

# IT CONTROL OBJECTIVES

---

# SAMPLE

---

*for* **CLOUD  
COMPUTING:**

**CONTROLS AND ASSURANCE IN THE CLOUD**



*Trust in, and value from, information systems*

### ISACA®

With 95,000 constituents in 160 countries, ISACA ([www.isaca.org](http://www.isaca.org)) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. Founded in 1969, the nonprofit, independent ISACA hosts international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations. ISACA continually updates COBIT®, which helps IT professionals and enterprise leaders fulfill their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business.

### Disclaimer

ISACA has designed and created *IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud* (the “Work”) primarily as an educational resource for security and control professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, security and control professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

### Reservation of Rights

© 2011 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorization of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and noncommercial use and for consulting/advisory engagements, and must include full attribution of the material’s source. No other right or permission is granted with respect to this work.

### ISACA

3701 Algonquin Road, Suite 1010  
Rolling Meadows, IL 60008 USA  
Phone: +1.847.253.1545  
Fax: +1.847.253.1443  
E-mail: [info@isaca.org](mailto:info@isaca.org)  
Web site: [www.isaca.org](http://www.isaca.org)

ISBN 978-1-60420-185-7

*IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud*  
Printed in the United States of America

CRISC is a trademark/service mark of ISACA. The mark has been applied for or registered in countries throughout the world.

## ACKNOWLEDGMENTS

### ISACA wishes to recognize:

#### Development Team

Phillip J. Lageschulte, CGEIT, CPA, KPMG LLP, USA, Chair  
 Steven Babb, CGEIT, CRISC, KPMG LLP, UK  
 Jeimy J. Cano M., Ph.D., CFE, CMAS, Ecopetrol S.A., Colombia  
 Joshua Davis, CISA, CISM, CRISC, CISSP, Qualcomm Inc., USA  
 Urs Fischer, CISA, CRISC, CIA, CPA (Swiss), Switzerland  
 Sailesh Gadia, CISA, ACA, CIPP, CPA, KPMG, USA  
 Ramses Gallego, CISM, CGEIT, CISSP, Entel IT Consulting, Spain  
 Jeff Kalwerisky, CISA, CA (SA), HISP, CPEInteractive, USA  
 Norm Kelson, CISA, CGEIT, CPA, CPEInteractive, USA  
 Nitin Khanapurkar, CISA, CISM, CGEIT, ACA, AICWA, CFE, CISSP, MBCI, KPMG, India  
 Mark A. Lundin, CISA, CISSP, CPA, KPMG LLP, USA  
 Peet Rapp, CISA, Rapp Consulting LLC, USA  
 Jeff Spivey, CRISC, CPP, PSP, Security Risk Management, USA

#### Expert Reviewers

Niall Browne, CISA, CCSI, CCSP, CISSP, LiveOps, USA  
 Jeimy J. Cano M., Ph.D., CFE, CMAS, Ecopetrol S.A., Colombia  
 Nitin Khanapurkar, CISA, CISM, CGEIT, ACA, AICWA, CFE, CISSP, MBCI, KPMG, India  
 Marc Vael, CISA, CISM, CGEIT, CISSP, Valuendo, Belgium  
 Anna Maria Yrjana, CISA, Tieto Finland OY, Finland

#### ISACA Board of Directors

Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd., USA, International President  
 Christos K. Dimitriadis, Ph.D., CISA, CISM, INTRALOT S.A., Greece, Vice President  
 Ria Lucas, CISA, CGEIT, Telstra Corp. Ltd., Australia, Vice President  
 Hitoshi Ota, CISA, CISM, CGEIT, CIA, Mizuho Corporate Bank Ltd., Japan, Vice President  
 Jose Angel Pena Ibarra, CGEIT, Alintec S.A., Mexico, Vice President  
 Robert E. Stroud, CGEIT, CA Technologies, USA, Vice President  
 Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Vice President  
 Rolf M. von Roessing, CISA, CISM, CGEIT, Forfa AG, Germany, Vice President  
 Lynn C. Lawton, CISA, FBCS CITP, FCA, FIIA, KPMG Ltd., Russian Federation,  
 Past International President  
 Everett C. Johnson Jr., CPA, Deloitte & Touche LLP (retired), USA, Past International President  
 Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Director  
 Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government,  
 Australia, Director  
 Howard Nicholson, CISA, CGEIT, CRISC, City of Salisbury, Australia, Director  
 Jeff Spivey, CRISC, CPP, PSP, Security Risk Management, USA, ITGI Trustee

#### Knowledge Board

Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Chair  
 Michael Berardi Jr., CISA, CGEIT, Nestle USA, USA  
 John Ho Chi, CISA, CISM, CBCP, CFE, Ernst & Young LLP, Singapore  
 Jose Angel Pena Ibarra, CGEIT, Alintec S.A., Mexico  
 Jo Stewart-Rattray, CISA, CISM, CGEIT, CSEPS, RSM Bird Cameron, Australia  
 Jon Singleton, CISA, FCA, Auditor General of Manitoba (retired), Canada  
 Patrick Stachtchenko, CISA, CGEIT, CA, Stachtchenko & Associates SAS, France  
 Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA

## ACKNOWLEDGMENTS (CONT.)

### **Guidance and Practices Committee**

Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Chair  
Kamal N. Dave, CISA, CISM, CGEIT, Hewlett-Packard, USA  
Urs Fischer, CISA, CRISC, CIA, CPA (Swiss), Switzerland  
Ramses Gallego, CISM, CGEIT, CISSP, Entel IT Consulting, Spain  
Phillip J. Lageschulte, CGEIT, CPA, KPMG LLP, USA  
Ravi Muthukrishnan, CISA, CISM, FCA, ISCA, Capco IT Service India Pvt. Ltd., India  
Anthony P. Noble, CISA, CCP, Viacom Inc., USA  
Salomon Rico, CISA, CISM, CGEIT, Deloitte, Mexico  
Frank Van Der Zwaag, CISA, Westpac New Zealand, New Zealand

### **ISACA and IT Governance Institute® (ITGI®) Affiliates and Sponsors**

American Institute of Certified Public Accountants  
ASIS International  
The Center for Internet Security  
Commonwealth Association for Corporate Governance Inc.  
FIDA Inform  
Information Security Forum  
Institute of Management Accountants Inc.  
ISACA chapters  
ITGI Japan  
Norwich University  
Solvay Brussels School of Economics and Management  
Strategic Technology Management Institute (STMI) of the National University of Singapore  
University of Antwerp Management School  
ASI System Integration  
Hewlett-Packard  
IBM  
SOAProjects Inc.  
Symantec Corp.  
TruArx Inc.

