Continuous media attention has highlighted the proliferation of security breaches affecting enterprises across numerous industries on a global basis. These security failures have not only resulted in significant expense to the affected enterprises, but have significantly damaged consumer trust and brand reputation. No longer relegated to the domain of the IT organization, the topic is now unquestionably a C-suite priority. Organizations need to move toward a more holistic and proactive approach to addressing security threats and managing compliance requirements in today’s information-driven economy. Thus, today, more than ever, enterprises need strong IT governance based on sound IT risk management in order to restore confidence in the security and privacy protections provided by governments and private industry worldwide.

To do this, a holistic approach is needed that embodies IT governance, security and privacy based on IT risk management—all working in concert and all essential for success—to ensure that the “right” decision is made every time and, more important, through a good decision-making process for consistency and accountability. Key for moving forward is a framework that integrates the policies within an overall enterprise governance approach. Figure 1 illustrates a holistic perspective of enterprise and IT governance through which organizations govern their IT operations, based on sound IT risk management and addressing security and privacy concerns, which will enhance effectiveness in implementing security and privacy across the enterprise. Each of these essential elements is briefly described in this article:

- **IT governance**—Provides the consistency, processes, standards and repeatability needed for effective IT operations at the lowest possible cost within compliance requirements. IT governance must be part of enterprise governance, a discipline that addresses all stakeholder needs, conditions and options to ensure that they are evaluated for determining balanced, agreed-on enterprise objectives to be achieved; sets direction through

---

**John W. Lainhart IV, CISA, CISM, CGEIT, CRISC, CIPP/G, CIPP/US**
Is cybersecurity fellow, Center for the Business of Government/Partner and chief information security officer, US Public Sector at IBM. As the Center’s first cybersecurity fellow, he is responsible for framing new approaches for government, collaborating with authors and third-party stakeholders, and ensuring that the Center’s work in this area adds value for government and taps into best commercial practices. He also represents IBM as a member of the board of directors of the Center for Cyber and Homeland Security (CCHS) at George Washington University (Washington DC, USA). He is a past international president of ISACA® and a thought leader of ISACA and ITGI initiatives, including the family of COBIT® products and publications. He can be reached at john.w.lainhart@us.ibm.com.

**Zhiwei Fu, Ph.D., CISA, CGEIT, CRISC, CFE, CISSP, ITIL, PMP**
Is the senior principal of governance, risk, and compliance and cybersecurity at IBM Global Business Services. Fu is a renowned researcher and practitioner in cybersecurity and business intelligence, predictive analytics, modeling and optimization, performance measurement, and process improvement, with multiple works published in international journals, book series and conference proceedings. He can be reached at zhiwei.fu@us.ibm.com.

**Christopher M. Ballister, CISM, CGEIT, CRISC**
Is an associate partner for IBM Global Business Services, supporting risk management, IT governance, information security and privacy. He provides subject matter expert support in a variety of cybersecurity areas based on his experience as a chief information officer and senior systems engineer and in multiple areas of executive government and industry. Ballister is a senior fellow for the George Washington University CCHS and a member of the CCHS Active Defense Task Force. He can be reached at cmballis@us.ibm.com.
As discussed in COBIT®, enterprises exist to create value for their stakeholders. Consequently, any enterprise—private or public—will have value creation as a governance objective. Value creation means realizing benefits at an optimal resource cost while optimizing risk (figure 2). Benefits can prioritization and decision making; and monitors performance and compliance against agreed-on direction and objectives. Governance and management of enterprise information and related technology is ultimately the board of directors’ or other governing entity’s) responsibility. The board sets the direction for management to achieve the enterprise objectives and is accountable to the enterprise stakeholders. Governance is typically thought of as the purview of senior leadership, but all stakeholders have a role to play, as good decisions cannot be made in a vacuum. Enterprises have many stakeholders, and creating value means different—and sometimes conflicting—things to each of them. Governance is about negotiating and deciding among different stakeholders’ value interests. By consequence, the governance system should consider all stakeholders when making benefit, risk and resource assessment decisions for IT operations. Increased IT governance improves the effectiveness of security and privacy controls.
take many forms, e.g., financial gain for commercial enterprises or public service for government entities.

