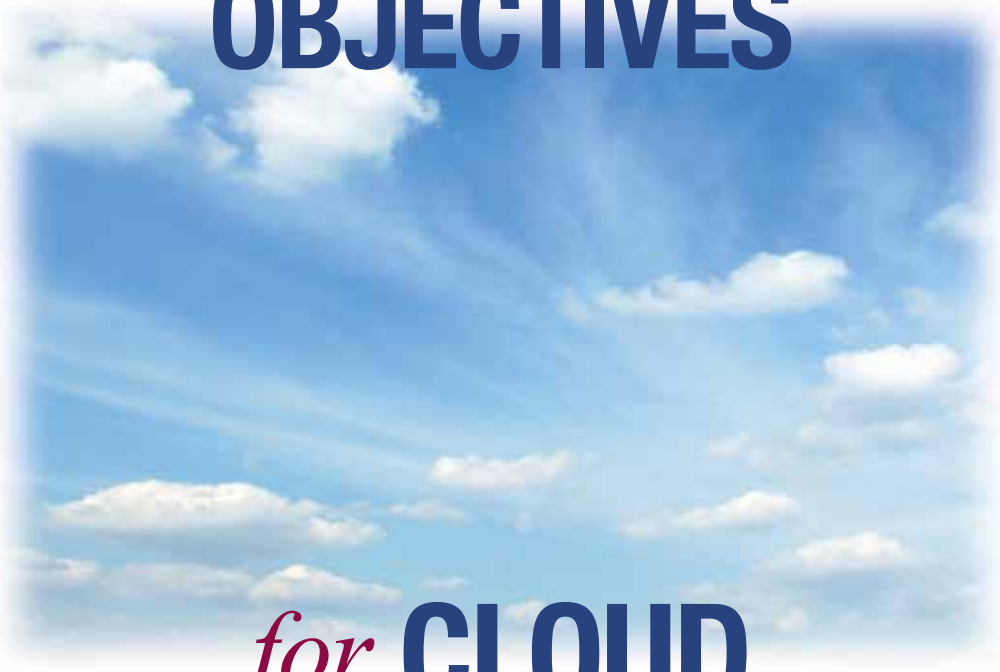
IT CONTROL OBJECTIVES



for CLOUD COMPUTING:

CONTROLS AND ASSURANCE IN THE CLOUD

ISACA®

Trust in, and value from, information systems

ISACA®
With 95,000 constituents in 160 countries, ISACA (*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

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*
Web site: *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

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, KMPG 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

Table of Contents *(cont.)*

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:[1]

> *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.

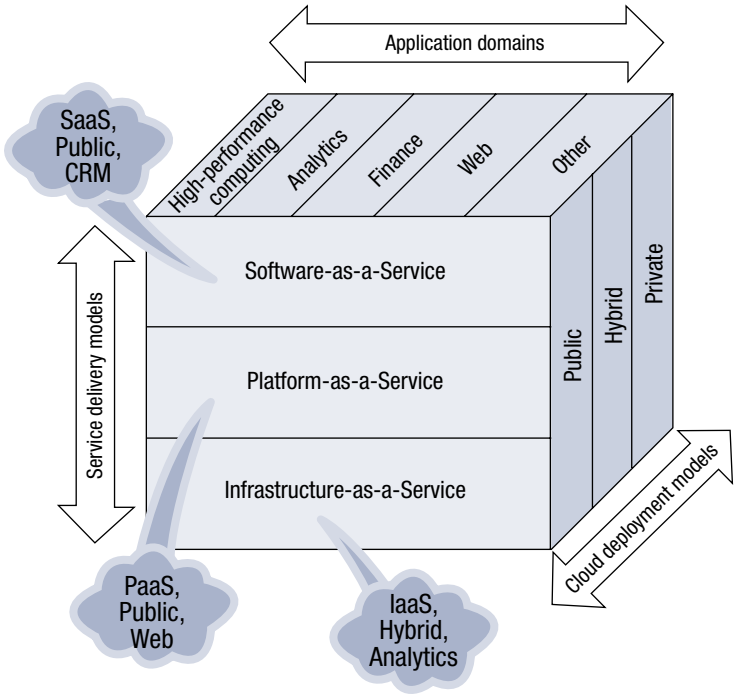
[1] Mell, Peter; Timothy Grance; US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145 (Draft), The NIST Definition of Cloud Computing, NIST, USA, 2011

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**).

