Privacy and IT policies have a lot in common: Both are considered important; organizations are concerned about not having them, but not everybody fully understands the implications and consequences if they are wrongly understood. Privacy and IT policies are concepts that evolve—what is an acceptable policy today (or what is considered a privacy concern) may not be a satisfactory practice tomorrow. Similarly, COBIT® has evolved from an audit framework in 1996 to a governance and management of enterprise IT (GEIT) framework in 2012, presenting, among other aspects, policies as fundamental factors for influencing proper governance and management over IT.

This article presents a modern approach for designing a policy framework using COBIT® 5 principles, which provide a robust and systematic approach to ensure that policies are used as instruments to implement accepted business strategies. A policy framework provides a logical structure for organizing and defining policies. It also establishes additional documentation that supports the policies’ implementation and enforcement.

The objective of this article is to provide a structured methodology for assisting organizations in developing and implementing an effective policy framework.

EVOlUTION OF IT POLICIES
IT policies help organizations to properly articulate the organization’s desired behavior, mitigate risk and contribute to achieving the organization’s goals. The evolution of IT policies can be illustrated by comparing the following two documents: Generally Accepted Principles and Practices for Securing Information Technology Systems¹ and Information Security Handbook: A Guide for Managers.²

The first one, published in September 1996, states that a policy should, among other aspects, define and specify rules for particular systems. The second one, published in October 2006, defines a policy, in the context of information security, as an aggregate of directives, rules and practices that prescribe how an organization manages, protects and distributes information.

Configuration and standardization of IT systems and infrastructure were priorities in 1996. After 10 years, organizations realized that taking advantage of IT requires proper management and governance of information resources.

Further, it has become apparent that failure to design and implement robust business processes more quickly renders technology-based controls ineffective. For example, the Verizon 2011 Payment Card Industry Compliance Report³ points out that organizations struggling to meet Payment Card Industry Data Security Standard (PCI DSS) requirement 12 (maintain security policies) fail to drive practice and successfully implement other PCI requirements.
Finally, as illustrated in the *Information Security Management Handbook*, the core of any business is its people—their individual attributes, including integrity, ethical values and competence. Therefore, policies should be communicated, understood, supported and accepted by everybody; otherwise, they are meaningless.

Policies as Enablers

COBIT 5 introduces seven enablers (see figure 1) as support tools for the implementation of GEIT. The four dimensions (stakeholders, goals, life cycle and best practices) of the enabler Principles, Policies and Frameworks are discussed in the following sections and suggestions for a systematic method of designing and implementing a policy framework are provided.

**Figure 1—COBIT 5 Enterprise Enablers**

COBIT 5 ensures that a policy framework meets stakeholders’ needs, covers the end-to-end process (and not only the IT function), and establishes the additional documentation required to ensure that governance and management goals and activities are achieved.

**Stakeholders Dimension**

There are stakeholders who define and set policy principles, and there are others who follow, adhere to or implement such principles.

The first group of stakeholders defines and sets policy principles, taking into consideration general organizational governance principles and analyzing and identifying internal and external factors (e.g. regulation), business direction, and organizational culture. The organization’s board of directors and executive management belong to this group. They are, in addition, accountable for giving direction about, communicating on and implementing governance objectives, and for defining the core components of a policy framework.

The core components of a policy framework are:

- Appointment of individuals who have the authority to approve policies and their associated responsibilities
- Determination of the consequences for failing to comply with given policies
- Definition of a process for handling exceptions to policies
- Definition of a method for measuring and monitoring compliance with policies
- Definition of the scope of the policy and the group of stakeholders that has to follow the policy

The fear, uncertainty and doubt of the other stakeholders are reduced by following policy principles.

**Goals Dimension**

Goals are statements, based on the policy principles defined previously, that describe the desired outcome. Examples of goal statements are:

- Provide a tool for staff orientation.
- Document proper delegation and define limits of authority and responsibility.
- Serve as a documentation source for regulatory compliance.
- Protect intellectual property and business continuity.
- Improve clarity and momentum in projects and operations.