# TABLE OF CONTENTS

<b>1. Cloud Computing Preface</b> .....	7
Using This Publication.....	7
Introduction to Cloud Computing.....	9
Cloud Computing Deployment Models and Service Delivery Models.....	10
Service Delivery Models.....	11
Cloud Deployment Models.....	12
<b>2. Cloud Computing Fundamentals</b> .....	15
Evolution of the Cloud.....	15
The Technical Building Blocks.....	18
Essential Cloud Computing Characteristics.....	19
Cloud Drivers.....	20
Cloud Computing Challenges.....	21
<b>3. Governance in the Cloud</b> .....	25
Business and Governance of Enterprise IT (GEIT).....	25
Cloud IT Benefits/Value Enablement Risk.....	26
ISACA’s GEIT and Management Frameworks and Models.....	27
Leveraging and Integrating IT Governance Frameworks, Standards and Good Practices.....	27
Strategic Vision.....	30
Risk IT for the Cloud.....	31
Val IT for the Cloud.....	33
Business Case Development.....	34
How and Why to Use COBIT.....	35
Governance Considerations.....	36
Establishing Business Goals for the Cloud.....	36
Linking IT and Business With COBIT.....	37
Mapping Governance to the COBIT, Risk IT and Val IT Frameworks.....	40
Outcome of Good Governance.....	43
<b>4. Security and Cloud Computing</b> .....	45
Businesses Are Ready for the Cloud.....	45
Risk Considerations.....	46
Graduated Risk Responsibilities.....	47
IAM.....	49
Physical Security.....	50
Operational Risk.....	50
Security Concerns.....	51
Secure Code.....	53

## TABLE OF CONTENTS (*CONT.*)

<b>5. Assurance in Cloud Computing</b> .....	55
Assurance by CSP .....	56
Many Requirements and Standards.....	57
Many Assurance Frameworks .....	58
Unified IT Compliance Approach.....	65
Key Elements of a Unified IT Compliance Program .....	65
Assurance for Cloud Clients .....	66
Assurance Through the Vendor Management Process .....	66
Assurance Provided by CSP Clients' Independent Auditors/Assessors .....	68
 <b>Appendix A. IT Control Objectives for Cloud Computing</b> .....	69
 <b>Appendix B. Cloud Computing Management Audit/Assurance Program</b> .....	113
I. Introduction.....	113
II. Using This Appendix.....	114
III. Controls Maturity Analysis .....	118
IV. Assurance and Control Framework .....	121
V. Executive Summary of Audit/Assurance Focus .....	121
VI. Audit/Assurance Program .....	126
VII. Maturity Assessment.....	168
VIII. Assessment Maturity vs. Target Maturity .....	176
 <b>Glossary</b> .....	177
 <b>ISACA Professional Guidance Publications</b> .....	189

# 1. CLOUD COMPUTING PREFACE

As enterprises look for innovative ways to save money and increase the trust and value in their information systems, cloud computing has emerged as an important platform, offering enterprises a potentially less expensive model to handle their computing needs and accomplish business objectives. Cloud computing offers enterprises many possible benefits, which are discussed throughout this publication. Some of these benefits include:

- Optimized server utilization
- Cost savings for cloud computing clients and the transitioning of capital expenses (CAPEX) to operating expenses (OPEX)
- Dynamic scalability of IT power for clients
- Shortened life cycle development of new applications or deployments
- Shortened time requirements for new business implementations

As cloud computing continues to escalate in importance and evolve, it is important that enterprises understand how to best handle the paradigm change in business operations that the cloud presents. This level of understanding will enable enterprises to maximize the benefits that cloud platforms offer, while simultaneously addressing the cloud's unique and emerging threats and vulnerabilities.

## Using This Publication

The purpose of this publication is to:

- Provide readers with an understanding of cloud computing, its technology enablers and the business drivers behind this new IT platform
- Identify the related risks, controls and frameworks that can be used to address challenges and maximize value in the cloud

Readers will not only learn how to understand the cloud computing landscape, but also to build the relevant controls and governance mechanisms around it.

There is no question that significant cloud business opportunities are available; at the same time, there are also many recognized information security risks to be addressed. This book provides insight into how frameworks and tools such as COBIT, Risk IT, Val IT™ and the Business Model for Information Security™ (BMIS™) can assist enterprises in assessing the cloud's business value vs. its business risk, to determine whether the risk aligns with the established levels of risk within the enterprise and whether the rewards are worth the cost and effort to mitigate that risk.

This publication also provides useful guidance for enterprises that are considering promoting data and business processes into a cloud environment. ISACA is committed to providing practical guidance and direction for members through publications such as this one and its frameworks/model (COBIT, Risk IT, Val IT and BMIS). These governance and control frameworks/model can help information

security and risk specialists objectively quantify the possible business benefits available from cloud computing measured against the security challenges. These tools provide risk governance metrics from many perspectives: internal (from within the current IT enterprise), from the cloud service provider (CSP) view, and from external legal and regulatory factors.

Various ISACA management and governance publications are identified in this book to provide the means to determine whether a cloud environment is appropriate for the data and business application in consideration. In addition, this document provides practical guidance for the design and operation of monitoring activities over IT controls within traditional IT enterprises. Effective IT-enabled monitoring can be of benefit to senior management, which includes the governance bodies, audit committee and board of directors. This is of utmost importance in the merging of traditional internal enterprises with those in the cloud.

Management should carefully consider the monitoring mechanisms that are appropriate and necessary for the enterprise's own circumstances. Management may choose not to include all of the activities and approaches discussed in this document and, similarly, may choose activities not mentioned in this document. In either case, customization of the approaches described in this document will undoubtedly be necessary to reflect the specific circumstances of each enterprise.

There are many variables, values and risk in any cloud opportunity or program that affect the decision whether a cloud application should be adopted from a risk/business value standpoint. Each enterprise has to weigh those variables to decide for itself whether the cloud is an appropriate solution.

Many of the values and risk associated with the cloud will vary based on certain factors:

- **The type of cloud service models: Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS)**—Each of the three cloud service models (detailed in an upcoming section) has varied business purposes and levels of business risk.
- **The robustness of the enterprise's existing IT operations**—Enterprises need to ensure that their own governance, risk management and security are well defined and managed within the existing IT operations. New threats and vulnerabilities may be identified in the cloud, but if the enterprise is prepared to handle the issues, the overall risk to the enterprise may be lower.
- **An enterprise's current level of business risk acceptance**—The level of risk an enterprise is willing to accept varies among industries and among enterprises within the same industry.
- **The aggregated "street value" of the data to be promoted to the cloud**—With acknowledged cybercriminals seeking to penetrate enterprises' clouds for financial gain, enterprises need to assess the value of the data promoted to the cloud in terms of the potential value those data may hold for people with malicious intent.

- **An enterprise’s internal security classification of data being promoted to the cloud**—In addition to the criminal “street value” of data promoted to the cloud, the data have internal value to the enterprise, which provides the enterprise a vested interest in keeping them proprietary and not releasing them publicly.
- **The identified compliance obligations of the data shared within the cloud**—Personally identifiable information (PII) security controls and financial reporting compliance are two prime examples of compliance obligations that need to be managed in the cloud.
- **The risk from the CSP**—Enterprises must exercise due diligence when considering moving services to the cloud. Since no consistent cloud security standards have yet been commonly accepted, CSPs may have different approaches to cloud security. CSPs should be following best practices and making use of internationally accepted standards such as the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001/27002. It is very important for enterprises to have defined their own requirements well enough to be able to reap the maximum benefit from the due diligence phase.