Figure 1.1—Cloud Security Alliance Cloud Computing Service Delivery and Deployment Model



Source: Cloud Computing Service Delivery and Deployment Model, © Cloud Security Alliance, *https://cloudsecurityalliance.org*. Used with permission.

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: • Amazon Web Services™ • Mosso from Rackspace®
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: • Microsoft's Azure™ Services Platform • Google's Google App Engine • Salesforce.com's Force.com®

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).	Applications are complete and available on demand to the customer. Traditional licensing and asset management are changed. Example CSPs: • Microsoft Online Services • Salesforce customer relationship management (CRM) • LotusLive™ from IBM®
Source: Pijanowski, Keith; "Understanding Public Clouds: IaaS, PaaS and SaaS," Keith Pijanowski's Blog, 31 May 2009, *www.keithpij.com/Home/tabid/36/EntryID/27/Default.aspx*		

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	• Operated solely for an enterprise • May be managed by the enterprise or a third party • May exist on- or off-premise
Public cloud	• Made available to the general public or a large industry group • Owned by an organization selling cloud services
Community cloud	• Shared by several enterprises • Supports a specific community that has a shared mission or interest • May be managed by the enterprises or a third party • May reside on- or off-premise
Hybrid cloud	• 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)

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.)

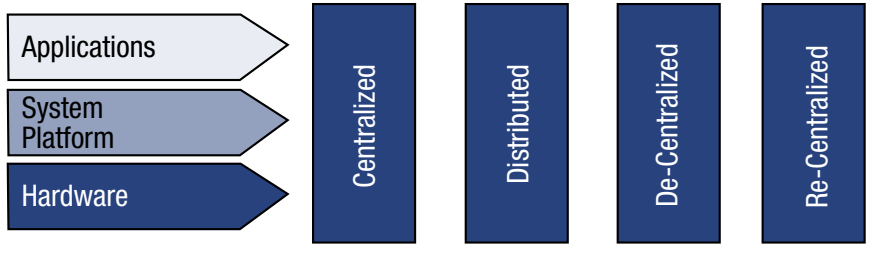
Evolution of the Cloud

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 midsized 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.

Figure 2.1—The Return to Central Processing

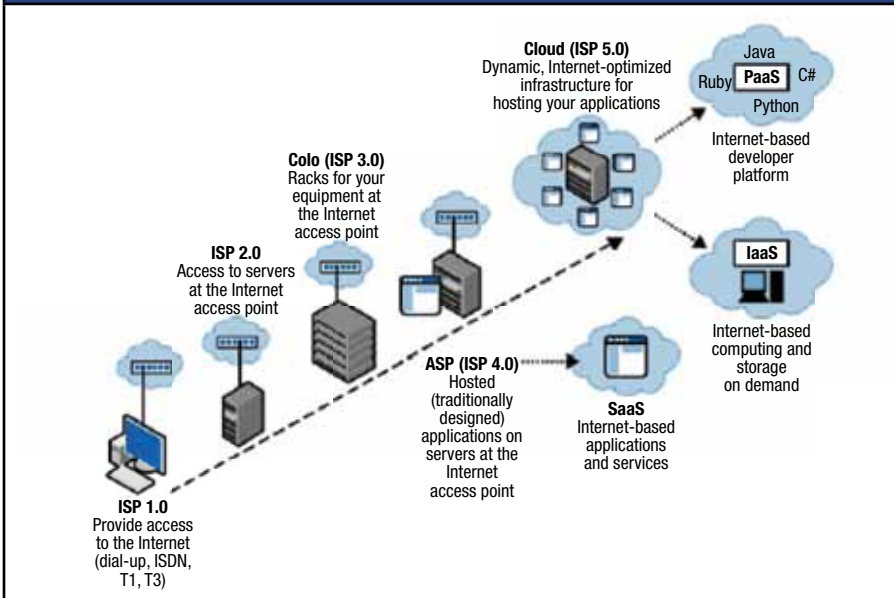


Source: © Novell, Cloud Presentation 9.09. Used with permission.

