ISACA Privacy Principles and Program Management Guide

Yves LE ROUX  CISM, CISSP
ISACA Privacy TF Chairman
Yves.leroux@zoho.com

Québec, 1er juin 2017
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”
- Second action: Elaborating a « Privacy Principles and Program Management Guide”
Development team

- Rebecca Herold, CISA, CISM, CIPM, CIPP/US, CIPP/IT, CISSP, FLMI, USA (Lead Developer)
- Alberto Ramirez Ayon, CISA, CISM, CRISC, CBCP, CIAM, Seguros Monterrey New York Life, Mexico
- Frank Cindrich, CGEIT, CIPP/US, CIPP/G, PwC, USA
- Nancy A. Cohen, CPA, CIPP/US, ISACA, USA
- Alan Lee, CISA, CISM, CISSP, Ernst & Young, Hong Kong
- Yves Le Roux, CISM, CISSP, CA Technologies, France, Chair
- John O’ Driscoll, CISA, CISM, CGEIT, CIA, ANZ, Australia
- Fidel Santiago, CISA, CISM, Belgium
- Roberto Soriano, CISA, CISM, CRISC, Seidor, Spain
Document structure 1/2

- Two volumes (currently tome I is available, tome II planned for July 2017)
- Volume I is organized into six chapters and seven appendices,
- Chapter 1—Introduction to Privacy
  Introduction to privacy, including an explanation of why security and privacy are not the same and a list of privacy terms.
- Chapter 2—Privacy Legal Models, Categories and Emerging Concepts
  Overview of seven different categories of privacy as defined by major privacy laws, regulations and frameworks.
- Chapter 3—Privacy Risk from New and Evolving Technologies
  Overview of relatively new technologies and their corresponding privacy risk and impacts to the seven privacy categories.
- Chapter 4—ISACA Privacy Principles Description of the 14 ISACA privacy principles.
- Chapter 5—COBIT 5 and Privacy Guidance on how to embed privacy throughout enterprise processes and technologies, using COBIT 5 as the overarching framework for information governance and management of
Chapter 6—Establishing a Privacy Protection Program
Guidance on how to use the concepts that are provided in earlier chapters to create, implement and sustain a privacy program. The guidance is divided into major phases:
- Enabling privacy protection change
- Implementing a life cycle approach to privacy governance and management
- Key success factors for a successful implementation of a privacy management program
- Creating the appropriate privacy protection environment and enabling change

Appendix A—List of Privacy Laws and Regulations by Region
Overview and listing of privacy laws, regulations and standards in the different regions of the world.

Appendix B—Legal Actions for Privacy by Country
Overview and listings of some of the legal privacy protections throughout the world, worldwide legal enforcement actions for privacy, and global industry-specific privacy standards.

Appendix C—Privacy Standards, Frameworks and Self-Regulation Programs
Existing privacy standards, principles and frameworks, and relevant security standards.

Appendix D—Professional Privacy and Security Certifications
List of generally and worldwide accepted professional certifications that are related to privacy.

Appendix E—Connecting the ISACA Privacy Principles to Other Privacy Standards, Frameworks, Models and Good Practices
List of privacy advice publications and standards to consider and how the ISACA privacy principles map to a few of these standards.
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
## PRIVACY CATEGORIES\TECHNOLOGIES

<table>
<thead>
<tr>
<th></th>
<th>Social media</th>
<th>Cloud computing</th>
<th>Apps</th>
<th>Big Data Analytics</th>
<th>Internet of Things</th>
<th>BYOD</th>
<th>Tracking and surveillance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy of the person</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Privacy of behaviour and action</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Privacy of communication</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Privacy of data and image</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Privacy of thought and feelings</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Privacy of location and space</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Privacy of association</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Data Privacy legislations around the world

107 countries have put in place legislation to secure the protection of data and privacy.

Data Protection and Privacy Legislation Worldwide

[Map showing data protection and privacy legislation worldwide, legend indicating 'Legislation', 'Draft Legislation', 'No Legislation', and 'No Data'. Source: UNCTAD, 14/04/2016]
Models used in data protection laws

- **Comprehensive Model**
  e.g. European Union countries and the Canadian provinces

- **Sectoral Model**
  e.g. United States and Japan

- **Co-Regulatory Model**
  e.g. Australia, New Zealand and the Netherlands.