One of the benefits that frameworks such as COBIT offer is that they produce a summary assessment of the business risks and achieved business value of an application, and they can help practitioners evaluate (often to a highly granular degree) many security or value issues.

## Introduction to Cloud Computing

Cloud computing is defined by the US National Institute of Standards and Technology (NIST) as a:<sup>1</sup>

*Model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*

Cloud computing has often been likened to utility service. In many countries, utilities such as electricity are available when needed and to the extent needed. Users pay for this service by the amount used. CSPs have adopted this bill-for-service model, and as a result, cloud computing users pay by the central processing unit (CPU) cycles measured and by the amount of data storage required over time. This billing model enables enterprises to save money by not paying for unused or underutilized equipment, power, etc.

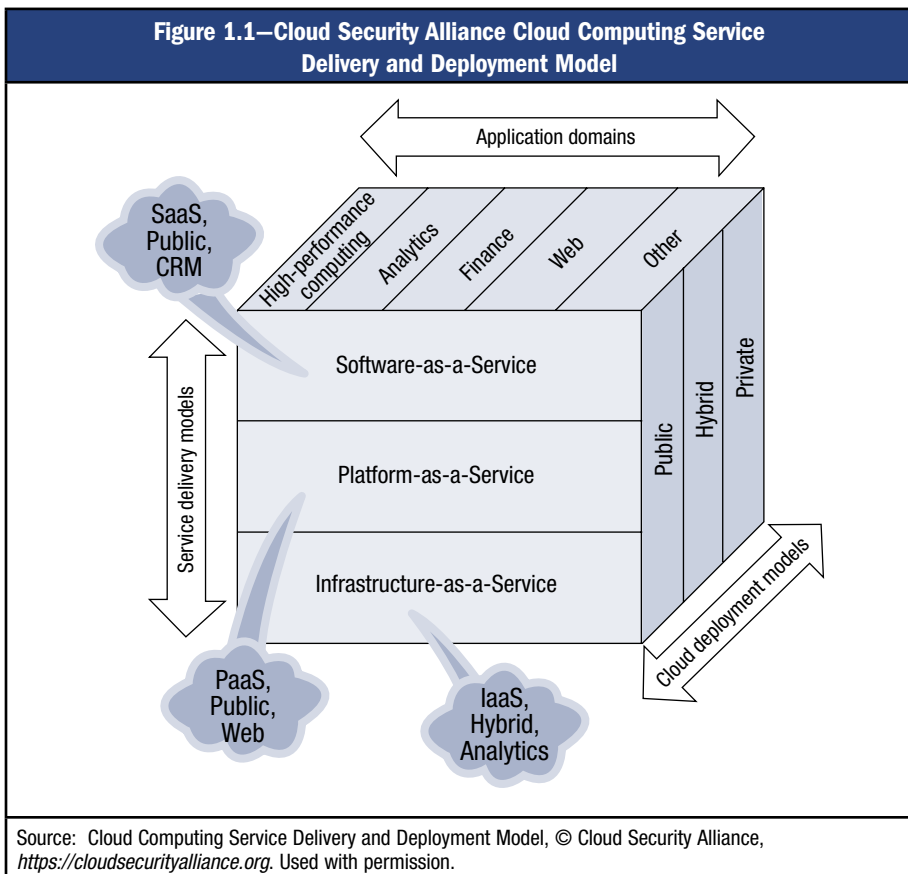
---

<sup>1</sup> Mell, Peter; Timothy Grance; US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145 (Draft), The NIST Definition of Cloud Computing, NIST, USA, 2011

Virtualization is one technique often used in cloud computing. By consolidating many instances of (virtualized) servers on a single physical server, enterprises lower their hardware expenditures. In addition to lower capital expenditures, virtualized environments enable enterprises to save on maintenance and energy, often resulting in a reduced total cost of ownership (TCO). Virtualization facilitates computer operating systems (OSs), applications and data to be transferred from computer to computer as needed. The actual physical location of the OS, application and data (referred to as the “platform”) is irrelevant. Where and to what extent this platform resides is determined by the volume of user demand and the physical location of available processing power.

## Cloud Computing Deployment Models and Service Delivery Models

By combining the concept of computer virtualization with the NIST definition (on-demand computer resources requiring minimal management effort), cloud computing offers enterprises virtual processing power in a variety of possible implementations (**figure 1.1**).



### Service Delivery Models

Cloud computing is implemented in three delivery models: SaaS, PaaS and IaaS (SPI) (figure 1.2). Each delivery model provides a distinct computing service to the enterprises that utilize them:

- **IaaS**—Provides online processing or data storage capacity. This cloud service is ideal for enterprises considering very large, one-time processing projects or infrequent, extremely large data storage requirements (i.e., test environments). IaaS offers the capability to provision processing, storage, networks and other fundamental computing resources, enabling the customer to deploy and run arbitrary software, which can include OSs and applications.
- **PaaS**—Provides the application development sandbox in the cloud. PaaS provides the capability to deploy customer-created or -acquired applications developed using programming languages and tools offered by the provider. The CSP offers organization developers elemental service-oriented architecture (SOA) application building blocks to configure a new business application. In-house development requires development, testing and user acceptance platforms, all separate from the production environment. Through PaaS, organization developers can rent their development environment complete with an SOA tool kit, and they are charged only for the time the tools and environment are in use.
- **SaaS**—Provides a business application used by many individuals or enterprises concurrently. SaaS provides the most used cloud applications to nearly everyone online. Facebook, G-mail™, LinkedIn®, Yahoo® user applications, Google Docs and Microsoft® Online Services are all popular consumer-directed SaaS applications. SaaS allows customers to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser.

**Figure 1.2—Cloud Computing Service Models**

Service Model	Description	Considerations
IaaS	Capability to provision processing, storage, networks and other fundamental computing resources, offering the customer the ability to deploy and run arbitrary software, which can include OSs and applications. IaaS puts these IT operations into the hands of a third party.	IaaS can provide infrastructure services such as servers, disk space, network devices and memory.  Example CSPs: <ul style="list-style-type: none"> <li>• Amazon Web Services™</li> <li>• Mosso from Rackspace®</li> </ul>
PaaS	Capability to deploy onto the cloud infrastructure customer-created or customer-acquired applications developed using programming languages and tools supported by the provider	PaaS is designed for developers.  Example vendors and services: <ul style="list-style-type: none"> <li>• Microsoft's Azure™ Services Platform</li> <li>• Google's Google App Engine</li> <li>• Salesforce.com's Force.com®</li> </ul>

Figure 1.2—Cloud Computing Service Models (cont.)