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.

Figure 2.2—The Evolution of Cloud Computing From an Online Perspective



Source: Mather, Tim; Subra Kumaraswamy; Shahed Latif; *Cloud Security and Privacy*, O'Reilly Media, Inc., USA, 2009. Used with permission.

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 21st 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**.

Figure 2.3—Cloud Computing Essential Characteristics

Characteristic	Description
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, *Cloud Computing Business Benefits With Security Governance and Assurance Perspectives*, USA, 2009, *www.isaca.org/cloud*

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.[2] 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

[2] Kanellos, Michael; "Is Cyber Monday Really Energy Efficient?," Greentech Enterprise, 24 November 2010, *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.

3. Governance in the Cloud

Cloud computing is a combination of technologies through which dynamically scalable and often virtualized resources are provided as a service over the Internet. Users need not have knowledge of, expertise in or control over the infrastructure in the cloud.

The role of the chief information officer (CIO) is transitioning from simply managing operations to managing IT as service value chain. If, previously, the CIO ran the internal "IT factory," now, both enterprises and external service providers have become producers and consumers of services. With cloud computing, the CIO must weave together and optimize this value chain to best support various customers and enable a company's business. The cloud is accelerating and mandating the transition and, therefore, governance is mandatory.[3]

Business and Governance of Enterprise IT (GEIT)

When enterprises decide to utilize cloud services for some or all IT services, business processes are impacted, which makes governance more critical than ever. The following are just a few reasons why enterprises should implement and maintain a sound GEIT program:[4]

- To effectively manage increasing risk, including security, compliance, projects and partners
- To ensure continuity of critical business processes that now extend beyond the data center
- To communicate clear enterprise objectives internally and to third parties
- To adapt easily. Flexibility, scalability and services are changed in the cloud, enabling the enterprise and business practices to adjust to create new opportunities and reduce cost.
- To facilitate continuity of IT knowledge, which is essential to sustain and grow the business
- To handle a myriad of regulations

For enterprises to gain benefit from the use of cloud computing, a clear governance strategy and management plan must be developed. The strategy should set the direction and objectives for cloud computing within the enterprise, and the management plan should execute the achievement of the objectives.

Business consultancies have long recognized that the various functional departments of highly successful enterprises tend to interact nearly seamlessly. Key to this successful departmental integration is recognizing and leveraging

[3] Stroud, Robert; "Providing Governance in a Rapidly Changing World," ISACA Euro Computer Audit, Control and Security (EuroCACS) conference 2010, Budapest, Hungary
[4] *Ibid*.

the interrelationships and interdependencies among departments. This originates from the tone at the top and is manifested and reinforced via cross-departmental corporate governance programs.

IT, with its particular requirements and terminology, has historically been viewed as a cost center rather than a corporate asset. However, the cloud presents the opportunity to fully align IT with the goals and objectives of the enterprise as a whole. To "sit at the table" of the enterprise's governance programs, IT must adapt to methodologies and the language used in other areas of the enterprise's governance.

ISACA defines governance as the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved and ascertaining that risks are managed appropriately.[5] Although ISACA defines five outcomes of good governance that can contribute to overall enterprise success, GEIT is primarily concerned with two: IT value delivery to the business and the management of IT-related risks. These are enabled by the other three outcomes:
- Strategic alignment of IT to the business
- The availability and management of adequate resources
- The measurement of performance to monitor progress toward the desired goals

Cloud IT Benefits/Value Enablement Risk

IT benefits and value enablement are key considerations of a cloud program. The cloud can provide enterprises with many business benefits by enabling new business initiatives or more efficient operations.

