (near Windsor, UK)

8-9 July 2015

ca technologies



- ● North America CACS
- ● Latin America CACS
- ● EuroCACS
- ● Asia-Pacific CACS
- ● Oceania CACS
- ● Information Security and Risk Management (ISRM) Conference
- ● IT Governance, Risk and Control (ITGRC) Conference (an IIA and ISACA collaboration)

ISACA

+ Indicates a new chapter formed in 2014

Curacao

Gaborone (Botswana)

Medellin (Colombia)

Cairo (Egypt)

Regina, Saskatchewan (Canada)

122,045 members in **185** countries

207 chapters in **87** countries

35 chapters with **1,000+** members

4% membership growth

81% member retention

Privacy Guidance Task Force

- Secretary: Nancy Cohen ISACA
- Yves Le Roux, CISM, CISSP, CA Technologies, France (Chair)
- Alberto Ramirez Ayon, CISA, CISM, CRISC, Seguros Monterrey New York Life, Mexico
- Frank Cindrich, JD, CGEIT, CIPP/US, CIPP/G, PwC, USA
- Rebecca Herold, CISA, CISM, CIPM, CIPP/US, CIPP/IT, CISSP, FLMI, The Privacy Professor & SIMBUS Security and Privacy Services, USA
- Alan Lee, CISA, CISM, CISSP, CIPP/IT, Ernst & Young, Hong Kong
- John O'Driscoll, CISA, CISM, CIA, ANZ Banking Group, Australia
- Fidel Santiago, European Data Protection Supervisor, Belgium
- Roberto Soriano Domenech, CISA, CISM, CRISC, Seidor, Spain

Privacy Guidance Task Force

- Established in June 2014, in order to develop a series of practical privacy knowledge products in support of members currently responsible for managing or supporting privacy initiatives, and non-members in privacy operational roles.
- First action: realizing a survey "How enterprises are managing their Privacy function" to be published August 2015
- Second action: Elaborating a « Privacy Principles and Program Management Guide" to be published in November 2015

“How enterprises are managing their Privacy function” Survey

Who is primarily accountable for enterprise privacy?

- Chief information security officer (CISO) or chief security officer (CSO) (23percent)
- Chief privacy officer (CPO) (18percent).
- CEO (11 percent)
- CIO (11 percent)
- The privacy function has a significant or moderate level of interaction with information security for more than 90 percent of the respondents

Privacy Governance and Management

- Most commonly used frameworks are:
  - ISO/IEC 27002:2013 (50percent)
  - COBIT (43 percent)
  - EU directive 95/46 (23 percent)
  - AICPA/CICA Generally Accepted Principles (23 percent)
  - NIST SP 800-53 (22 percent)

- 75 percent of the respondents indicate that their enterprises' use of privacy policies, procedures, standards and other management approaches is mandatory,
- 19 percent indicate that their use is "recommended".

Metrics and Monitoring

- Number of privacy breaches/incidents handled is the most commonly used metric, selected by 65 percent.
- Number of privacy complaints received from customers/patients/clients,
- Number of privacy risk assessments
- Number of employees that have participated in privacy training

Top monitoring approaches:

- Privacy risk assessment
- Privacy self-assessment
- Privacy audit/assessment

Privacy Issues and Mitigation

Obstacles to Privacy Program Establishment

- Complex international legal and regulatory landscape (49percent)
- Lack of clarity on the mandate, roles and responsibilities (39 percent)
- Lack of a privacy strategy and implementation road map (37 percent)

Common type of privacy-related failure after implementation

- Lack of training or poor training (54 percent),
- Data breach/leakage
- Not performing a risk assessment

Attitudes toward Privacy Breaches

- 54 percent report that their enterprise did not experience a material privacy breach
- 32 percent are “unsure” whether such a breach had occurred
- Negative consequences of a privacy breach
  - Decline in enterprise reputation (80 percent)
  - Legal action (62 percent),
  - Regulatory action (60 percent)
  - Unfavorable media coverage (58 percent)
- 29 percent of ISACA survey respondents report that they are “very” confident in their enterprise’s ability to ensure the privacy of sensitive data
- 60 percent are only somewhat confident.
- The remaining 11 percent indicate no confidence.

ISACA Privacy Principles and Program Management Guide

What is privacy?