• **IT risk management**—Identifies the alignment of critical business processes with supporting technology systems. IT risk management serves to focus IT governance, security and privacy investments in the areas contributing most to mission success. IT risk management must be a part of enterprise risk management (ERM), a discipline that addresses the full spectrum of an organization’s risk, including challenges and opportunities, and integrates them into an enterprise-wide, strategically aligned portfolio view. ERM contributes to improved decision making and supports the achievement of an organization’s mission, goals and objectives.² The Risk IT Framework³ and The Risk IT Practitioner Guide⁴ are based on existing and emerging practices and methodologies for effective IT risk management to form a set of guiding principles, featuring business processes and management guidelines that conform to these principles. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management—Integrated Framework⁵ has also been widely accepted and used across industries to enhance an organization’s ability to manage risk and improve understanding of opportunities to increase and preserve stakeholders’ values.

• **Information security**—Encompasses efforts to protect data and information systems from inappropriate access, manipulation, modification and destruction, ensuring the confidentiality, integrity and availability of the systems and data. This is normally managed by the enterprise’s chief information security officer (CISO). The US National Institute for Standards and Technology’s (NIST’s) Framework for Improving Critical Infrastructure Cybersecurity⁶ focuses on using business drivers to guide security activities while considering cybersecurity risk factors as part of the organization’s risk management processes and includes technology, processes, policies and people. This NIST Cybersecurity Framework is based on a set of industry standards (including COBIT) and best practices to help organizations manage cybersecurity risk and is gaining usage on a global basis. In order for the information security program to achieve an acceptable level of risk to operate, IT governance must incorporate a minimal level of maturity. COBIT® 5 for Information Security⁷ provides detailed and practical guidance to help information security professionals and other interested parties at all levels of the enterprise understand, utilize, implement and direct important information security–related activities and make more informed security decisions. ISO/IEC 27001 Information security management⁸ and other industry best practices have also been widely applied to help organizations keep information assets secure.

• **Privacy**—Within a secure enterprise, privacy controls allow only properly designated personnel to access information governed under privacy laws, and encompass efforts to protect an individual’s ability to determine how their personal information is collected, used, stored and disclosed. Information security and IT governance directly impact the success of a privacy program. Privacy cannot exist without information security. Privacy must be considered in all information security programs—the NIST Cybersecurity Framework includes the “Methodology to Protect Privacy and Civil Liberties,”⁹ which specifically addresses individual privacy and civil liberty implications that may result from cybersecurity operations. Finally, privacy must be part of the organization’s IT governance program to ensure that it is adequately addressed in all discussions where personally identifiable information (PII) is involved.

**A Road Map for Implementing and Improving IT Governance**

Optimal value can be realized from leveraging IT governance only if it is effectively adopted
and adapted to suit each enterprise’s unique environment. Effective implementation of IT governance requires a strong business case, the appropriate culture and environment, and a proper organizational structure. Each implementation approach must address specific challenges, including managing changes to culture and behavior. In addition, implementation must be based on a continual improvement life cycle.

“Optimal value can be realized from leveraging IT governance only if it is effectively adopted and adapted to suit each enterprise’s unique environment.”

Based on the experience of COBIT users (and the authors’ experiences implementing IT governance at a number of diverse organizations), it is critically important that the road map discussed herein be addressed up front before undertaking a project to implement or improve IT governance within an organization. The “tone at the top” is a critical first step—leadership at the top of the organization must support the efforts and let staff know that this is critical from his/her perspective. The business case must be strong to ensure this. In addition, creating the right environment—making sure that the implementation/improvement approach addresses the culture of the organization—is a critical success factor that is often overlooked. Finally, it may be that the organizational alignment needs to be changed or new organizations formed in order to effectively and efficiently implement the changes needed to achieve optimal value from the IT governance implementation/improvement program.