New cloud initiatives may include:
- A broad-based consumer-oriented online marketing campaign that requires highly elastic processing power and provides video feeds to consumers on demand
- A one-time information processing exercise to catalog current stored data for easy query selections
- An informational web site that provides area residents with up-to-date emergency guidance in the event of a local emergency, disaster or impending weather event

More efficient operations involving the cloud may include:
- A transfer from an internal to a cloud-based CRM program that allows the enterprise's sales force to utilize and collaborate on a best-of-breed application for less cost than the current in-house application
- An upgrade to an industry-recognized best-practice online enterprise resource planning (ERP) application to coordinate product scheduling plans with suppliers and resellers

[5] IT Governance Institute (ITGI), *Board Briefing on IT Governance, 2nd Edition*, USA, 2003

- A consumer-facing e-commerce web page with near-infinite scalability for market volume recognized to be widely variable over the course of a day
- A marketing/promotional blog prepared for variable scalability, but also including smart profiling of registered client bloggers that e-mails them when a message in their interest space has been posted

ISACA's GEIT and Management Frameworks and Models

ISACA has developed several GEIT tools to assist IT executives and managers with integrating and aligning IT operations into the primary business focus of the enterprise:

- **COBIT**—The comprehensive GEIT framework that addresses every aspect of IT and integrates all of the main global IT standards
- **Val IT**—The GEIT framework that focuses on value delivery and ensures that IT-enabled investments are managed through their full economic life cycle
- **Risk IT**—A set of guiding principles and the first framework to help enterprises identify, govern and effectively manage IT risk
- **BMIS**—A holistic model for managing information security that takes a business-oriented approach

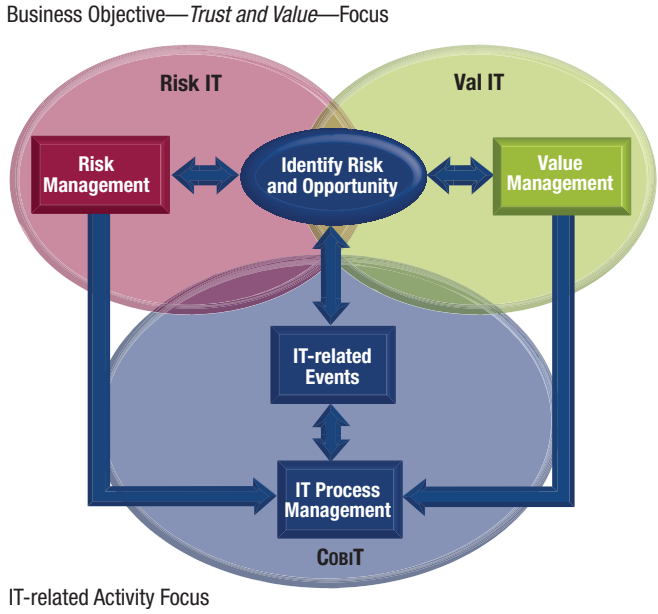
While these tools have not been designed specifically for cloud environments, the principles are applicable. In fact, cloud computing may amplify the importance these tools have in an enterprise as the impact that the cloud has on the business may change business processes. In traditional IT environments, everyone in the business has to go to the IT department to obtain IT-related services; with the capabilities that the cloud provides enterprises, employees can go directly to a CSP to acquire services. This elevates the enterprise's level of risk. Having tools such as those mentioned from ISACA will help the enterprise to implement repeatable processes and appropriate control levels.

Appendix A provides the IT control objectives from COBIT 4.1 and maps the control objectives that are appropriate for enterprises to consider when choosing to utilize cloud computing services.

Leveraging and Integrating IT Governance Frameworks, Standards and Good Practices

It is clear that there are strong links among COBIT, Val IT and Risk IT. Val IT and Risk IT complement and extend the COBIT guidance in the two governance focus areas of value delivery and risk management (**figure 3.1**). If these areas are the focus of the enterprise's GEIT implementation efforts, then Val IT and Risk IT can help identify more specifically *what* should be addressed to enable better governance of value management and risk management.

Figure 3.1—Business Objective, Trust and Value, and Focus



Source: ISACA, *The Risk IT Framework*, USA, 2009, figure 1, *www.isaca.org/riskit*

Since Val IT and Risk IT extend and complement the IT processes in COBIT with processes that manage value and risk, including better business involvement, all three frameworks can be used together to help create a set of end-to-end IT-related processes. This will help to integrate all business and IT activities for effective GEIT.