- No single world-wide definition of privacy
- Seven categories of privacy (from“European data protection: coming of age?” edited by Serge Gutwirth, Ronald Leenes, Paul de Hert and Yves Poullet)
  - Privacy of the person
  - Privacy of behaviour and actions
  - Privacy of communication
  - Privacy of association
  - Privacy of data and image (information)
  - Privacy of thoughts and feelings
  - Privacy of location and space (territorial)

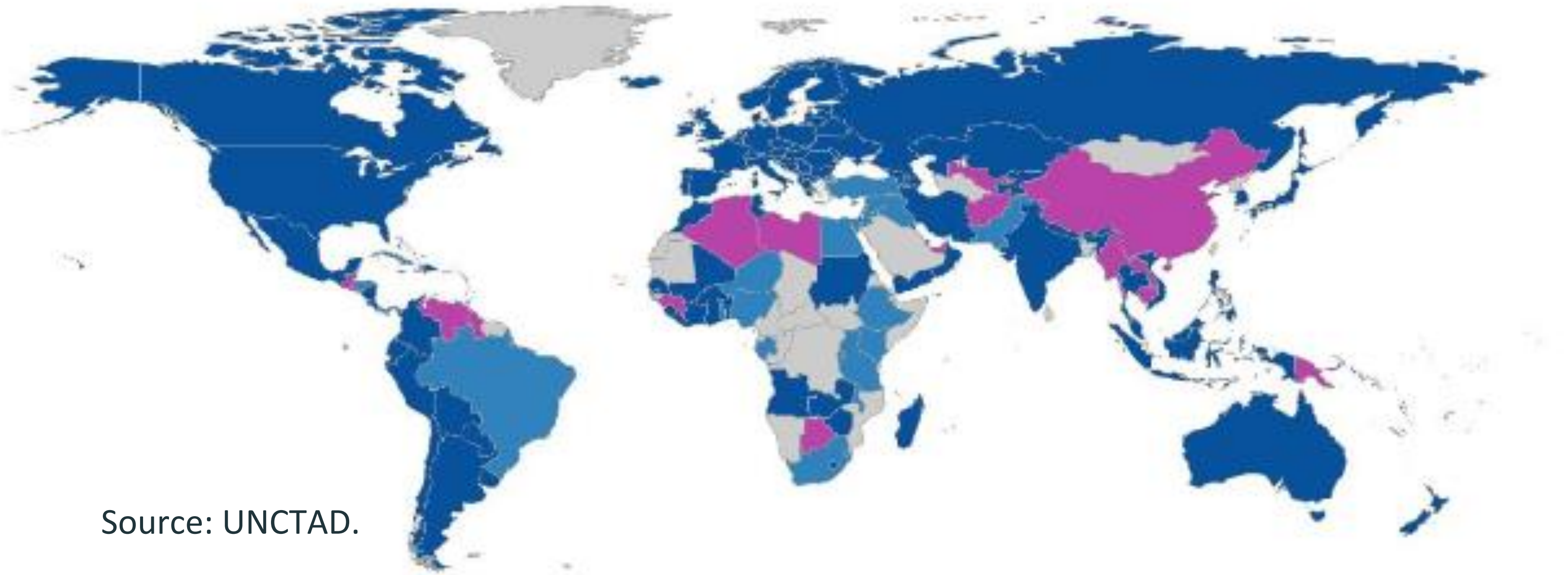
Applications of Privacy categories to relatively new technologies

- Social media
- Cloud computing
- Apps (the term most commonly used for mobile applications)
- Big Data Analytics
- Internet of Things
- BYOD (the common term used for “bring your own device” practices in organizations) including wearable technologies
- Tracking and surveillance technologies

Document structure

- Section I. Privacy Primer
  - Introduction to Privacy: A short history
  - Overview of Legal Issues for Privacy
  - Privacy Views and Concepts
  - New Privacy Risks from New Technologies
  - Other Privacy Standards and Principles
  - ISACA Privacy Principles and Descriptions
  - COBIT 5 Principles
- Section II. Using COBIT 5 Enablers for Implementing Privacy in Practice
- Section III. Adapting the ISACA Privacy Principles to the Enterprise Environment

Data Privacy legislations around the world



Source: UNCTAD.