Making a Business Case for the Implementation and Improvement of IT Governance

IT governance does not occur in a vacuum. Every enterprise needs to design its own implementation plan depending on factors in the enterprise’s specific internal and external environment, including:

- Ethics and culture
- Applicable laws, regulations and policies
- Mission, vision and values
- Enterprisewide governance policies and practices
- Business plans and strategic intentions
- Operating model and level of maturity
- Management style and risk appetite
- Capabilities and available resources

Optimal value can be realized from leveraging IT governance only if it is effectively adopted and adapted to suit each enterprise’s unique environment.

It is critically important to leverage and build on existing enterprise governance initiatives. The optimal approach for implementing IT governance will be different for every enterprise, and the context needs to be understood and considered. Key success factors for successful implementation include:

- Top executives providing the direction and mandate for the initiative on an ongoing basis
- Visible, ongoing commitment and support from key leadership executives
- All parties supporting the processes to understand the business and IT objectives
- Ensuring effective communication and enablement of the necessary changes
• Tailoring good practices and standards to fit the unique context of the enterprise

• Focusing on quick wins and prioritizing the most beneficial improvements that are easiest to implement

IT governance implementation initiatives must be properly and adequately managed. Support and direction from key leadership executives can ensure that improvements are adopted and sustained. Requirements based on current challenges should be identified by management as areas that need to be addressed, supported by early commitment and buy-in from relevant key leadership executives, and enabled objectives and benefits that are clearly expressed in a business case. Following leadership commitment, ensuring adequate resources, and assigning key program roles and responsibilities will ensure sound implementation for the IT governance program with care taken on an ongoing basis to maintain commitment from all affected executives. Indeed, appropriate structures and processes for oversight and direction will also ensure ongoing alignment with enterprisewide governance and risk management approaches.

Successful implementation depends on implementing the appropriate changes in the appropriate ways. In many enterprises, there is a significant focus on the first aspect—core IT governance—but not enough emphasis on managing the human, behavioral and cultural aspects of change and motivating key leadership executives to buy into change. Indeed, various key leadership executives involved in, or impacted by, new or revised IT governance enablers may not readily accept and adopt change, making it necessary to address resistance through a structured and proactive approach. Also, a communication plan that defines what will be communicated, in what way and by whom, throughout the various phases of the program can optimize awareness of the implementation program. Human, behavioral and cultural barriers can be overcome to properly adopt change, instill the will to adopt change and ensure the ability to adopt change.

The implementation life cycle provides a way for enterprises to address typically encountered complexity and challenges. The three interrelated components of the life cycle are the core continual improvement life cycle (as opposed to a one-off project), change enablement (addressing the behavioral and cultural aspects) and program management (following generally accepted project management principles). The implementation life cycle and its seven phases are illustrated in figure 3 from COBIT 5.

The definitions of each phase include:

• Phase 1—What are the drivers? This phase starts with recognizing and agreeing to the need for an implementation or improvement initiative. It identifies the current pain points and triggers and creates a desire to change at executive management levels.

• Phase 2—Where are we now? This phase focuses on defining the scope of the implementation or improvement initiative using COBIT’s mapping of enterprise goals to IT-related goals to the associated IT processes, and considers how risk scenarios could also highlight key processes on which to focus.

• Phase 3—Where do we want to be? This phase sets an improvement target followed by a more detailed analysis leveraging COBIT’s guidance to identify gaps and potential solutions. Some solutions may offer quick wins and others might be more challenging.

• Phase 4—What needs to be done? This phase plans practical solutions by defining projects supported by justifiable business cases. A change plan for implementation is also developed.

• Phase 5—How do we get there? This phase implements the proposed solutions into day-to-day practices. Measures can be defined and
established using COBIT’s goals and metrics to ensure that business alignment is achieved and maintained and performance can be measured.