Together, COBIT, Val IT and Risk IT provide an effective way to understand business and governance priorities and requirements; this knowledge can then be used when implementing cloud services. This approach also enhances the preparation of business cases for governance improvements, obtaining the support of stakeholders, and realizing and monitoring the expected benefits.[6]

The relationship can be summarized in this top-down flow. COBIT, Val IT and Risk IT help drive what to do, supported by a cascade of the business goals to IT goals to IT processes:

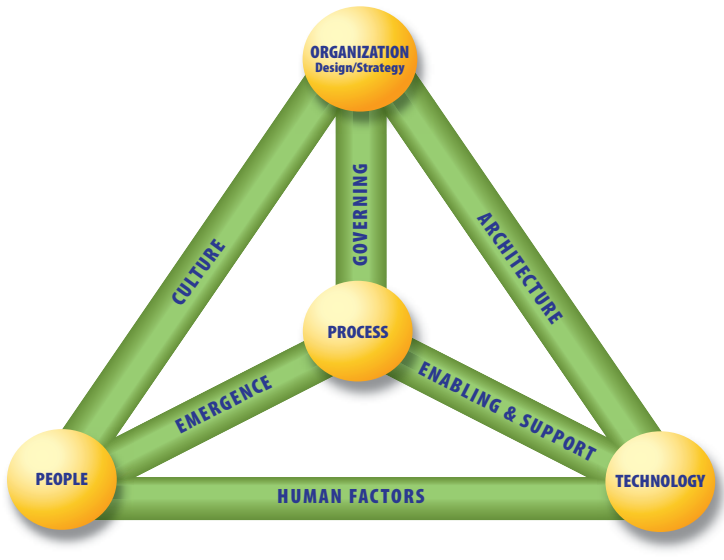
- Business goals
  - IT goals
    - Governance requirements
      - Critical IT processes
        - Prioritized control objectives and practices

[6] ISACA, *Implementing and Continually Improving IT Governance*, USA, 2009, *www.isaca.org*

The links between COBIT and Val IT are focused on program and portfolio management; investment management; and, primarily, the COBIT IT processes that deal with strategy and portfolios. The links between COBIT and Risk IT are focused on risks related to strategic choices, roles and responsibilities for risk-related functions, risk-related policies and frameworks, risk management, business continuity, and various other specific risk-related service delivery activities.

BMIS (**figure 3.2**) describes, in business terms, how taking a holistic view of security more effectively addresses business risk, value, resource utilization and program effectiveness. Understanding how BMIS works may help enterprises realize how moving to cloud services will affect the enterprise in a holistic manner.

Figure 3.2—BMIS



Source: ISACA, *The Business Model for Information Security*, USA, 2010, figure 2, *www.isaca.org/bmis*

There are many stakeholders interested in GEIT who need to collaborate to achieve the overall business goal of improved IT performance. When moving to a cloud environment, this group of stakeholders may expand because it may affect processes within other business units and IT. If the enterprise does not already have a robust GEIT program in place, the move toward a cloud solution provides a good opportunity to develop one. If there is a mature program in place, it will certainly need to be reviewed; assessed; and, most likely, adjusted to account for changes in business processes, security and risk. When creating or adjusting a GEIT program, key success factors for implementation are:

- Top management should provide the direction and mandate for GEIT.
- All parties supporting the governance process should understand the business and IT objectives.

- Ensure that there is effective communication and enablement of the necessary organizational and process changes.
- Tailor GEIT frameworks and good practices to fit the purpose and design of the enterprise.
- Focus on quick wins and the prioritization of the most beneficial improvements that are easiest to implement.

Strategic Vision

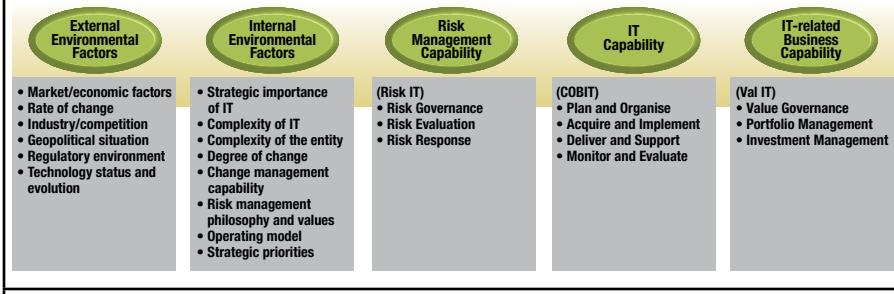
Risk IT and Val IT, both based on COBIT, provide tangible business benefits to enterprises. Risk IT reduces regulatory concerns, which allows more IT innovation to support new or expanded business initiatives. Its implementation can also result in fewer operational surprises and failures, improved information quality, and increased stakeholder confidence. From the valuation side of an enterprise's governance program, Val IT provides continued real-time quantification of current IT investments, verifying if and why a specific IT investment has been successful. Val IT is also used to assess the value of new or in-process development IT projects, monitoring the development and the operational costs.