Legend : Dark blue – countries with legislation
Light blue – countries with draft legislation
Violet – countries with no legislation
Grey – countries with no data

77 Countries are analyzed in the last
DLA Piper's Data Protection Laws of the World Handbook

BUILDING TRUST
IN A HYPERCONNECTED
WORLD

Ditton Manor (near Windsor, UK)

8-9 July 2015

Models used in data protection laws

1. Comprehensive Model

   e.g. European Union countries and the Canadian provinces

2. Sectoral Model

   e.g. United States and Japan

3. Co-Regulatory Model

   e.g. Australia, New Zealand and the Netherlands.

4. Self-Regulatory Model

   e.g. Network Advertising Initiative (NAI) Code of Conduct and North American Energy Standards Board (NAESB)

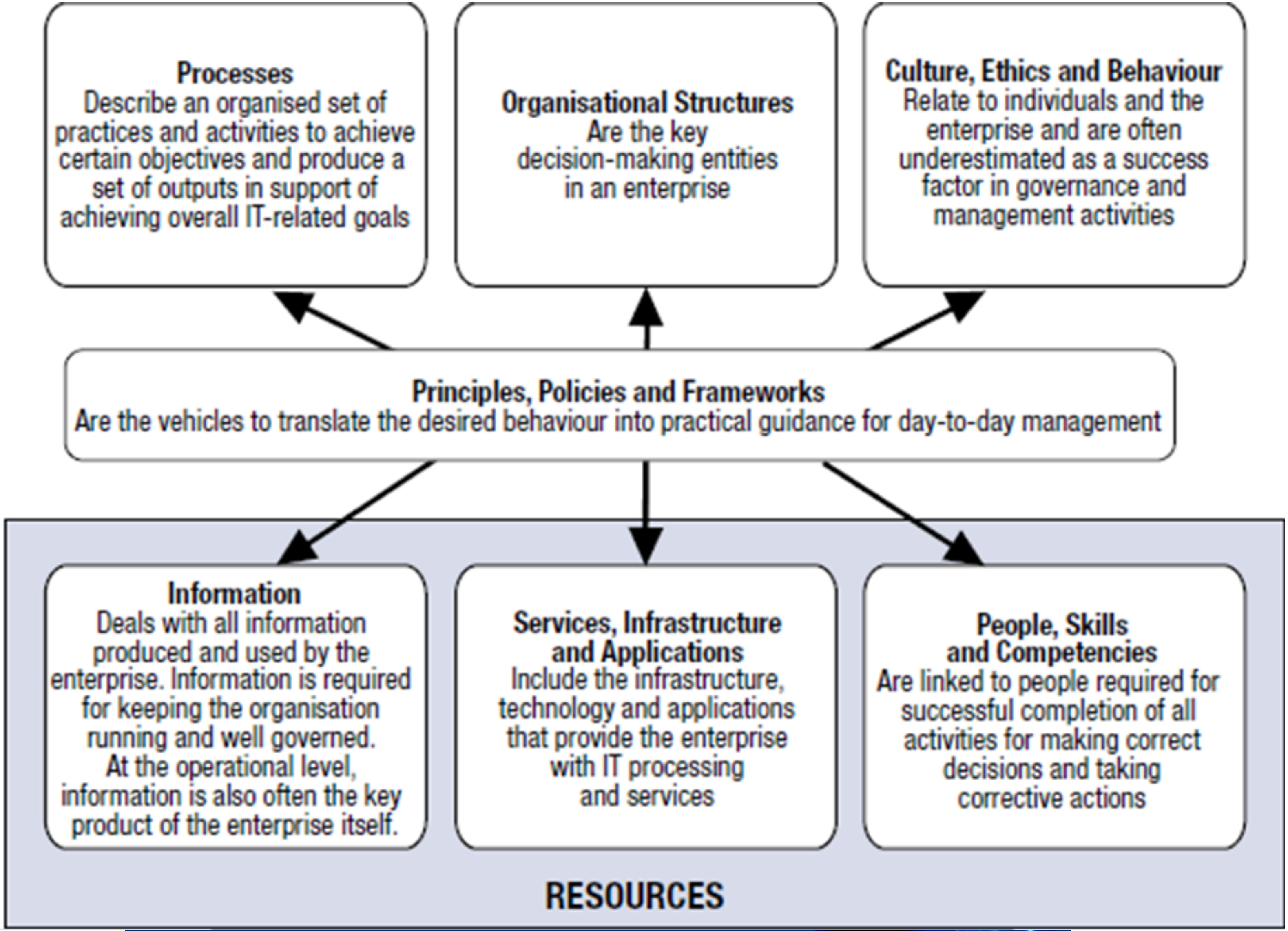
The 14 ISACA Privacy Principles 1/2

- After studying existing privacy standards, frameworks and principles, ISACA defined a uniform set of practical principles
  - Principle1: Choice and Consent
  - Principle 2: Legitimate Purpose Specification and Use Limitation
  - Principle 3: Personal information and Sensitive Information Life Cycle
  - Principle 4: Accuracy and Quality
  - Principle 5: Openness, Transparency and Notice
  - Principle 6: Individual Participation
  - Principle 7: Accountability

The 14 ISACA Privacy Principles 2/2

- Principle 8: Security Safeguards
- Principle 9: Monitoring, Measuring and Reporting