Service Model	Description	Considerations
SaaS	Capability to use the provider's applications running on cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based e-mail).	<p>Applications are complete and available on demand to the customer. Traditional licensing and asset management are changed.</p> <p>Example CSPs:</p> <ul style="list-style-type: none"> <li>• Microsoft Online Services</li> <li>• Salesforce customer relationship management (CRM)</li> <li>• LotusLive™ from IBM®</li> </ul>
<p>Source: Pijanowski, Keith; "Understanding Public Clouds: IaaS, PaaS and SaaS," Keith Pijanowski's Blog, 31 May 2009, <a href="http://www.keithpij.com/Home/tabid/36/EntryID/27/Default.aspx">www.keithpij.com/Home/tabid/36/EntryID/27/Default.aspx</a></p>		

### Cloud Deployment Models

The three cloud service delivery models are offered to cloud customers in four cloud deployment models: private, public, community and hybrid:

- **Private cloud**—Has one enterprise as its user. Several different departments or divisions may be represented, but all exist within the same enterprise. Private clouds often employ virtualization within an enterprise's existing computer servers to improve computer utilization. A private cloud typically also involves provisioning and metering components, enabling rapid deployment and chargeback where appropriate. This model is most closely related to the existing IT outsourcing models in the marketplace, but can be an enterprise's internal delivery model as well.
- **Public cloud**—An offering from one CSP to many clients who share the cloud processing power concurrently. Public cloud clients share applications, processing power and data storage space communally. Client data are commingled, but segregation is provided through the use of metatags.
- **Community cloud**—A private-public cloud with users having a common connection or affiliation, such as a trade association, the same industry or a common locality. The community cloud business model allows a CSP to provide cloud tools and applications specific to the needs of the community. When the community is in a PaaS cloud, the SOA applets can be specific to communal requirements, e.g., business-process-specific, industry-specific.
- **Hybrid cloud**—A combination of two or more of the previously mentioned deployment models. Each of the three cloud deployment models has specific advantages and disadvantages relative to the other deployment models. A hybrid cloud leverages the advantage of the other cloud models, providing a more optimal user experience.

Of the matrix of cloud delivery/deployment variants, a private cloud deployment of any delivery model is the most similar to traditional IT enterprises and, thus, offers the least amount of new risk and security challenges. A public cloud deployment of any variant, but likely in an SaaS delivery with the most number of concurrent users, will present security and risk managers with the greatest assurance challenges.

Figure 1.3 summarizes the available cloud deployment models.

Figure 1.3—Cloud Deployment Models	
Deployment Model	Description
Private cloud	<ul style="list-style-type: none"> <li>• Operated solely for an enterprise</li> <li>• May be managed by the enterprise or a third party</li> <li>• May exist on- or off-premise</li> </ul>
Public cloud	<ul style="list-style-type: none"> <li>• Made available to the general public or a large industry group</li> <li>• Owned by an organization selling cloud services</li> </ul>
Community cloud	<ul style="list-style-type: none"> <li>• Shared by several enterprises</li> <li>• Supports a specific community that has a shared mission or interest</li> <li>• May be managed by the enterprises or a third party</li> <li>• May reside on- or off-premise</li> </ul>
Hybrid cloud	<ul style="list-style-type: none"> <li>• A composition of two or more clouds (private, community or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)</li> </ul>

Levels of information security vary among the private, community and publicly deployed clouds, with private clouds having the most limited user access and, most likely, the fewest new threats. Public clouds may have a less constrained user access and may be exposed to the greatest number of new threats.

Likewise, the costs of services vary across the different deployment models. Private cloud services are currently the most costly option, public clouds the least. For users looking to save on expenses, the hybrid cloud offers a combination of two or more deployment models with varying levels of security as needed. Users can choose to leverage private or community clouds for their most business-critical data while choosing to utilize the public cloud for data that are already publicly available or for other nonclassified data or applications. Some enterprises may just accept the risk and go to the public cloud regardless of data classification. The decision on how to leverage the cloud will be unique to each enterprise.

Because of the dynamic and evolving nature of this industry and the currently limited acceptance of standards or security certifications, offerings of CSPs are not standardized. It is the responsibility of prospective cloud clients to determine the amount of security provisioning they will require in light of the type of application and the security classifications of the data they would promote into the cloud.

**Page intentionally left blank**

## 2. CLOUD COMPUTING FUNDAMENTALS

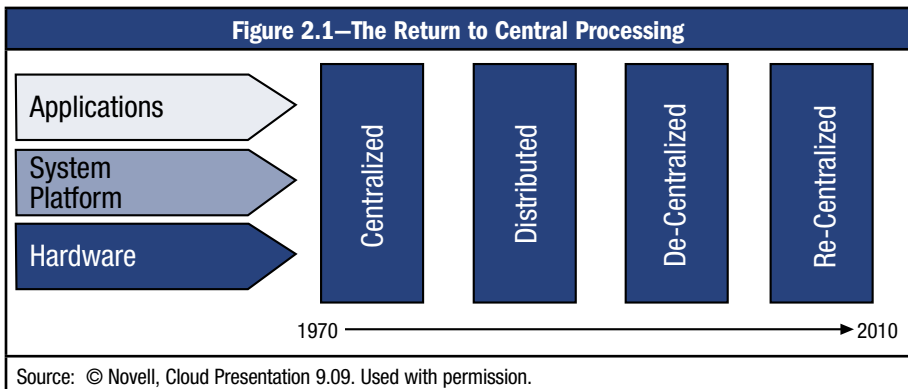
As with many emerging technologies, there are a variety of definitions and understandings of cloud technology. It is, therefore, important to clearly define it so that there is a common understanding of the technology, benefits, risk and governance of a cloud computing technology platform. This book utilizes NIST’s definition. (See page 9.)

### Evolution of the Cloud

The aggregation of technologies into today’s cloud computing services was first successfully accomplished by several of today’s largest CSPs—for their own internal use. Enterprises such as Amazon and Google demonstrated internally the business benefits obtained by successfully implementing the cloud’s “technical building blocks,” described later in this chapter. These enterprises then leveraged their own in-house expertise in virtual computing and created the cloud computing service offerings that are now available to the public.

Since then, cloud computing has evolved and is now commonly viewed as a major technology enhancement similar to the Internet. However, cloud computing is not really new; it has been built on existing infrastructure and processes. As depicted in **figure 2.1**, cloud computing has many similarities to the computer processing methods of the 1960s and 1970s. For example, 40 years ago, computing was centralized within enterprises, with large-scale operations using interfaces with mainframe computers. User interfaces were limited primarily to dumb terminals or punch cards. The 1980s delivered mid-sized computers and minicomputers, which enabled computer processing to be distributed and accessed more readily throughout an enterprise. With the adoption of the Windows® OS in the 1990s, computer processing was further distributed via client-server or simply client applications to nearly every office desktop, factory or warehouse station in an enterprise.