BMIS facilitates a system's look at security, allowing for proactive, business-focused security management. By looking at areas such as enterprise culture and process, BMIS helps security professionals identify threats and risks that may not have been previously recognized until they were realized. In the cloud, BMIS will enable IT professionals to look at additional threats that arise from third parties, such as CSPs, and understand the impact that those threats have on the rest of the business.

These tools enable enterprise executives to manage IT direction in the same manner as all other business areas. This model and these frameworks "speak" the same language used in recognized best-practice business enterprise risk and value management programs. They provide C-level, non-IT decision makers a realistic, business-based comprehension of the risk and potential rewards arising from their IT initiatives.

The cloud provides very compelling business value reasons to opt in, but there is significant known, and still unknown, risk in this virtual space. The COBIT, Risk IT and Val IT governance and management frameworks and the BMIS model offer a means to address cloud IT risk and expected value at very granular levels. These interrelated risk/valuation point assessments are then aggregated into factors of external and internal environments, risk management capabilities, IT capabilities, and IT-related business capabilities (**figure 3.3**).

Figure 3.3—Cloud Factors



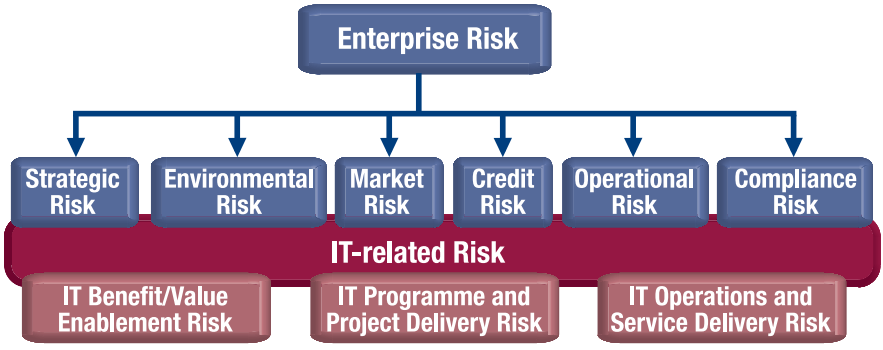
Source: ISACA, *The Risk IT Practitioner Guide*, USA, 2009, figure 38

Risk IT for the Cloud

Once cloud risk is brought into an enterprise's overall risk management plan, it becomes apparent that IT itself is involved in nearly every facet of an enterprise's operation. GEIT needs to be considered in all other governance, risk and compliance (GRC) programs moving forward. The cloud impacts every one of the six categories of enterprise risk in an enterprise (**figure 3.4**):

- **Strategic**—Can the enterprise's IT organization successfully execute the planned new cloud program successfully, on budget and on schedule? Will the cloud program provide the expected business benefit? Would not moving to the cloud cause additional levels of risk?
- **Environmental**—Will the cloud project provide a user environment—be it internal, partner or customer users—that is well thought out, intuitive and welcoming to use? Will the environment address the prespecified business needs and be able to accommodate requirements identified postimplementation?
- **Market**—Will the cloud program provide a user environment that matches or exceeds the experience offered by competitors? Will current and new users welcome and embrace the experience?
- **Credit**—Will the cloud program be completed and then maintained within estimated budgets, providing or exceeding the expected value?
- **Operational**—Will the operational support provided by the CSP maintain expected performance?
- **Compliance**—Can the new cloud program meet current and future regulatory requirements?

