Role of ISACA in Promoting Data Privacy through Information Systems

Dr.Kris Seeburn
Member – ISACA , Professional Standards & Career Management Committee
Chair – ISACA, Academic Program Subcommittee
Chair & GRA – ISACA Mauritius Chapter
Lecturer – University of Technology, Mauritius

ISACA

- An independent, nonprofit, global association, ISACA engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems.
- 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 Privacy Landscape

- The privacy of personally identifiable information (PII) continues to be a growing regulatory and enterprise concern.
- The debate over privacy seems to have shifted to the larger discussion about the new types of PII, individual rights, and enterprise use of personal data.
- This expanding debate results from the proliferation of technologies, and opportunities for organisations to gain value by leveraging new data items.

Privacy and Personal Information

- Privacy is defined as the rights and obligations of individuals and organizations with respect to the collection, use, retention and disclosure of personal information.
- Personal information is information that is, or can be, about or related to an identifiable individual.
- It includes any information that can be linked to an individual or used to directly or indirectly identify an individual.
- Most information collected by an organization about an individual is likely to be considered personal information if it can be attributed to an identified individual.

Some examples of personal information

- Name
- Home or e-mail address
- Identification number (e.g., a Social Security or Social Insurance number)
- Physical characteristics
- Consumer purchase history - Some personal information is considered sensitive.

Some laws and regulations define the following as sensitive personal information

- Information on medical or health conditions
- Financial information
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Sexual preferences
- Information related to offenses or criminal convictions

- Sensitive personal information generally requires an extra level of protection and a higher duty of care.
  - For example, sensitive information may require explicit consent to be processed or recorded.
- Some information about or related to people cannot be associated with specific individuals. Such information is referred to as non-personal information.
  - This includes statistical or summarized personal information for which the identity of the individual is unknown or linkage to the individual has been removed.
  - In such cases, the individual's identity cannot be determined from the information that remains, because the information is "de-identified"or "anonymized."
  - Nonpersonal information ordinarily is not subjected to privacy protection because it cannot be linked to an individual.

ISACA's Role in Data Privacy

- ISACA is looking at ways that it can help its constituents play an equally important role in promoting data privacy through information systems.
- ISACA will go beyond simply the protection of personally identifiable information and instead focus on providing its constituents with guidance on an expanded set of business, risk and implementation issues surrounding privacy.

Personally Identifiable Information

- Personally Identifiable Information has been defined as data relating to a specific, identified or identifiable person.
- Forrester Research segments this into four distinct categories:
  - **Individual identity data** – entered by individuals directly
  - **Behavioral data** – captured by recording activities of users, as opposed to data they volunteer
  - **Derived data** – based on the analysis of personal data
  - **Self-identified data** – such as likes, networks, intent and product opinions

Trust in the Information Systems

- In order for individuals to have trust in the systems that capture this data, there must be:
  - **Transparency** – knowing what data is captured about them and how it will be used
  - **Trust** – confidence that the attributes of availability, reliability, integrity and security are embraced in the applications
  - **Control** – ability to effectively manage the extent to which their personal data is shared and its accuracy
  - **Value** – understanding of the value created by the use of their data and how they are compensated for it.

The Need for Trust

- Evidence suggests that there is a decline in trust in the personal data ecosystem. This is caused by:
  - Security breaches
  - Identity theft and fraud
  - Concern from individuals regarding the accuracy and use of their personal data
  - Confusion by companies about what they can and cannot do
  - Increasing attention and sanctions from regulators

Privacy Guideline

- ISACA's Privacy guideline is founded on key concepts from significant domestic and international privacy laws, regulations, guidelines and good business practices.
- By using these privacy principles, IS auditors can address the significant challenges that companies face in establishing and managing their privacy programs and risks.

The basic principles of the ISACA Privacy guideline

- Privacy means adherence to trust and obligation in relation to any information relating to an identified or identifiable individual (data subject). Management is responsible for complying with privacy in accordance with its privacy policy or applicable privacy laws and regulations.
- The IS auditor is not responsible for what is stored in the personal databases. He/she should check whether personal data are correctly managed with respect to legal prescriptions by adoption of the correct security measures.