"Appropriate structures and processes for oversight and direction will also ensure ongoing alignment with enterprise-wide governance and risk management approaches."

• Phase 6—Did we get there? This phase focuses on the sustainable operation of the new or improved enablers and the monitoring of the achievement of expected benefits.

• Phase 7—How do we keep the momentum going? This phase reviews the overall success of the initiative, further identifies requirements for the governance or management of the enterprise, and reinforces the need for continual improvement.

Creating the Appropriate Environment for Successful Adoption of IT Governance

Managing the human, behavioral and cultural aspects of change and motivating key leadership executives to buy into the change is critical to the success of IT governance that supports an enterprise’s IT security program.

To start, guiding principles can ensure that all staff have a common understanding of the core IT governance criteria. These guiding principles let staff know that IT governance is recognized by the C-suite as critical to the organization’s success and that IT resources result in maximum effectiveness and efficiency across the organization. It ensures that security is integrated in meeting requirements and delivers benefits set by an organization’s business leaders. As a model, the US Department of Veterans Affairs (VA) established a number of principles that could be adapted by other organizations, followed by related imperatives and characteristics.
Those principles are called the IT Governance Guiding Principles and they include:10

• IT governance is critical to the success of the organization’s governance and business needs.
• Business (mission) requirements and benefit realization are the basis for setting IT priorities.
• Business leaders (administrations and staff officers) establish IT requirements, business benefits and priorities based on the organization’s strategic plan.
• Business leaders oversee full life cycle execution of the IT program to manage risk.
• The chief information officer’s (CIO) office determines technology solutions and IT-related life cycle costs.
• The CIO manages IT resources and IT program execution to maximum effectiveness and efficiency across the organization to meet requirements and deliver benefits set by business leaders.
• Existing organizational governance mechanisms are used to the maximum extent possible.
• CIO policies, procedures and processes must be published, communicated, monitored, measured and reported across the organization.
• IT governance enforcement must be equitable, timely and consistent.
• Industry/government best practices and standards are assessed and implemented as appropriate.

These and similar imperatives must be addressed up front for IT governance to be effectively implemented. These imperatives describe how people will operate within the new IT governance program—the need for trust and partnership to make the IT governance plan successful.

IT Governance Imperatives

• Build trust:
  – Trust must be built among the stakeholders in the management of information and technology in the enterprise.
  – Trust is not achieved in documents; it is achieved through cooperative partnerships between the business needs of the business and staff offices and the IT service provider.
  – Structure alone without a foundation of trust will not function effectively.
  – IT governance, by carefully defining roles and responsibilities, provides the requisite foundation to address the central theme of concern—how to establish trust among stakeholders in the management of information and technology in the enterprise.

  “Guiding principles can ensure that all staff have a common understanding of the core IT governance criteria.”

• Build partnerships:
  – IT governance is not an isolated discipline.
  – IT governance should form an integral part of an organization’s governance and needs to be addressed at the most senior levels of leadership.
  – IT governance can be seen as a structure of relationships and processes to direct and control the enterprise to achieve its enterprisewide goals by adding value while balancing risk vs. return over IT and its processes.

  – Senior leaders must ensure that IT operational risk factors are mitigated and the value that is returned by technology investments meets the strategic goals and objectives of the enterprise.
  – Day-to-day communication between the business and staff offices with various IT offices can help to ensure close coordination between the business and IT.
IT Governance Characteristics
Also, key characteristics or a list of the “rules of the game” are needed to guide the IT governance effort, and include:

• Builds relationships and processes to direct and control the enterprise in order to achieve the enterprise’s goals by adding value while balancing IT risk vs. return
• Specifies the distinction between input rights and decision rights to clarify the differences between advisory entities (such as steering committees) and those assigned to manage the process
• Specifies the accountability allocated between business requirement owners and the IT organization to encourage desirable behaviors in the use of IT
• Assures a process for managing and controlling the use of technology to create value for the organization and assure benefit realization
• Oversees the rules and regulations under which an IT organization functions to serve the business lines
• Ensures that everyone is playing by the same rules so that the IT environment works for everyone
• Adopts an attitude of “doing the right things right”

These guiding principles, imperatives and characteristics provide a model to help enterprises create the appropriate environment for addressing specific challenges, including managing changes to culture and behavior. Security and privacy must be based on a rigorous risk management process and a sound IT governance program. It is critical to establish a strong IT governance program before an organization can effectively address its security weaknesses and prevent future data breaches.