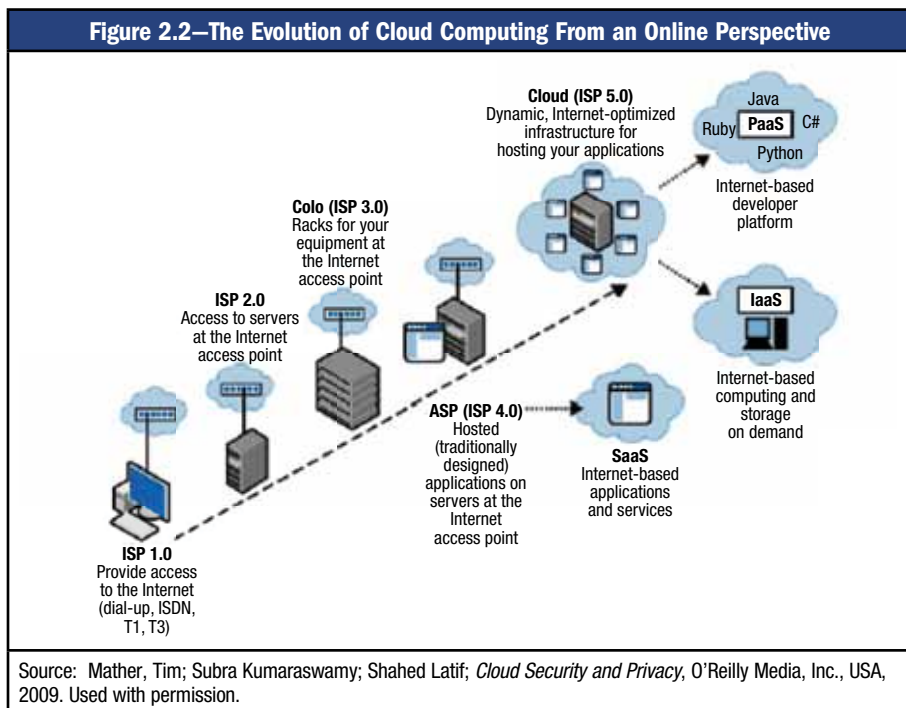
In 2011, cloud computing is now returning users to centralized processing. Services are provided from hosts within the Internet. Through the World Wide Web, cloud computing is seen as the new mainframe.



While many similarities exist, there are major differences between today's centralized cloud and the original mainframes. Among the notable differences are:

- Cloud processing power is much greater than that of the original mainframes.
- Storage capabilities have increased exponentially.
- The cloud allows a much larger number of user clients to connect.
- Connectivity is now over the World Wide Web; the transport protocols have changed.

The cloud evolution can be viewed as the progressive integration of the Internet with computer processing, data storage and data retrieval. **Figure 2.2** illustrates the online perspective of the evolution of cloud computing.



Initial user exposures to the precursors of the cloud came when the Internet provided e-mail messaging between Internet-connected computer users beginning in 1990, referred to as Internet service provider (ISP) 1.0 (**figure 2.2**).

At the ISP 2.0 stage, one-to-one user messaging evolved into one-to-many information distributions via web sites. Graphical information (content pages stored on Internet-connected computers) provided Internet users with online access to all types of information from web site owners. This was initially fixed or static information, but quickly evolved into dynamic or real-time information in the areas of weather, traffic or news. Dynamic web site information also provided current marketing information, inventories, product pricing and delivery information for both consumers and businesses. The computer servers hosting these web sites were

located either on the premises of the supporting organization having sufficient bandwidth access to the Internet or were colocated at ISPs that, by their very business charter, had sufficient Internet bandwidth to allow adequate web site/browser interaction.

ISP 3.0 is the stage in the cloud computing evolution that offers outsourced computer server locations (colocation). This occurred in the late 1990s when colocation provided customers third-party best-practice expertise managing computer operations. Client users navigated from their desktops through the Internet to access their internal applications hosted externally. Colocation also provided clients who had developed e-commerce web sites with enough bandwidth access to offer online shopping services without long, irritating waits for web page downloads. In both ISP 2.0 and 3.0, colocation service providers offered their hosted clients shared Internet bandwidth, i.e., resource pooling.

ISP 4.0 arrived at the turn of the 21<sup>st</sup> century. At this time, application service providers (ASPs) offered to enterprises were the direct predecessor of cloud computing's current SaaS service model. ASPs offered clients traditional software applications operated for a single client, most often on a single server.

By using an ASP, an enterprise no longer had to pay software acquisition costs in addition to the typical annual fees, which could reach 18 to 20 percent for technical support, software maintenance and upgrades. ASP clients merely rented use of the application and server capacity from the ASP and connected via the web.

ASPs were also responsible for maintaining high levels of uptime availability, often quoted as “three nines” (99.9 percent), “four nines” (99.99 percent), etc. Good-quality ASPs would maintain at least dual access points to the Internet through different network service providers (NSPs) via two physically separate cables, ensuring connectivity in the event that an NSP went down. Many ASPs maintained updated application versions and what is now referred to as “patch management”—application upgrades and security or bug fixes.

ASPs marketed themselves as providing clients with better application availability and performance at costs that were far below those incurred by purchasing and supporting a business application internally. ASPs were another portion of the evolution to today's cloud computing resource pooling.

ISP 5.0 is the next evolution of cloud computing and represents the current state of activity.

Many ASPs have evolved to SaaS as web-based SOA applications for use by multiple tenants running on the same application at the same time on the same server or servers. Through the use of Extensible Markup Language (XML) tags, SaaS providers state that a client's data can be segregated from other clients' data, even though all customer data share the same memory space.

SaaS providers are expected to provide the requisite security tools and maintain application and OS patches as needed. Also, because SaaS providers use the maximum server utilization cloud computing model, there are cost savings from reduced server usage, power and cooling that can be passed on to customers.

## The Technical Building Blocks

Cloud computing combines several technical innovations from the last 10 to 15 years that constitute its fundamental technical building blocks, including:

- **SOA**—A library of proven, functional software applets that can be connected to become a useful application
- **Application programming interfaces (APIs)**—Tags to direct applets about the Internet
- **XML**—Identifier tags attached to information (data, pages, pictures, files, fields, etc.) that allow them to be transported to any designated application located on the Internet

Simplistically, one could look at SOA in the same way as designing a necklace. The beads are the SOA applets, while the string is the Internet bringing the applets together. Most often, this is a complex, matrix-type necklace that is interwoven with various possible applet selections, depending on specific output values from the previous applet. API and XML are used to connect web-based SOA applications. While the ensuing SOA application may require more lines of code than an equivalent application that is perfectly designed from scratch, the ease of design and the development time savings that result from creating a “bead-based” SOA application far outweigh the added line costs.

There are many components and terms used in cloud computing that are helpful in understanding the internal working of cloud technologies. Some of these terms include:

- **Hypervisor**—A computer tool allowing various software applications running on different OSs to coexist on the same server at the same time. This means that Windows, Java, Linux, C++, Simple Object Access Protocol (SOAP) and Pearl-based applications can operate concurrently on the same machine. The hypervisor is the enabling technology for server virtualization.
- **Virtualization**—The process of adding a “guest application” and data onto a “virtual server,” recognizing that the guest application will ultimately part company from this physical server
- **Dynamic partitioning**—The variable allocation of CPU processing and memory to multiple applications and data on a server. Also known as logical partitioning (LPAR), dynamic partitioning provides variable CPU and server memory capacity to the various concurrently operating applications as needed. This is important because of the variable processing requirements experienced with batch jobs and real-time processing. Multiple concurrent applications may require near-equal portions of CPU cycles and memory, but in some instances, one of the applications may need a much larger appropriation of processing power and

memory space to avoid throughput delays. Dynamic partitioning reallocates the CPU and memory capacity as needed.