- The IS auditor should review management's privacy policy to ascertain that it takes into consideration the requirements of applicable privacy laws and regulations, including transborder data flow requirements, such as the EU-US Safe Harbor agreement and the Organization for Economic Cooperation and Development (OECD) *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*.

IS auditors should review the privacy impact analysis or assessment carried out by management. Such assessments should:

- Identify the nature of personally identifiable information associated with business processes
- Document the collection, use, disclosure and destruction of personally identifiable information
- Provide management with a tool to make informed policy, operations and system design decisions based on an understanding of privacy risk and the options available for mitigating that risk
- Provide reasonable assurance that accountability for privacy issues exists
- Create a consistent format and structured process for analyzing technical and legal compliance with relevant regulations
- Reduce revisions and retrofit the information systems for privacy compliance
- Provide a framework to ensure that privacy is considered starting from the conceptual and requirements analysis stage to the final design approval, funding, implementation and communication stage

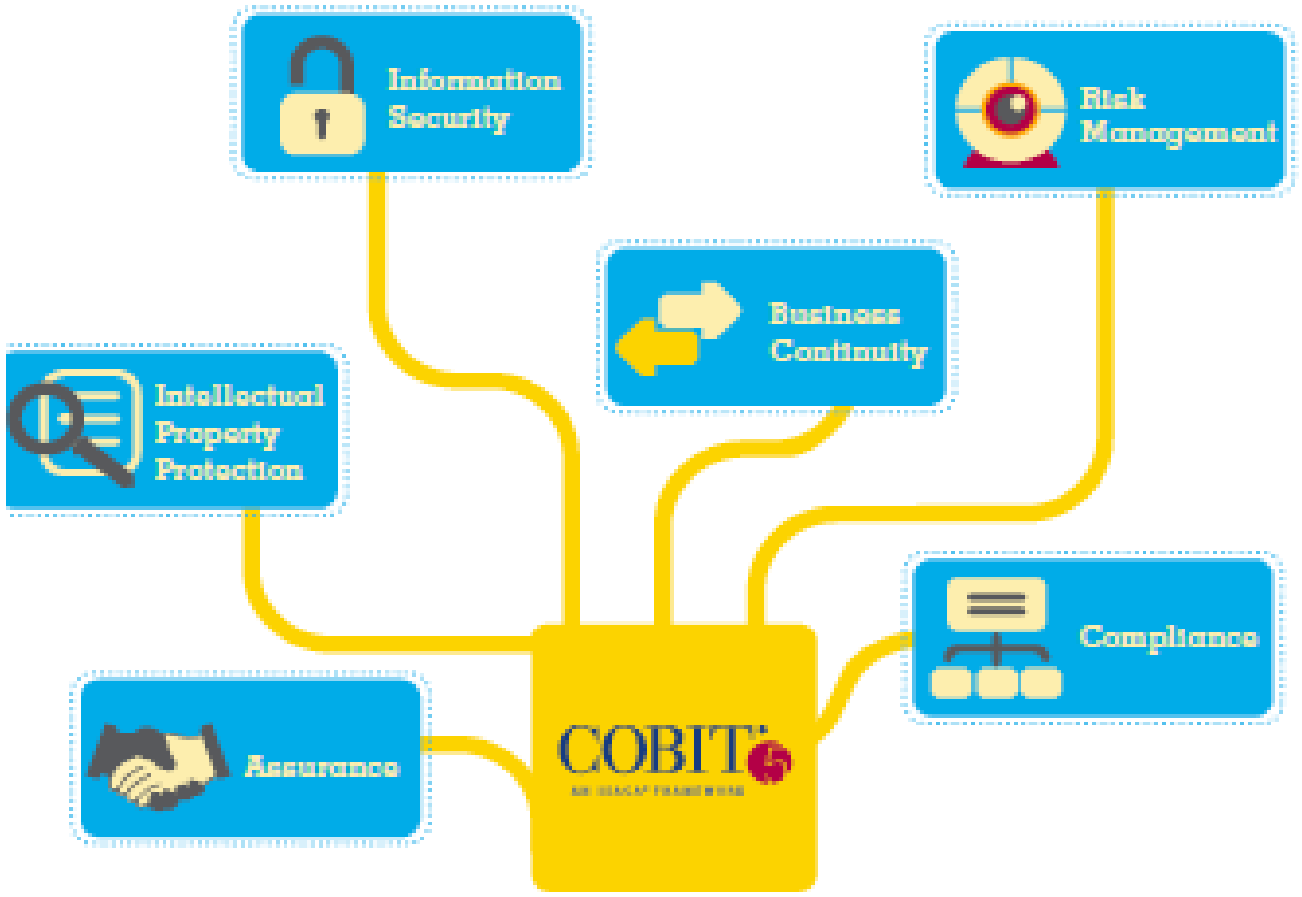
- IS auditors should determine whether these assessments are conducted as part of an initial privacy review and on an ongoing basis for any change management project, such as:
  - Changes in technology
  - New programs or major changes in existing programs
  - Additional system linkages
  - Enhanced accessibility
  - Business process reengineering
  - Data warehousing
  - New products, services, systems, operations, vendors and business partners