Aligning Organizational Structure for an Effective IT Governance Program With Strong Security
After organizations put an appropriate governance environment in place, they can implement a new and more secure approach to IT. This consists of communicating a definition of IT governance throughout the enterprise and establishing a new organizational structure to ensure that the IT governance program is effective and continuously improved. For example, the VA adopted an organizational structure to support its enterprise and IT governance based on its definition. The VA model provides an excellent example for enterprises to consider as they implement their IT governance.

The VA defines IT governance as, “A structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise’s goals by adding value while balancing risk versus return over IT and its processes.” This definition addresses the key issues of risk and value, which are two major components of IT governance (the other major component is resource optimization). This is done to ensure that stakeholder needs are being met, the most important of which to the VA is caring for US veterans, their widows and dependents, in an effective and secure manner. The definition was rolled out to all staff at the VA to ensure that all had a common vision of IT governance. Next, the VA developed the organizational structure (boards) necessary to ensure that the IT governance program was effectively implemented within the department. Figure 4 illustrates an example of the VA IT governance organizational structure, with a generic description of the IT governance functions provided as well.

Executive Board
The executive board performs the following functions:

• Serves as the senior board
• Approves enterprisewide IT strategy
• Decides the overall level of IT spending and priorities
• Establishes funding targets across lines of business in accordance with the enterprise’s strategic plan, US congressional or other mandates, etc.
• Assesses strategies, program initiatives and risk identification/reduction activities to ensure improved service to stakeholders, IT system and data security, and resource management
• Provides recourse for issues unresolved by the IT Leadership Board (ITLB)
Strategic Management Council
Chaired by the deputy secretary, the Strategic Management Council (SMC) serves as the senior board making decisions related to IT strategy and technology. It assures the formulation of budgets, strategic planning and policy processes, resource optimization, capital assets, planning and investment, risk management, and legislation. The SMC provides business recourse for issues unresolved by the ITLB. It meets at least quarterly and more frequently during the early stages of IT governance implementation. The SMC is the strategic, priority-setting, oversight and issue-resolution board for IT matters within the enterprise.

IT Leadership Board
The ITLB is chaired by the deputy secretary and includes the CIO, deputy undersecretaries and other key staff as determined by each assistant secretary. The ITLB represents the IT services, strategies, principles, governance and resources that support business organizations across the department and, more specifically, performs the following functions:

- Serves as the primary IT strategy and technology board
- Recommends IT spending levels
- Oversees IT resources and program execution
- Oversees the coordination and performance of IT services and support services
- Oversees IT system and data security
- Oversees enterprisewide privacy
- Makes decisions on budgeting and near-term issues and programming and long-term issues and recommendations
- Resolves disputes within IT governance

Budgeting and Near-term Issues Board
The Budgeting and Near-term Issues (BNTI) Board represents the business units and their needs/requirements for IT investments and monitors the fulfillment of those needs. Specifically, the BNTI Board performs the following functions:

- Develops the detailed budget documents supporting future-year budget formulation and current-year execution
• Monitors budget and technical performance execution-to-plan and makes recommendations for reallocation or reprogramming as warranted for ITLB consideration (mid-year review)
• Monitors performance such as service level agreements (SLAs) and other metrics
• Utilizes IT costing models and methodologies for validating execution-year budget recommendations
• Enforces technical/information security and privacy standards throughout the budgeting process
• Addresses near-term issues as required

It is essential to implement a continuous improvement process...for evaluating IT governance transformation...