- **Self-Regulatory Model**
  e.g. Network Advertising Initiative (NAI) Code of Conduct and North American Energy Standards Board (NAESB)
After studying existing privacy standards, frameworks and principles, ISACA defined a uniform set of practical principles

- Principle 1: 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

For more details see
# Mapping of the ISACA Privacy Principles

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Choice and Consent</td>
<td>NA</td>
<td>Consent and Choice</td>
<td>Choice</td>
<td>Choice and Consent</td>
</tr>
<tr>
<td>2. Legitimate Purpose Specification &amp; Use Limitation</td>
<td>Purpose specification; and Use limitation</td>
<td>Purpose legitimacy and specification; and Use, retention and disclosure limitation</td>
<td>Use of personal information</td>
<td>Use, retention and disposal</td>
</tr>
<tr>
<td>3. Personal and Sensitive Information Life Cycle</td>
<td>Collection Limitation</td>
<td>Collection limitation; and Data minimization</td>
<td>Collection Limitations</td>
<td>Collection</td>
</tr>
<tr>
<td>4. Accuracy and Quality</td>
<td>Data quality</td>
<td>Accuracy and quality</td>
<td>Integrity of personal information</td>
<td>Quality</td>
</tr>
<tr>
<td>5. Openness, transparency and notice</td>
<td>Openness</td>
<td>Openness, transparency and notice</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>6. Individual participation</td>
<td>Individual participation</td>
<td>Individual participation and access</td>
<td>Access and correction</td>
<td>Access</td>
</tr>
<tr>
<td>7. Accountability</td>
<td>Accountability</td>
<td>Accountability</td>
<td>Accountability</td>
<td>Management</td>
</tr>
<tr>
<td>9. Monitoring, Measuring and Reporting</td>
<td>NA</td>
<td>Privacy Compliance</td>
<td>NA</td>
<td>Monitoring and enforcement</td>
</tr>
<tr>
<td>10. Preventing Harm</td>
<td>NA</td>
<td>NA</td>
<td>Preventing Harm</td>
<td>Disclosure to third parties</td>
</tr>
<tr>
<td>11. Third Party Management</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>12. Breach Management</td>
<td>Data security breach notification</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>13. Security and Privacy by Design</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>14. Free flow of information and legitimate restriction</td>
<td>Free flow of information</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

[^25]: Reference to OECD 2013[^25]
[^26]: Reference to ISO 29100:2011[^26]
[^27]: Reference to APEC[^27]
[^28]: Reference to GApp[^28]
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.)
PRINCIPLES, POLICIES AND FRAMEWORKS

Privacy Policy Framework

- Privacy Principles
- Privacy Policies
- Privacy Procedures
- Privacy Standards
- Privacy Requirements and Documents

Input

- Contractual Requirements for Privacy Protections
- Mandatory Privacy Laws, Standards, Frameworks, and Models
- Generic Privacy Standards, Frameworks, Practices and Models
PROCESS

- For each process, a limited number of privacy-specific process goals are included, and for each process goal a limited number of privacy-specific example metrics is listed.

- For each practice, we will find privacy-specific practice inputs and outputs (work products), with indication of origin and destination and privacy-specific process activities.

- Volume II will provide the details of privacy-specific processes (those that involve personal information, or could be used to reveal details about individuals and their associated lives).
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
- BAI10 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

Processes for Management of Enterprise IT
## EDM02 Ensure Benefits Delivery

<table>
<thead>
<tr>
<th>Area: Governance</th>
<th>Domain: Evaluate, Direct and Monitor</th>
</tr>
</thead>
</table>

### COBIT 5 Process Description
Optimize the value contribution to the business from the business processes, IT services and IT assets resulting from investments made by IT at acceptable costs.

### COBIT 5 Process Purpose Statement
Secure optimal value from IT-enabled initiatives, services and assets; cost-efficient delivery of solutions and services; and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.