As far as policies are concerned, goals and policy principles should be related in order to provide assurance that stakeholders’ requirements are addressed.
Life Cycle Dimension

The policy life cycle combines the policy principles and goals defined previously and includes the following phases:

• **Plan**—This phase establishes the foundation for a policy framework by covering the stakeholders and goals dimensions defined previously. Usually, organizations already have some policies in place; therefore, identifying gaps between the governance principles and current, valid policies helps to redesign and improve the policy framework in use. In this phase, a logical structure of documentation that will support and clarify policy principles is defined. The optimal amount of documentation depends on the organization’s culture and management’s style; the objective of this activity is to improve clarity of policy principles and support their implementation.

• **Design**—There are two activities in this phase:
  1. **Priorities setup**—Identification of concrete policies, using a risk-based approach that addresses policy principles, setting deadlines and priorities for their review or creation.
  2. **Policy structure definition**—Writing a policy is not only a writing activity; it needs adequate coordination, including:
    - **Policy draft**—Identify the individuals responsible for researching and writing policies. A critical success factor is to resolve any potential issue concerning the feasibility for implementing policy principles.
    - **Policy review**—Identify the individuals responsible for providing an independent review. The objective of this activity is to increase the policy credibility and quality.
    - **Approval, communication and distribution**—Establish the procedure for obtaining final policy approval from the authorized individuals defined in the stakeholders dimension previously, and determine the policy communication and training strategy.
    - **Style**—Define writing quality standards, including document format, font type, language style, glossary of terms and document structure. The objective of this activity is to ensure that policies are written, presented and structured in a way that is clear, concrete, complete, consistent and easy to follow.

• **Implement**—This activity corresponds to implementation and enforcement policies, defining activities that will assist the organization in providing a transparent transition from a noncompliant to a compliant state.

• **Operate**—An effective policy should be part of the organization’s DNA. Building an accountable culture and using policies in daily operations ensures that the organization’s goals are met. In this phase, organizations should “walk the talk” of policy principles.

• **Evaluate/monitor**—This phase has the objective to confirm that policy requirements are properly implemented and the organization operates effectively. The degree of success of policy principles supporting business goals is evaluated, and the overall efficiency of the policy framework is communicated to relevant stakeholders.

• **Update/dispose**—To keep policies aligned with business direction, policies are reviewed for updating or removal. This activity has two objectives: to ensure that organizations have effective policies and to adjust the phases defined previously to maintain or improve the maturity of the policy framework. Good practice would require policies to be reviewed on a regular basis, typically every 12 months.

Good Practices Dimension

The separation of governance and management activities points out the need for more specific guidance on how policy principles are implemented and managed. A good practice is to create additional documentation to support policy effectiveness and efficiency, for example:

• **Standards**—A mandatory action, explicit rules, controls or configuration settings that are designed to support and conform to a policy. A standard should make a policy more meaningful and effective by including accepted specifications for hardware, software or behavior. Standards should always point to the policy to which they relate.

• **Procedures**—A written set of steps to execute policies through specific, prescribed actions; this is the *how* in relation to a policy. Procedures tend to be more detailed than policies. They identify the method and state in a series of steps how to accomplish an intended task, achieve a desired business or functional outcome, and execute the policy.

• **Guideline**—An outline for a statement of conduct. This is an additional (optional) document in support of policies, standards and procedures—general guidance on issues such as “what to do in particular circumstances.” These are not requirements to be met, but are strongly recommended.

• **Baseline**—A platform-specific rule that is accepted across the industry as providing the most effective approach to a specific implementation.

Creating policies is more than typing words on a page.
CONCLUSION

All organizations have policies that guide how decisions are made and how business objectives are achieved. An effective policy framework increases organizational accountability and transparency and is fundamental for helping the organization to meet its objectives.

Creating policies is more than typing words on a page; it involves a systematic approach for properly articulating governance and management principles. COBIT 5 principles help to provide a holistic approach to include all the minimum requirements for a policy framework, avoiding reinventing the wheel and ensuring that the complete life cycle of a policy is understood.

ENDNOTES

6 Bacik, Sandy; Building an Effective Information Security Policy Architecture, CRC Press, USA, 2008
7 Op cit, Tipton