- **OS, application and data migration**—The process of migrating data, the application and the underlying OS onto another server. Dynamic partitioning reallocates server processing and memory capacity as needed, automatically, on the fly. However, when the hypervisor senses that there is too much demand from the various applications for the host server's horsepower, tools exist to migrate data, the application and the underlying OS onto another server identified as available.
- **Cloud client usage measurement**—The ability to measure usage of CPU processing, input/output and memory utilization per customer, per application. This measured services tool allows the CSPs that operate the servers for the cloud to charge clients usage fees based on the actual processing consumed.

## Essential Cloud Computing Characteristics

Several notable characteristics differentiate cloud computing from traditional IT operations. Cloud computing services are available on demand and via self-service. Cloud computing offers new-to-client computer services in near-real time, with little to no human interaction required between clients and service representatives.

Cloud computing is accessible. It operates using a broad network access that allows any device with Internet access—desktops, notebooks, netbooks, smart phones, personal digital assistants (PDAs), etc.—access to cloud computing applications.

Cloud computing cost savings are realized via resource pooling. Rather than having required, reserve and backup computer processing systems in house, with the requisite capital outlays and ongoing OPEX, cloud computing resources (processing power, broadband Internet connectivity and systems administration) are pooled and then shared by multiple enterprises. Users are able to avoid the initial capital investments from building out a technology infrastructure, paying only the service charges for the computing capacity actually used.

A broadly promoted benefit of cloud computing is rapid elasticity. Clients are able to expand or contract data processing or storage power in real time, as needed. For enterprises offering on-demand customer services, this is a huge business advantage. Without the requirement of an up-front capital investment, costs for cloud computing services are directly proportional to the realized services provided.

Application sharing and multitenancy of data also are characteristics associated with cloud computing. Multitenancy occurs when multiple customers share an application. Customer data are separated through logical partitions so that customers have access to only their own data. Although security and privacy are often concerns among customers, many CSPs have multitenant applications that are secure, scalable and customizable.

Cloud computing can also track actual computer utilization by user. This measured service characteristic is a critical capability that enables CSPs to charge their clients based on the services consumed. A cloud computing user is charged by a CSP for the use of processing power and data storage in any amount, as needed—even to the degree of charging the enterprise’s internal cost centers for their use of different cloud applications. Thus, computer processing can be considered a utility, similar to electricity, phone, gas and water.

Cloud computing essential characteristics are summarized in **figure 2.3**.

<b>Figure 2.3—Cloud Computing Essential Characteristics</b>	
<b>Characteristic</b>	<b>Description</b>
On-demand self-service	The CSP can automatically provision computing capabilities such as server and network storage as needed, without requiring human interaction with each service’s provider.
Broad network access	The cloud network should be accessible anywhere, by almost any device (e.g., smart phone, laptop, mobile device, PDA).
Resource pooling	The CSP’s computing resources are pooled to serve multiple customers using a multitenant model, with different physical and virtual resources dynamically assigned and reassigned according to demand. There is a sense of location independence: The client generally has no control over or knowledge of the exact location of the provided resources, but may be able to specify location at a higher level of abstraction (e.g., country, region or data center). Examples of resources include storage, processing, memory, network bandwidth and virtual machines.
Rapid elasticity	Capabilities can be rapidly and elastically provisioned—in many cases, automatically—to accommodate customer needs. To the customer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
Measured service	Cloud computing systems automatically control and optimize resource usage by leveraging a metering capability (e.g., storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for both the provider and customer of the utilized service.
Multitenancy of data	Multitenancy is the sharing of an application by multiple customers.
Source: ISACA, <i>Cloud Computing Business Benefits With Security Governance and Assurance Perspectives</i> , USA, 2009, <a href="http://www.isaca.org/cloud">www.isaca.org/cloud</a>	

## Cloud Drivers

Cloud computing is viewed as a significant change in the platform in which business services will be translated, used and managed. Many consider it to be as large a shift in IT as was the advent of the personal computer (PC) or of Internet access. However, a major difference between the cloud and those technologies is that the introductions of those earlier technologies encompassed a slower development phase. With the cloud, the required pieces for use have come together

more rapidly for implementation. Some of the drivers bringing the cloud to the attention of enterprise decision makers are:

- **Optimized server utilization**—Enterprises typically utilize just 15 to 20 percent of server computing resources.<sup>2</sup> This means that they have five times the computing capacity than is typically used. By using many of the cloud-enabling tools described in this chapter, server utilization rates can increase four- to fivefold.
- **Cost savings**—Increased server utilization plus the transition of computational capability from acquired and maintained computers to rented cloud services change the computing cost paradigm from a CAPEX to an OPEX, with potentially significant up-front and total cost savings.
- **Dynamic scalability**—Many enterprises install five times their average computing requirements just to ensure that capacity exists to meet the large batch or peak demand. The cloud provides an extra processing buffer as needed, at low cost and without capital investment or a contingency fee to users.
- **Shortened development life cycle**—Using cloud computing’s SOA development approach, new business applications can be developed online, connecting proven functional application building blocks together. SOA-developed applications have measured completion times of one-fifth the time required for traditionally developed applications.
- **Reduced time for implementation**—Cloud computing provides processing power and data storage as needed and at the capacity needed. This can be obtained in near-real time, not requiring the weeks or months (or CAPEX) that accrue when a new business initiative is brought online in a traditional IT enterprise.

Depending on business needs, any or all of these benefits could be a sufficient reason to consider a cloud computing solution. The recent world economy has pushed many enterprises to be more fiscally conservative. In the IT space, cloud computing presents a potentially significant savings by enabling enterprises to maximize dynamic computing on a pay-per-use basis. By using the governance processes described in chapter 3, this advantage can be leveraged across entire enterprises.

## Cloud Computing Challenges

For all the benefits of cloud computing, it also incorporates unique and notable technical or business risk. Some of the business challenges related to cloud computing include:

- **Data location**—Regardless of the deployment model selected, customers may not know the physical location of the server used to store and process their data and applications. Cloud computing technology allows cloud servers to reside anywhere. From a technology standpoint, location becomes mostly irrelevant. However, for many compliance and data governance requirements, the physical location of the cloud computing server hosting user data is a critical issue. While

---

<sup>2</sup> Kanellos, Michael; “Is Cyber Monday Really Energy Efficient?,” Greentech Enterprise, 24 November 2010, [www.greentechmedia.com/articles/read/is-cyber-monday-really-energy-efficient](http://www.greentechmedia.com/articles/read/is-cyber-monday-really-energy-efficient)

the data may reside anywhere, it is important to understand that many CSPs can also specifically define where data are to be located—down to the server, data center and country levels.