### Primary Privacy Principles Involved:
- Principle 10: Preventing Harm
- Principle 12: Breach Management
- Principle 13: Security and Privacy by Design
- Principle 14: Free Flow of Information & Legitimate Restriction

### EDM02 Privacy-specific Process Goals and Metrics

<table>
<thead>
<tr>
<th>Privacy-specific Process Goals</th>
<th>Related Metrics</th>
</tr>
</thead>
</table>
| 1. Benefits, costs and risk of information security investments are balanced and managed and contribute optimal value. | • Percent of risk reduction vs. budget deviation (budgeted vs. projection)  
• Level of stakeholder satisfaction with the privacy program requirements in place, based on surveys |
| 1. Privacy harms and privacy breaches are prevented.                                           | • Number of breaches  
• Level of Data Subject satisfaction with privacy, based on phone calls, complaints, and surveys |
| 1. Information flow is not restricted.                                                        | • Number of communications with Data Protection Authorities necessary to enable personal information transmissions |
## EDM02 ENSURE BENEFITS DELIVERY

### EDM02 Privacy-specific Process Practices, Inputs/Outputs and Activities

<table>
<thead>
<tr>
<th>Governance Practice</th>
<th>Privacy-specific Activities</th>
</tr>
</thead>
</table>
| **EDM02.01 Evaluate value optimization.** Continually evaluate the portfolio of IT-enabled investments, services and assets to determine the likelihood of achieving enterprise objectives and delivering value at a reasonable cost. Identify and make judgement on any changes in direction that need to be given to management to optimise value creation. | • Identify and record the requirements of stakeholders (such as shareholders, regulators, auditors and customers) for protecting their interests and delivering value through privacy management activity. Set direction accordingly.  
• Identify and record the expectations of Data Subjects for protecting their personal information and privacy and determine the value of the privacy management activities. Change direction as appropriate. |
| **EDM02.02 Direct value optimization.** Direct value management principles and practices to enable optimal value realisation from IT-enabled investments throughout their full economic life cycle. | • Establish a method of demonstrating the value of privacy management activities (including defining and collecting relevant data) to ensure the efficient use of existing privacy-related assets.  
• Establish a method of demonstrating the value to Data Subjects of privacy protection activities (including defining and collecting relevant data) to ensure the effective use of existing privacy-related assets.  
• Ensure the use of financial and non-financial measures to describe the added value of privacy initiatives.  
• Use business-focused methods of reporting on the added value of privacy initiatives. |
| **EDM02.03 Monitor value optimization.** Monitor the key goals and metrics to determine the extent to which the business is generating the expected value and benefits to the enterprise from IT-enabled investments and services. Identify significant issues and consider corrective actions. | • Track outcomes of privacy initiatives and compare to expectations to ensure value delivery against business goals.  
• Track outcomes of providing privacy practices transparency to Data Subjects and Data Protection Authorities and compare to expectations to ensure value delivery with original goals. |
**APO03 MANAGE ENTERPRISE ARCHITECTURE**

<table>
<thead>
<tr>
<th>APO03 Manage Enterprise Architecture</th>
<th>Area: Management Domain: Align, Plan and Organize</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>COBIT 5 Process Description</strong></td>
<td>Establish a common architecture consisting of business process, information, data, application and technology architecture layers for effectively and efficiently realizing enterprise and IT strategies by creating key models and practices that describe the baseline and target architectures. Define requirements for taxonomy, standards, guidelines, procedures, templates and tools, and provide a linkage for these components. Improve alignment, increase agility, improve quality of information and generate potential cost savings through initiatives such as reuse of building block components.</td>
</tr>
<tr>
<td><strong>COBIT 5 Process Purpose Statement</strong></td>
<td>Represent the different building blocks that make up the enterprise and their interrelationships as well as the principles guiding their design and evolution over time, enabling a standard, responsive and efficient delivery of operational and strategic objectives.</td>
</tr>
</tbody>
</table>
| **Primary Privacy Principles Involved:** | - 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 & Legitimate Restriction |
| **APO03 Privacy-specific Process Goals and Metrics** | **Privacy-specific Process Goals** | **Related Metrics** |
| | 1. Privacy requirements are embedded within the enterprise architecture and translated into a formal privacy protection and management architecture. | • Number of exceptions to privacy management architecture standards |
| | 2. Privacy management architecture is understood as part of the overall enterprise architecture. | • Number of deviations between privacy management architecture and enterprise architecture |
| | 3. Privacy management architecture is aligned and evolves with changes to the enterprise architecture. | • Date of last review and/or update to privacy controls applied to enterprise architecture |
| | 4. A privacy management architecture framework and methodology are used to enable reuse of privacy management components across the enterprise. | • Percent of projects that use the privacy management architecture framework and methodology  
• Number of people trained in the privacy management framework and methodology |
# APO03 MANAGE ENTERPRISE ARCHITECTURE