- Principle 10: Preventing Harm
- Principle 11: Third Party / Vendor Management
- Principle 12: Breach Management
- Principle 13: Security and Privacy by Design
- Principle 14: Free flow of information and legitimate restriction

COBIT 5 Enabler: Systemic model with Interacting Enablers



Processes
Describe an organised set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals

Organisational Structures
Are the key decision-making entities in an enterprise

Culture, Ethics and Behaviour
Relate to individuals and the enterprise and are often underestimated as a success factor in governance and management activities

Principles, Policies and Frameworks
Are the vehicles to translate the desired behaviour into practical guidance for day-to-day management

Information
Deals with all information produced and used by the enterprise. Information is required for keeping the organisation running and well governed. At the operational level, information is also often the key product of the enterprise itself.

Services, Infrastructure and Applications
Include the infrastructure, technology and applications that provide the enterprise with IT processing and services

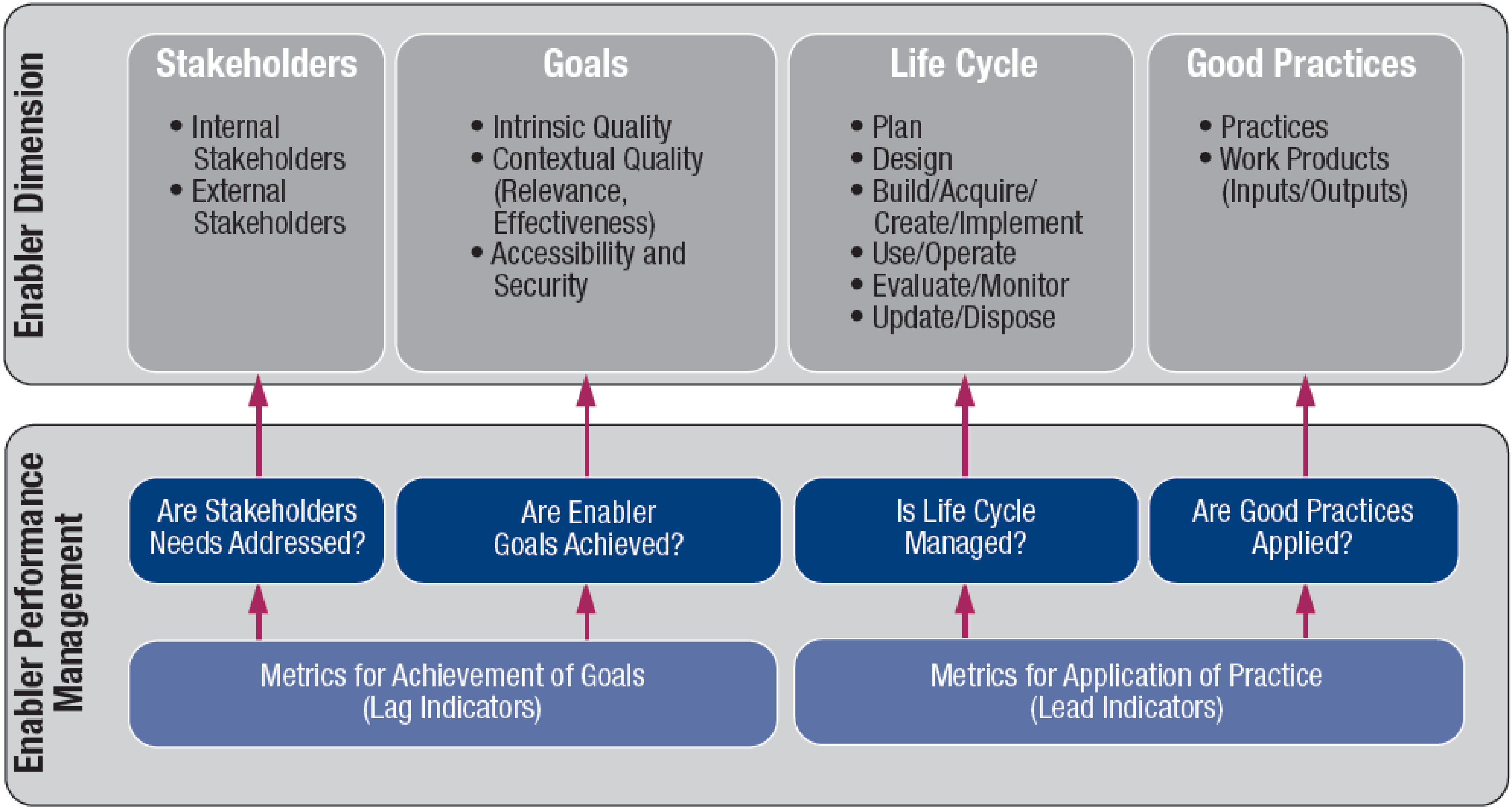
People, Skills and Competencies
Are linked to people required for successful completion of all activities for making correct decisions and taking corrective actions