- **Commingled data**—Many clients will use the same application on the same server concurrently, which may result in the clients' data being stored in the same data files. SaaS providers claim that each data field has an appropriate metatag affixed to keep clients' commingled data separate. Encryption is another control that can assist in data confidentiality; however, users need to ascertain the specifics of encryption key management and the process used to unencrypt data prior to being processed. Ultimately, to be sure that data are not commingled or exposed, some auditability must be built into the contract between the customer and the provider.
- **Cloud security policy/procedure transparency**—Some CSPs may have less transparency than others when it comes to their current information security policies. The rationalization for this is that the policies may be proprietary. This practice may cause conflict with clients' information compliance requirements. Clients need to have an understanding of and detailed contracts with service level agreements (SLAs) that provide the desired level of security to ensure that CSPs are applying appropriate controls.
- **Cloud data ownership**—Contract agreements may state that the CSP owns the data placed in the cloud computing environment that it maintains. The CSP may also require significant service fees for data to be returned to clients if and when a cloud computing services agreement terminates.
- **Lock-in with CSP's proprietary APIs**—As in the 1970s, with proprietary software vendor applications, many CSPs currently implement their applications using proprietary APIs. This makes transitioning between CSPs extremely difficult, time-consuming and labor-intensive. Uploading data into a cloud SaaS is easier and less costly than transferring data from one CSP with proprietary APIs to another replacement CSP.
- **CSP business viability**—As cloud computing continues to mature, there will be CSPs going out of business. Clients need to consider the risk and how data and applications can be easily transferred back to the traditional enterprise or to another CSP.
- **Record protection for forensic audits**—Clients must also consider the availability of data and records if required for forensic audits. Since data may have been commingled and migrated among multiple servers located widely apart, it may be possible that the data for a specific point in time cannot be identified. Furthermore, local authorities may impound a cloud computing server to assess court-warranted data records of a suspect client—taking with it the data of all the cloud computing clients sharing this impounded server.
- **Identity and access management (IAM)**—Current CSPs may not develop and implement adequate user access privilege controls. With ever more sophisticated applications going online—available for access by enterprise users, partners and clients—highly granular, least privilege-based user access tools are required.

- **Penetration detection**—Consideration should be given to whether the CSP has a penetration detection system in use. If such a system is in use, it is important to ensure that it has the required sophistication to monitor all cloud computing activities adequately. It is also important to consider whether a real-time digital dashboard is provided to user managers, along with audit logs and records of security incidents.
- **Screening of other cloud computing clients**—By definition, CSPs leverage their cloud computing technology for many clients concurrently to maximize revenues. Clients should consider whether the other clients who share the same servers—and, in the case of SaaS, the same application and data files—are of the same repute as their own enterprise.
- **Compliance requirements**—For the many compliance requirements—including privacy and PII laws, Payment Card Industry (PCI) requirements, or various financial reporting laws—today’s cloud computing services can challenge various compliance audit requirements currently in place. Data location, cloud computing security policy transparency and IAM are all challenging issues in compliance auditing efforts.
- **Public cloud server owners’ due diligence**—Trust is a major component in the cloud computing business model. When contemplating transferring critical organizational data to the cloud computing platform, it is important to understand who and where all of the companies are that may touch the enterprise data. This includes not only the CSP, but all vendors that are in the critical path of the CSP. Background checks on these companies are important to ensure that data are not being hosted by an organization that is incapable of responding to outages or providing business continuity or that is engaging in malicious or fraudulent activity.
- **Data erasure for current SaaS or PaaS applications**—When an application and data are transferred from one server to another, as would be expected with dynamic scalability, the earlier application and data files may remain and may not be erased. Their space on the original hard drives is now available for overwrites. The original data files may still be available for copying up to the third rewrite of the original disk space. This remaining copy of data may be useful in the case of an emergency; however, it presents customers with the dilemma of ensuring that confidential data are permanently destroyed in the event of a contract termination. Customers need to ensure that this confidentiality is implemented by including language in the contract that provides for immediate data erasure upon contract termination.
- **Disaster recovery**—Disaster recovery is a concern for potential cloud customers. In traditional hosting or colocation sites, customers know exactly where their data are in the event that they need to quickly retrieve them. The cloud model can change in the sense that public CSPs may outsource capabilities to third parties who may also outsource—the original CSP may not be the CSP ultimately holding the data. Contracts should detail any testing or recovery time requirements.

At present, it is the cloud computing client’s responsibility to assess the cloud computing risk and controls, especially when using a public cloud computing delivery model. It is the client’s responsibility to ensure that the enterprise’s sensitive data will remain authentic, accurate and available and that the data falling under any applicable regulations will meet the specific compliance requirements.

With a now-established cooperative nature among nonprofit cloud computing security organizations, many CSPs, the Black Hat community and governments worldwide, evolving cloud risk should be readily identified, details disseminated, and corrective responses developed and quickly implemented with the hope of a proactive, rather than a reactive, approach.

Pages 25 through 188 deleted from this sample.

Please visit [www.isaca.org/ITCOCloud](http://www.isaca.org/ITCOCloud) for links to purchase the book.

# ISACA PROFESSIONAL GUIDANCE PUBLICATIONS

Many ISACA publications contain detailed assessment questionnaires and work programs that provide valuable guidance. Please visit [www.isaca.org/bookstore](http://www.isaca.org/bookstore) or e-mail [bookstore@isaca.org](mailto:bookstore@isaca.org) for more information.

## Frameworks and Model

- *The Business Model for Information Security*, 2010
- COBIT® 4.1, 2007
- *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0*, 2008
- *ITAF™: A Professional Practices Framework for IT Assurance*, 2008
- *The Risk IT Framework*, 2009

## BMIS-related Publication

- *An Introduction to the Business Model for Information Security*, 2009

## COBIT-related Publications

- *Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit*, 2008
- *Building the Business Case for COBIT® and Val IT™: Executive Briefing*, 2009
- *COBIT® and Application Controls*, 2009
- *COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2<sup>nd</sup> Edition*, 2007
- *COBIT® Mapping: Mapping of CMMI® for Development V1.2 With COBIT® 4.1*, 2011
- *COBIT® Mapping: Mapping of FFIEC With COBIT® 4.1*, 2010
- *COBIT® Mapping: Mapping of ISO/IEC 17799:2000 With COBIT®, 2<sup>nd</sup> Edition*, 2006
- *COBIT® Mapping: Mapping of ISO/IEC 17799:2005 With COBIT® 4.0*, 2006
- *COBIT® Mapping: Mapping of ISO/IEC 20000 With COBIT® 4.1*, 2011
- *COBIT® Mapping: Mapping of ITIL® V3 With COBIT® 4.1*, 2008
- *COBIT® Mapping: Mapping of NIST SP 800-53 With COBIT® 4.1*, 2007
- *COBIT® Mapping: Mapping of PMBOK® With COBIT® 4.0*, 2006
- *COBIT® Mapping: Mapping of SEI's CMM® for Software With COBIT® 4.0*, 2006
- *COBIT® Mapping: Mapping of TOGAF 8.1 With COBIT® 4.0*, 2007
- *COBIT® Quickstart™, 2<sup>nd</sup> Edition*, 2007
- *COBIT® Security Baseline™, 2<sup>nd</sup> Edition*, 2007
- *COBIT® User Guide for Service Managers*, 2009
- *Implementing and Continually Improving IT Governance*, 2009
- *IT Assurance Guide: Using COBIT®, 2007*
- *IT Control Objectives for Basel II*, 2007
- *IT Control Objectives for Cloud Computing*, 2011
- *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2<sup>nd</sup> Edition*, 2006
- *ITGI Enables ISO/IEC 38500:2008 Adoption*, 2009
- *SharePoint® Deployment and Governance Using COBIT® 4.1: A Practical Approach*, 2010