## APO03 Privacy-specific Process Practices, Inputs/Outputs and Activities

<table>
<thead>
<tr>
<th>Management Practice</th>
<th>Privacy-specific Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>APO03.01 Develop the enterprise privacy management architecture vision.</strong>&lt;br&gt;The privacy management architecture vision provides a first-cut, high-level description of the baseline and target architectures, covering the business, information, data, application, and technology domains. The architecture vision provides the sponsor with a key tool to sell the benefits of the proposed capability to stakeholders within the enterprise. The architecture vision describes how the new capability will meet enterprise goals and strategic objectives and address stakeholder concerns when implemented.</td>
<td>• Define privacy management objectives and requirements for the enterprise architecture.&lt;br&gt;• Define the privacy management value proposition and related goals and metrics.&lt;br&gt;• Consider industry good privacy practices, such as using the ISACA Privacy Principles, in building the privacy management architecture vision.</td>
</tr>
<tr>
<td><strong>APO03.02 Define reference architecture.</strong>&lt;br&gt;The reference architecture describes the current and target architectures for the business, information, data, application and technology domains.</td>
<td>• Ensure inclusion of privacy artefacts, policies and standards in the architecture repository.&lt;br&gt;• Ensure privacy is integrated throughout all architectural domains (e.g., business, information, data, applications, technology).&lt;br&gt;• Establish a centralised personal information inventory for all areas of the enterprise to use.&lt;br&gt;• Establish a catalogue of privacy tools, standards and technologies to be available for enterprise-wide use.</td>
</tr>
</tbody>
</table>
COBIT 5 ENABLER:
ORGANISATIONAL STRUCTURES

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: Operating Principles, Span of Control (Scope), Level of Authority, Delegation of Authority, Escalation Procedures
  - Work Products (Inputs/Outputs): Decisions

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)
ORGANIZATIONAL STRUCTURES

New organizational structures
- Chief Privacy Officer (CPO) / Data Protection Officer (DPO)
- Privacy Steering Committee (PSC)
- Privacy Manager (PM)
- Enterprise Risk Management (ERM) Committee
- Data Processor

In Volume II detailed descriptions of these groups and roles will be provided:
- **Composition**—An appropriate skill set should be required of all members of the organisational group.
- **Mandate, operating principles, span of control and authority level**—These elements describe the practical arrangements of how the structure will operate, the boundaries of the organisational structure’s decision rights, the responsibilities and accountabilities, and the escalation path or required actions in case of problems.
- **High-level RACI chart**—RACI charts link process activities to organisational structures and/or individual roles in the enterprise. The charts describe the level of involvement of each role, for each process practice: accountable, responsible, consulted or informed.
- **Inputs/Outputs**—A structure requires inputs (typically information) before it can make informed decisions; it produces outputs, such as decisions, other information or requests for additional inputs.
COBIT 5 ENABLER:
CULTURE, ETHICS AND BEHAVIOUR

**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:
  - Communication
  - Enforcement
  - Incentives and Rewards
  - Awareness
  - Rules and Norms
  - Champions
- Work Products (Inputs/Outputs)

**Enabler Performance Management**
- Are Stakeholder 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)
CULTURE, ETHICS AND BEHAVIOR ENABLER

Eight desirable privacy behaviors:

- Privacy protecting actions are performed in daily operations.
- Personnel respect the importance of privacy policies, procedures, standards and principles.
- Personnel are provided with sufficient and detailed privacy guidance, and are encouraged to participate in and proactively suggest privacy protection improvements.
- Everyone is responsible and accountable for the protection of personal information within the enterprise.
- Stakeholders are aware of how to identify and respond to privacy threats and vulnerabilities.
- Management proactively supports and anticipates new privacy protection innovations and communicates this to the enterprise.
- The enterprise is receptive to account for and deal with new privacy challenges.
- Business management engages in continuous cross-functional collaboration to allow for efficient and effective privacy programs.
- Executive management recognizes the business value of privacy protection.
CULTURE, ETHICS AND BEHAVIOR ENABLER