RESOURCES

Using COBIT 5 Enablers to support the Privacy Program

1. Privacy **policies, principles and frameworks** (e.g., the ISACA Privacy Principles, internal organizational privacy policies, the APEC Privacy Framework, etc.)
2. **Processes**, including privacy-specific details and activities (e.g., identity verification, providing notice, offering opt-in, etc.)
3. Privacy-specific **organizational structures** (e.g., Information Technology, Human Resources, Physical Security, Legal Counsel, etc.)
4. In terms of **culture, ethics and behavior**, factors determining the success of privacy governance and management (e.g., executive support of the privacy program, providing privacy training, etc.)
5. Privacy-specific **information** types (e.g., personal information, sensitive information, and other types of information that can have privacy impacts, such as communications metadata, etc.) and concepts for enabling privacy governance and management within the enterprise
6. **Service capabilities** required to provide privacy related functions and activities to an enterprise (e.g., applications, infrastructure, technologies, etc.)
7. **People, skills and competencies** specific for privacy (e.g., understanding of privacy enhancing technologies, knowing geographic locations where personal information is collected from and where it is stored, privacy certifications, etc.)

COBIT 5 Enablers: Generic



Enabler Dimension

Stakeholders

- Internal Stakeholders
- External Stakeholders

Goals

- Intrinsic Quality
- Contextual Quality (Relevance, Effectiveness)
- Accessibility and Security

Life Cycle

- Plan
- Design
- Build/Acquire/ Create/Implement
- Use/Operate
- Evaluate/Monitor
- Update/Dispose

Good Practices

- Practices
- Work Products (Inputs/Outputs)

Enabler Performance Management

Are Stakeholders Needs Addressed?