## Risk IT-related Publication

- *The Risk IT Practitioner Guide*, 2009

## Val IT-related Publications

- *The Business Case Guide: Using Val IT™ 2.0*, 2010
- *Enterprise Value: Getting Started With Value Management*, 2008
- *Value Management Guidance for Assurance Professionals: Using Val IT™ 2.0*, 2010

## Academic Guidance

- IT Governance Using COBIT® and Val IT™:
  - *Student Book, 2nd Edition*, 2007
  - *Caselets, 2nd Edition*, and *Teaching Notes*, 2007
  - *TIBO Case Study, 2nd Edition*, and *Teaching Notes*, 2007 (Spanish translation also available)
  - *Presentation, 2nd Edition*, 2007 (35-slide PowerPoint deck on COBIT)
  - *Caselets, 3rd Edition*, and *Teaching Notes*, 2010
  - *City Medical Center Case Study, 3rd Edition*, and *Teaching Notes*, 2010
- Information Security Using the CISM® Review Manual and BMIS™:
  - *Caselets*, 2010
  - *More4Less Foods Case Study*, 2010
  - *Caselets and More4Less Foods Case Study—Teaching Notes*, 2010

## Executive and Management Guidance

- *Board Briefing on IT Governance, 2nd Edition*, 2003
- *Defining Information Security Management Position Requirements: Guidance for Executives and Managers*, 2008
- *An Executive View of IT Governance*, 2008
- *Global Status Report on GEIT 2011*, 2011
- *Identifying and Aligning Business Goals and IT Goals: Full Research Report*, 2008
- *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*, 2006
- *Information Security Governance: Guidance for Information Security Managers*, 2008
- *Information Security Governance—Top Actions for Security Managers*, 2005
- IT Governance Domain Practices and Competencies:
  - *Governance of Outsourcing*, 2005
  - *Information Risks: Whose Business Are They?*, 2005
  - *IT Alignment: Who Is in Charge?*, 2005
  - *Measuring and Demonstrating the Value of IT*, 2005
  - *Optimising Value Creation From IT Investments*, 2005
- *IT Governance and Process Maturity*, 2008

## Executive and Management Guidance (cont.)

- IT Governance Roundtables:
  - *Defining IT Governance*, 2008
  - *IT Staffing Challenges*, 2008
  - *Unlocking Value*, 2009
  - *Value Delivery*, 2008
- *ITGI Enables ISO/IEC 38500:2008 Adoption*, 2009
- *Managing Information Integrity: Security, Control and Audit Issues*, 2004
- *Understanding How Business Goals Drive IT Goals*, 2008
- *Unlocking Value: An Executive Primer on the Critical Role of IT Governance*, 2008

## Practitioner Guidance

- Audit/Assurance Programs:
  - *Apache™ Web Services Server Audit/Assurance Program*, 2010
  - *Change Management Audit/Assurance Program*, 2009
  - *Cloud Computing Management Audit/Assurance Program*, 2010
  - *Crisis Management Audit/Assurance Program*, 2010
  - *Generic Application Audit/Assurance Program*, 2009
  - *Identity Management Audit/Assurance Program*, 2009
  - *Information Security Management Audit/Assurance Program*, 2010
  - *IT Continuity Planning Audit/Assurance Program*, 2009
  - *Microsoft® Internet Information Services (IIS) 7 Web Services Server Audit/Assurance Program*, 2011
  - *Mobile Computing Security Audit/Assurance Program*, 2010
  - *MySQL™ Server Audit/Assurance Program*, 2010
  - *Network Perimeter Security Audit/Assurance Program*, 2009
  - *Outsourced IT Environments Audit/Assurance Program*, 2009
  - *Security Incident Management Audit/Assurance Program*, 2009
  - *Social Media Audit/Assurance Program*, 2011
  - *Systems Development and Project Management Audit/Assurance Program*, 2009
  - *UNIX/LINUX Operating System Security Audit/Assurance Program*, 2009
  - *VMware® Server Virtualization Audit/Assurance Program*, 2011
  - *Windows Active Directory Audit/Assurance Program*, 2010
  - *z/OS Security Audit/Assurance Program*, 2009
- *Creating a Culture of Security*, 2011
- *Cybercrime: Incident Response and Digital Forensics*, 2005
- *Enterprise Identity Management: Managing Secure and Controllable Access in the Extended Enterprise Environment*, 2004
- *Information Security Career Progression Survey Results*, 2008
- *Information Security Harmonisation—Classification of Global Guidance*, 2005
- *Monitoring Internal Control Systems and IT*, 2010
- *OS/390—z/OS: Security, Control and Audit Features*, 2003
- *Peer-to-peer Networking Security and Control*, 2003

## Practitioner Guidance (cont.)

- *Risks of Customer Relationship Management: A Security, Control and Audit Approach*, 2003
- *Security Awareness: Best Practices to Serve Your Enterprise*, 2005
- *Security Critical Issues*, 2005
- *Security Provisioning: Managing Access in Extended Enterprises*, 2002
- *Stepping Through the InfoSec Program*, 2007
- *Stepping Through the IS Audit, 2<sup>nd</sup> Edition*, 2004
- Technical and Risk Management Reference Series:
  - *Security, Audit and Control Features Oracle® Database, 3<sup>rd</sup> Edition*, 2009
  - *Security, Audit and Control Features Oracle® E-Business Suite, 3<sup>rd</sup> Edition*, 2010
  - *Security, Audit and Control Features PeopleSoft, 2<sup>nd</sup> Edition*, 2006
  - *Security, Audit and Control Features SAP® ERP, 3<sup>rd</sup> Edition*, 2009
- *Top Business/Technology Survey Results*, 2008
- White Papers:
  - *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*, 2009
  - *Data Leak Prevention*, 2010
  - *E-commerce and Consumer Retailing: Risks and Benefits*, 2010
  - *Electronic Discovery*, 2011
  - *Leveraging XBRL for Value in Organizations*, 2011
  - *New Service Auditor Standard: A User Entity Perspective*, 2010
  - *Securing Mobile Devices*, 2010
  - *Security Information and Event Management: Business Benefits and Security, Governance and Assurance Perspectives*, 2010
  - *Social Media: Business Benefits and Security, Governance and Assurance Perspectives*, 2010
  - *Sustainability*, 2011
  - *Virtualization: Benefits and Challenges*, 2010



*Trust in, and value from, information systems*

3701 Algonquin Road, Suite 1010  
Rolling Meadows, IL 60008 USA  
Phone: +1.847.253.1545  
Fax: +1.847.253.1443  
E-mail: [info@isaca.org](mailto:info@isaca.org)  
Web site: [www.isaca.org](http://www.isaca.org)

ISBN 978-1-60420-185-7  
9 0000 >