For each of the behaviors defined, the following attributes are:

- **Organisational privacy ethics**: Determined by the values by which the enterprise wants to operate

- **Individual privacy ethics**: Determined by the personal values of each individual in the enterprise and, to an important extent, depend on external factors, such as personal experiences, beliefs, socio-economic background and geographic location

- **Leadership**: Ways that leadership can influence desired behavior and privacy-impacting actions:
  - Privacy policy enforcement and rules and norms
  - Incentives and rewards
  - Communications and activities

- **Detailed description will be in Volume II**
COBIT 5 ENABLER: INFORMATION

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: Define Information Attributes:
  - Physical (Carrier, Media)
  - Empirical (User Interface)
  - Syntactic (Language, Format)
  - Semantic (Meaning), Type, Currency, Level
  - Pragmatic (Use), Includes Retention, Status, Contingency, Novelty
  - Social (Context)

Enabler Performance Management

Are Stakeholder 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)
INFORMATION

The following items are discussed:
1. The information model
2. Examples of common information types
3. Information stakeholders and how to identify the impacted parties within the enterprise
4. Information life cycle, describing the different phases of information management in this context

For each of the examples of common information types, we provide:

- **Goals**—This describes a number of goals to be achieved, using the three categories defined in the COBIT 5 information model. For these information types, goals for information are divided into three dimensions of quality:
  - Intrinsic quality—The extent to which data values are in conformance with the actual or true values
  - Contextual quality—The extent to which information is applicable to the task of the information user and is presented in an intelligible and clear manner, recognizing that information quality depends on the context of use
  - Privacy/accessibility quality—The extent to which information is available or obtainable
- **Life cycle**—A specific description of the life cycle requirements
- **Good practices** for this type of information—A description of typical contents and structure
EXAMPLES OF INFORMATION TYPES 1/2

- Privacy management strategy
- Privacy management budget
- Privacy management plan
- Privacy policies
- Privacy principles
- Privacy standards
- Privacy procedures
- Privacy protection requirements, which can include:
  - Privacy protection configuration requirements
  - SLA/OLA privacy protection requirements
- Training and Awareness material
EXAMPLES OF INFORMATION TYPES 2/2

- Privacy management review reports, which include:
  - Privacy management audit findings
  - Privacy management maturity report
  - Privacy impact assessment
  - Privacy management-related risk management
    - Threat analysis
    - Vulnerability assessment reports
    - Harms analysis
- Privacy management dashboard (or equivalent), which includes:
  - Privacy breaches
  - Privacy management problems
  - Privacy compliance fines and penalties
  - Privacy management metrics
<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Privacy Strategy</th>
<th>Privacy Budget</th>
<th>Privacy Plan</th>
<th>Privacy Policies</th>
<th>Privacy Requirements</th>
<th>Privacy Awareness Material</th>
<th>Privacy Review Reports</th>
<th>Privacy Services Catalogue</th>
<th>Privacy Risk Profile</th>
<th>Privacy Program Dashboard</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internal: Enterprise</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Board</td>
<td>U</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A</td>
</tr>
<tr>
<td>Chief Executive Officer (CEO)</td>
<td>U</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>U</td>
</tr>
<tr>
<td>Chief Financial Officer (CFO)</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>U</td>
</tr>
<tr>
<td>Chief Privacy Officer (CPO)</td>
<td>O</td>
<td>U</td>
<td>O</td>
<td>O</td>
<td></td>
<td>O</td>
<td>O</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Chief information security officer (CISO)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy Steering Committee (PSC)</td>
<td>A</td>
<td>O</td>
<td>A</td>
<td>U</td>
<td>U</td>
<td>U</td>
<td>I</td>
<td>U</td>
<td>U</td>
<td>U</td>
</tr>
<tr>
<td>Business Unit Head</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>U</td>
</tr>
<tr>
<td>Head of Human Resources (HR)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>U</td>
</tr>
<tr>
<td><strong>Internal: IT</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chief information officer (CIO)/IT manager</td>
<td>U</td>
<td>O</td>
<td>U</td>
<td>U</td>
<td>U</td>
<td>U</td>
<td>U</td>
<td>U</td>
<td>I</td>
<td>U</td>
</tr>
<tr>
<td>Privacy Manager (PM)</td>
<td>U</td>
<td>U</td>
<td>U</td>
<td>O</td>
<td>U</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td><strong>External</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Investors</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>I</td>
</tr>
<tr>
<td>Insurers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>I</td>
</tr>
<tr>
<td>Data Protection Authorities</td>
<td>I/U</td>
<td>I/U</td>
<td>I/U</td>
<td>I/U</td>
<td>I/U</td>
<td>I/U</td>
<td>I/U</td>
<td>I/U</td>
<td>I/U</td>
<td>I/U</td>
</tr>
<tr>
<td>Regulators</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>I</td>
</tr>
<tr>
<td>Business Partners</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>I</td>
</tr>
<tr>
<td>Vendors/Suppliers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>I</td>
</tr>
<tr>
<td>External Auditors</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>I</td>
</tr>
</tbody>
</table>
COBIT 5 ENABLER:
SERVICES, INFRASTRUCTURE AND APPLICATIONS
SERVICES, INFRASTRUCTURE AND APPLICATIONS