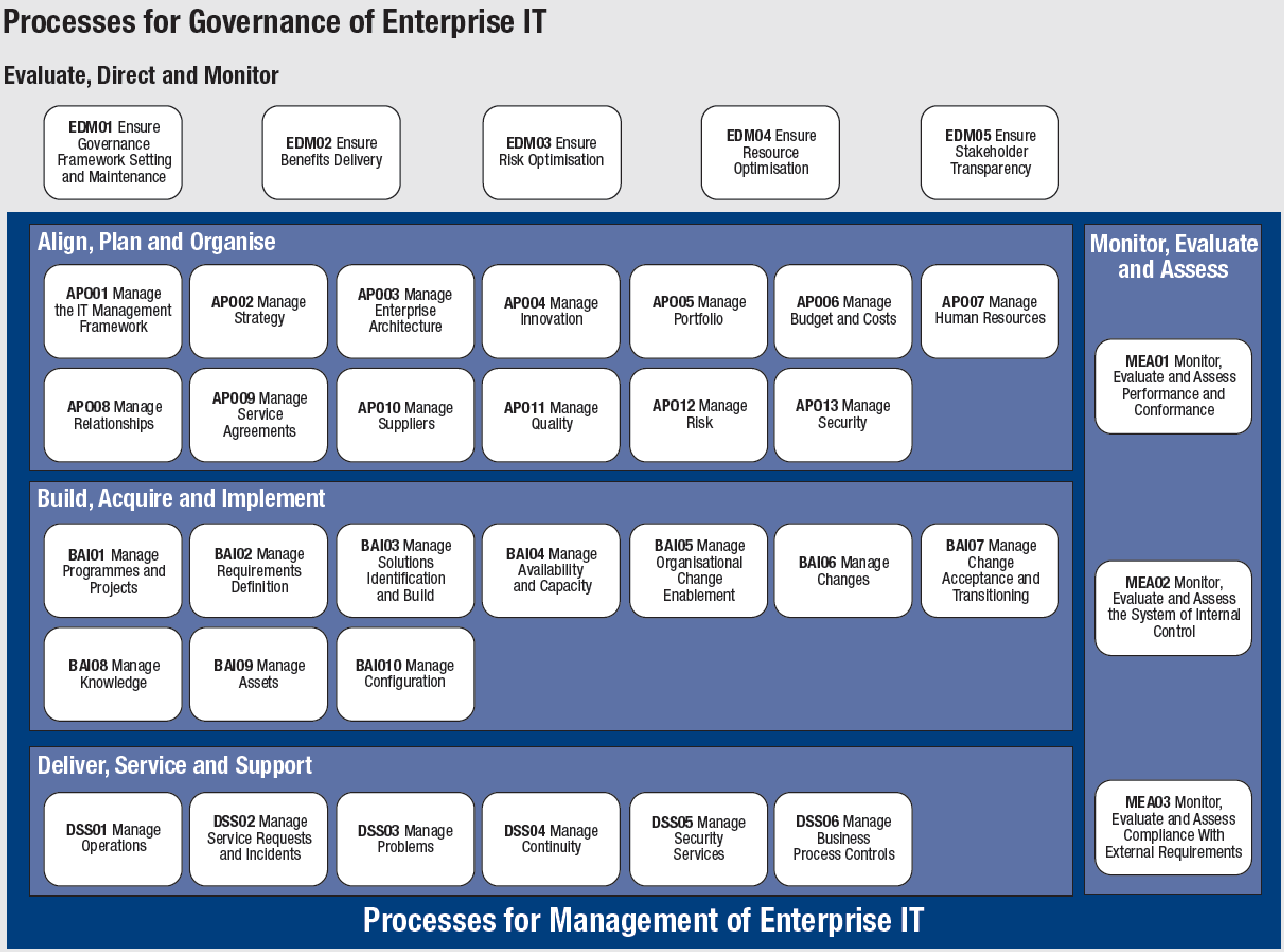
Are Enabler Goals Achieved?

Is Life Cycle Managed?

Are Good Practices Applied?

Metrics for Achievement of Goals (Lag Indicators)

Metrics for Application of Practice (Lead Indicators)



Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

- **EDM01** Ensure Governance Framework Setting and Maintenance
- **EDM02** Ensure Benefits Delivery
- **EDM03** Ensure Risk Optimisation
- **EDM04** Ensure Resource Optimisation
- **EDM05** Ensure Stakeholder Transparency

Align, Plan and Organise

- **APO01** Manage the IT Management Framework
- **APO02** Manage Strategy
- **APO03** Manage Enterprise Architecture
- **APO04** Manage Innovation
- **APO05** Manage Portfolio
- **APO06** Manage Budget and Costs
- **APO07** Manage Human Resources
- **APO08** Manage Relationships
- **APO09** Manage Service Agreements
- **APO10** Manage Suppliers
- **APO11** Manage Quality
- **APO12** Manage Risk
- **APO13** Manage Security

Build, Acquire and Implement

- **BAI01** Manage Programmes and Projects
- **BAI02** Manage Requirements Definition
- **BAI03** Manage Solutions Identification and Build
- **BAI04** Manage Availability and Capacity
- **BAI05** Manage Organisational Change Enablement
- **BAI06** Manage Changes
- **BAI07** Manage Change Acceptance and Transitioning
- **BAI08** Manage Knowledge
- **BAI09** Manage Assets
- **BAI010** Manage Configuration