Programming and Long-term Issues Board
The Programming and Long-term Issues (PLTI) Board recommends the overall enterprisewide priorities for IT-related business solutions and defines IT service offerings, infrastructure and technology architecture/standards. It is critical to assuring standardization, interoperability, security, privacy, reliability and flexibility of the IT infrastructure. Specifically, the PLTI Board performs the following functions:
• Develops the weighting criteria and prioritization methodology for long-term, multi-year IT programming

• Utilizes ITLB-approved weighted criteria, and develops future year IT program/project priorities consistent with the enterprise’s IT architecture, IT strategy, strategic goals, lines of business priorities and previous-year funding allocation
• Develops options and recommendations for the program/project “cut line” based on fiscal reality, the prior year’s execution, IT ability to execute, etc.
• Utilizes IT costing models and methodologies for validating future-year budget recommendations
• Evaluates business cases and priorities, including required supporting infrastructure
• Evaluates adherence to technical/information security and privacy standards
• Conducts milestone reviews
• Identifies IT services and required funding for future SLAs and other metrics
• Recommends technology strategy and enabling technology initiatives and priorities
• Addresses long-term issues as required
• Ensures that security, privacy and risk management are integrated within the IT governance program thereby ensuring that stakeholder needs are met in an effective and secure manner

It is essential to implement a continuous improvement process, as the VA has, for evaluating IT governance transformation, not only to gauge prior progress toward a final enterprisewide vision, but also to ensure that IT is being effectively deployed to support all those working or being served by the enterprise in a secure manner. This approach provides a model for organizations in both public and private industry to adapt to their own journey toward IT governance maturity.

Benefits That Can Be Achieved by Establishing Effective IT Governance

There are significant benefits that can be achieved by establishing a sound IT governance program at an organization. Several IT governance implementation
cases and lessons learned assisting organizations implement and/or improve their IT governance programs are cited in this section. These lessons learned apply to all organizations—and these are just a few selected organizations, many more success stories exist in addition to these discussed.

Case 1
The VA needed to transform the way it governed and managed IT within the department. It created three boards: an ITLB, a BNTI board and a PLTI board. The key accomplishments included:

- Approaching IT governance in the “right way,” enabling it to deliver better results to its constituents
- Increasing its enterprisewide governance understanding and adopting a new approach to IT governance, positioning it for maximum business effectiveness and improved success over the long term
- Institutionalizing IT governance committees with charters, policies, standards and procedures for critical IT decision making across the organization
- Transforming its business framework and moving to a more effective and efficient IT environment
- Developing a more effective regulatory and governance framework for overall business operations
- Developing a framework for enhanced participation, transparency and accountability in the alignment of IT to the business and the management of IT itself
- Developing a plan to implement and sustain IT governance for the benefit of all—employees, constituents and other stakeholders
- Developing a framework for organizing the IT workforce under a centralized model
- Assigning roles and responsibilities for IT management to effectively deal with oversight organizations on IT matters
- Moving its IT organization to a process-based organization defining the target environment for transformation
- Institutionalizing management practices based on industry best practices described in COBIT 5 and Information Technology Infrastructure Library (ITIL)\(^\text{12}\)
- Establishing metrics to track implementation progress and performance improvements
- Comparing the department’s strategic plan to the activities required by the US Federal Information Security Management Act of 2002 (FISMA)\(^\text{13}\) and modifying the strategic plan to bring it into complete alignment with FISMA
- Producing a gap report, assessing departmental policy, procedures and tools for data security and identifying gaps and recommended remediation in key areas identified
- Developing a performance management plan that detailed the tasks, milestones, resources and completion dates for remediating data security weaknesses
- Diagnosing and solving a major business and IT challenge for the C-suite by implementing business, applications and processes, and IT general controls that met both internal and external audit requirements

Case 2
A US federally regulated financial institution established four IT governance committees: Enterprise Architecture Committee, Change Authorization Board, IT Controls Committee and IT Governance Leadership Committee. Some key accomplishments achieved include the following:

- The Enterprise Architecture Committee eliminated half of the 950 software packages that were being maintained by staff at the organization, resulting in more efficient and effective use of the staff and eliminating the maintenance costs of the software packages, saving millions of dollars for
the organization—and this was just the first round of reviews. More software was eliminated as the process continued.