Examples of potential privacy-related services (1/2)

- Privacy Management Architecture
- Privacy Training and Awareness Communications
- Provide a process to allow Data Subjects (individuals) to get access to their associated personal information
- Provide privacy protecting development (development in line with privacy by design standards)
- Privacy Assessments
- Provide legal resources for privacy protections
- Provide systems with adequate privacy protections and configurations, supporting privacy requirements and privacy architecture
- Provide user (data processor) access and access rights to personal information in line with business and legal requirements
SERVICES, INFRASTRUCTURE AND APPLICATIONS

Examples of potential privacy-related services (2/2)

- Provide adequate protection against inappropriate sharing, misuse, unauthorized access, malware, external attacks and intrusion attempts
- Provide adequate privacy incident response
- Provide privacy protection testing
- Provide monitoring and alert services for privacy-impacting events

For each of these service capabilities, we provide:

- Detailed description of the service, including business functionality
- Attributes: The inputs, supporting technologies (including applications and infrastructure)
- Goal: The quality and compliance goals for each service capability and the related metrics
COBIT 5 ENABLER:
PEOPLE, SKILLS AND COMPETENCIES
To effectively operate the privacy function within an enterprise, individuals with appropriate knowledge and experience (e.g., skills and competencies) must exercise that function. Some typical privacy-related skills and competencies are:

- Privacy management governance
- Privacy management strategy formulation
- Privacy risks and harms management
- Privacy management architecture development
- Privacy management operations
- Privacy impact assessment, testing and compliance

For each of the skills and competencies, the following attributes are described:

- Skill description and definition
- Experience, education and qualifications required for the skill/competency
- Knowledge, technical skills and behavioral skills
- Related structure (if relevant):
ADAPTING THE ISACA PRIVACY PRINCIPLES TO THE ENTERPRISE ENVIRONMENT

This section provides generic guidance for a privacy governance and management. Major considerations discussed include:

- 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.
- Enabling privacy protection change.
- Implementing a life cycle approach to privacy governance and management.
IMPLEMENTATION LIFE CYCLE SEVEN PHASES

- **Phase 1**: What are the privacy protection program drivers?
- **Phase 2**: Where is the enterprise now with the privacy management program?
- **Phase 3**: Where does the enterprise want to be with the privacy management program?
- **Phase 4**: What needs to be done for the privacy management program?
- **Phase 5**: How does the enterprise get the new or updated privacy management program?
- **Phase 6**: Was there success with the privacy management program plans?
- **Phase 7**: How does the enterprise achieve continued privacy protection program improvement?
ADAPTING THE ISACA PRIVACY PRINCIPLES TO THE ENTERPRISE ENVIRONMENT

- The ISACA Privacy Program Management Guide was created to provide information assurance practitioners of all kinds (information security, privacy, risk management, audit, legal, etc.) with a practical guide to creating, improving and evaluating a privacy program specific to a practitioner’s own organization, and to support or be used in conjunction with other privacy frameworks, good practices and standards.

- In order to facilitate this work, we describe and explore the relationship of the ISACA privacy principles to some of the other existing privacy frameworks, good practices and standards.
“That’s all Folks!”

Yves.Leroux @zoho.com
Y a-t-il des questions?