- In assessing applicable privacy laws and regulations that need to be complied with by any particular organization, particularly for organizations operating in different parts of the globe, IS auditors should seek an expert opinion as to the requirement of any laws and regulations, and carry out the necessary compliance and substantive tests to form an opinion and report on the compliance of such laws and regulations.
- The data controller is a party who is competent to decide about the contents and use of personal data regardless whether such data are collected, stored, processed or disseminated by that party or by an agent on its behalf.

Trust Through COBIT 5

- COBIT 5 complements existing security standards and frameworks and providing a holistic approach to identifying threats against data privacy, security and compliance.
- ISACA's plan is to leverage COBIT 5 as a framework that provides a basis for bringing together stakeholder needs and individual and enterprise goals, providing a common structure and language that business leaders, compliance officers, risk managers, privacy and security managers and practitioners and assurance professionals use in structuring solutions and managing privacy programs.

ISACA
Trust in, and value from, information systems



Using COBIT 5 in India

- Working with ISACA's India Growth Task Force, a paper was published providing guidance on how COBIT 5 can be used to secure sensitive personal data or information (SPDI) in India.
- Adherence to this guidance, along with India's IT Act can bring organizations in India one step closer to compliance with safe harbor guidelines of the EU.

- “In today’s world, SPDI is used in every aspect of a business.
- It is used by very small organisations as well as very large enterprises.
- Securing SPDI cannot be done in isolation; the entire enterprise needs to be involved.
- The approach should be holistic as well as customisable to suit the size and nature of the business of the organisation, and COBIT 5 helps enable that.”

- The Indian IT Act has a specific category, ”sensitive personal data or information,” which consists of password, financial information (including bank account, credit card, debit card or other payment details), physical, physiological and mental health conditions, sexual orientation, medical records, and biometric information.
- This category in the Indian IT Act legally obligates all stakeholders (i.e., any individual or organisation that collects, processes, transmits, transfers, stores or deals with sensitive personal data) to adhere to its requirements.
- Some of the largest stakeholders could include owners of websites, banks, insurance companies, financial institutions, hospitals, educational institutions, service providers, travel agents, payment gateway providers and social media platforms, among many other entities.

According to India's IT Act, the accountability for SPDI is with the governing body, which could be the chairman, board of directors, owner, proprietor, partner, head of an association or head of an institute

Current ISACA Projects

- Audit/assurance program on Personally Identifiable Information (PII) to assist IT auditors with an assessment of PII policies and procedures and their operating effectiveness.
- Creation of a global privacy task force that will assist in creating a strategy to position ISACA in the privacy market.

Questions?

kseeburn@umail.utm.ac.mu