- Forty change control committees were replaced by the Change Authorization Board. Rather than allowing software and data changes to be implemented in a haphazard manner, all changes went through this one board. This resulted in controlled implementations of changes and, for the first time, a decision to not implement a major new software platform until the entire system could be thoroughly tested and accredited by the CIO—something that had never been done before at the organization.

- The IT Controls Committee implemented COBIT’s control objectives and control practices for all of its IT general and application controls, resulting in the institution getting a clean audit and Sarbanes-Oxley Section 404 opinion that had eluded this institution for three years. It allowed the organization to register its common stock with the US Security and Exchange Commission (SEC), which increased investor confidence and its stock value.

- The IT Governance Leadership Committee developed a dashboard that allowed the CIO, chief operating officer (COO) and chief executive officer (CEO) to visualize the organization’s IT general and applications controls posture for the entire institution on one “pane of glass.”

**Case 3**
A US health insurance company, faced with a multitude of process audits each year, needed to make its response to audits consistent in order to reduce the overall impact on the business and establish compliance with new insurance industry regulatory requirements. Because of the central role IT played in the running of the business, leadership knew it needed to implement an appropriate IT governance program to ensure good enterprise governance. Some key accomplishments were:

- Collaboratively instituting industry-standard IT governance controls that spanned all of the company’s operations, which ensured high internal standards and uniform procedures and helped to achieve regulatory compliance

- Assessing and implementing key IT processes based on COBIT

- Implementing a continuous process for monitoring compliance with industry regulations and standards

- Reducing the amount of effort needed for audit response by approximately half

- Creating more effective, uniform responses to audits

- Better supporting regulatory compliance

- Implementing IT governance enterprisewide

**Conclusion**
IT governance has become critically important on a global basis to today’s enterprises, whether public or private. It is critical that a strong IT governance program be established so that organizations can effectively address their security weaknesses and prevent future data breaches. To that end, public and private sector organizations alike should implement a holistic approach that embodies IT governance, security and privacy based on IT risk management all working in concert and essential for success. Effective IT governance creates clarity of, and establishes proper relationships between, enterprise mission, business strategy and IT goals; sets direction through prioritization and decision making; ensures that stakeholder needs, conditions and options are evaluated and balanced; and ensures that agreed-on enterprise objectives are continually monitored and improved. IT governance implemented through a holistic approach has proven to be effective in helping to ensure that organizations make the “right” decision every time and, more importantly, arrive at those decisions through a good decision-making process for consistency and accountability.

**References**


ISACA, *COBIT® 5 for Assurance*, USA, 2013


ISACA, *COBIT® 5 Implementation*, USA, 2012

ISACA, *The Val IT Framework*, USA, 2008
Information Technology Industry Council, ITI’s IT Alliance for Public Sector Task Force Recommendations, IT Alliance for Public Sector, USA, 2015, www.itic.org/dotAsset/5/1/511cc94e-ca93-4d7c-87cd-678c05af7495.pdf


Project Management Institute, Project Management Body of Knowledge (PMBOK2), USA, 2008

Endnotes

1 ISACA, COBIT® 5: A Business Framework for the Governance and Management of Enterprise IT, USA, 2012
3 ISACA, The Risk IT Framework, USA, 2009
4 ISACA, The Risk IT Practitioner Guide, USA, 2009
5 Committee of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Management—Integrated Framework, USA, 2004
6 National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, USA, 2014
7 ISACA, COBIT® 5 for Information Security, USA, 2012
9 Op cit, NIST
11 Ibid.