Deliver, Service and Support

- **DSS01** Manage Operations
- **DSS02** Manage Service Requests and Incidents
- **DSS03** Manage Problems
- **DSS04** Manage Continuity
- **DSS05** Manage Security Services
- **DSS06** Manage Business Process Controls

Monitor, Evaluate and Assess

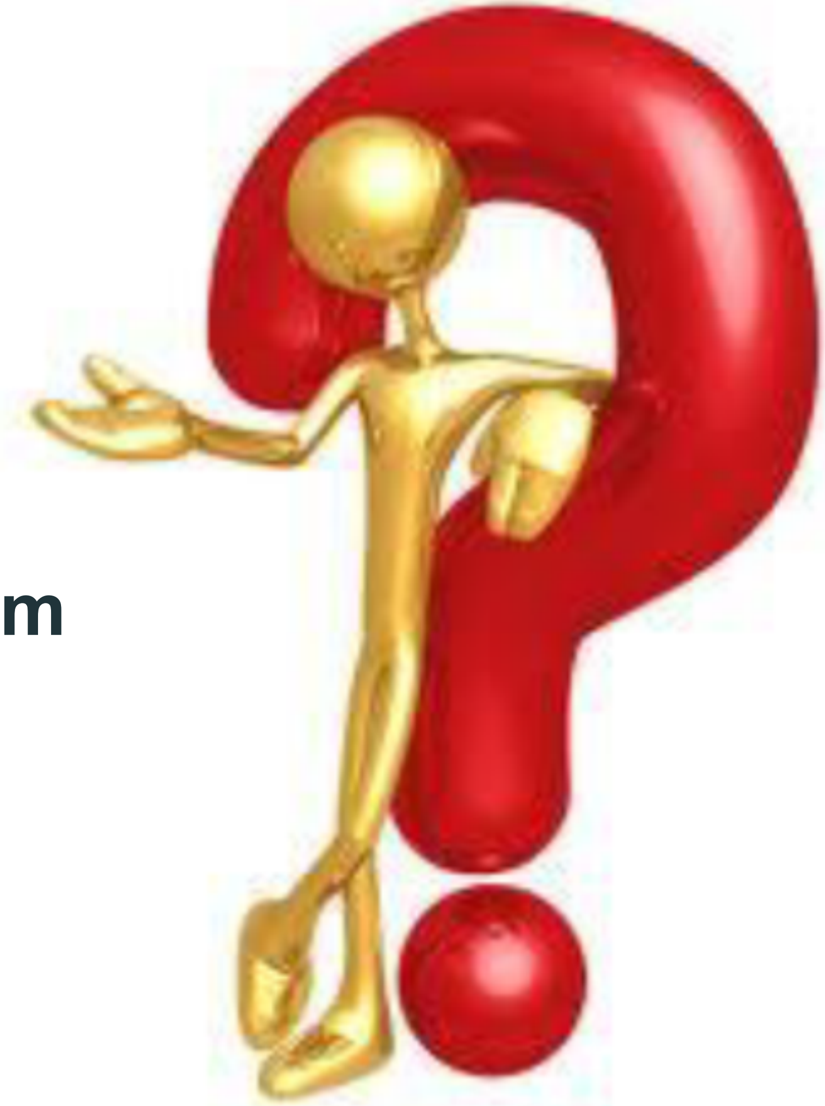
- **MEA01** Monitor, Evaluate and Assess Performance and Conformance
- **MEA02** Monitor, Evaluate and Assess the System of Internal Control
- **MEA03** Monitor, Evaluate and Assess Compliance With External Requirements

Processes for Management of Enterprise IT

Adapting the ISACA Privacy Principles to the Enterprise Environment

- Considering the context for which personal information is collected, and how it is used within the enterprise’s privacy context.
- How to create the appropriate privacy protection environment for your organization to match your business environment.
- Recognizing and addressing privacy protection pain points and trigger events.
- Understanding potential privacy risks as well as privacy harms
- Enabling privacy protection change.
- Implementing a life cycle approach to privacy governance and management.

QUESTIONS ?



Yves.leroux@ca.com

Yves LE ROUX CISM, CISSP

Principal consultant

Yves.leroux@ca.com

@yves_le_roux

slideshare.net/CAinc

linkedin.com/company/ca-technologies

ca.com