Figure 3.4—IT Risk in the Risk Hierarchy



Source: ISACA, *The Risk IT Framework*, USA, 2009, figure 3

Based on these six aggregated risk factors, specific and detailed risk scenarios for a possible cloud initiative can be identified (**figure 3.5**).

Figure 3.5—Example Cloud Initiative

High-level Risk Scenarios	Positive Example Scenarios	Negative Example Scenarios
New (cloud) technologies	• New technologies for new initiatives or more efficient operations adopted and exploited • Competitive advantage • Business innovation potential	• Failure to adopt and exploit new technologies (i.e., functionality, optimization) on a timely basis • New and important technology trends not identified • Inability to use the technology to realize desired outcomes (e.g., failure to make required business model or organizational changes)
(Cloud) technology selection	• Optimal technology selected for implementation • Ability to switch faster to newer technology	• Wrong technologies (i.e., cost, performance, features, compatibility) selected for implementation
Cloud investment decision making	• Coordinated decision making over IT investments between business and IT • Reduced IT investment	• Business managers or representatives not involved in important IT investment decision making (e.g., new applications, prioritization, technology opportunities)
Accountability over cloud (IT)	• Business assumes appropriate accountability over IT and codetermines the strategy for the cloud, especially application portfolio	• Business not assuming accountability over those cloud areas for which it should (e.g., functional requirements, development priorities, opportunity assessment through new technologies)

Figure 3.5—Example Cloud Initiative *(cont.)*		
High-level Risk Scenarios	**Positive Example Scenarios**	**Negative Example Scenarios**
Integration of cloud computing with business processes	• Fully integrated cloud solutions in place across business processes	• Separate and nonintegrated solutions to support business processes
Integration with legacy systems	• Systems with interoperability that work together to effectively handle enterprise information	• Systems unable to work together and key information not accessible. Security issues and duplication of efforts may also arise, resulting in increased costs for the enterprise.
State of cloud (infrastructure) technology	• Modern and stable technology used	• Obsolete technology in use that cannot satisfy new business requirements (e.g., security, storage)
Architectural agility and flexibility	• Modern and flexible architecture that supports business agility/innovation	• Complex and inflexible IT architecture obstructing further evolution and expansion
Software implementation in the cloud	• Faster development and higher quality of testing	• Operational glitches when new software is made operational • Users not prepared to use and exploit new application software
Selection/performance of cloud suppliers	• Cloud supplier acting as strategic partner • More choices and information available on cloud suppliers	• Inadequate support and services delivered by vendors, not in line with SLAs • Inadequate performance of CSP in large-scale, long-term cloud arrangements
Contractual compliance	• CSP exceeds contractual obligations	• Contractual obligations by CSP with customers/clients not met

Val IT for the Cloud

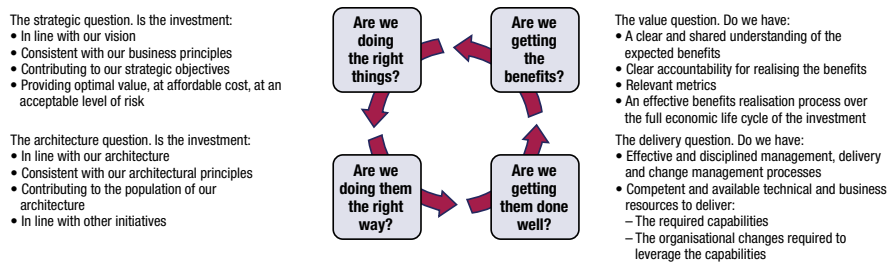
Concurrent or sequential to assessing cloud risk, evaluating the value of the cloud completes an enterprise's full business assessment of a cloud implementation: risk vs. reward.

Val IT helps determine an enterprise's possible value from a cloud project from a holistic viewpoint, best exemplified in **figure 3.6**, the Val IT "Four Ares":

- **Are we doing the right things?**—Would a cloud initiative align with existing business strategies of the enterprise? There may be financial benefits to the enterprise as a result of leveraging cloud services. Additionally, opportunities for growth and innovation that were constrained precloud because of IT costs may become available to enterprises.

- **Are we doing them the right way?**—Is the cloud initiative a natural fit to the existing enterprise? If an enterprise wishes to grow without increasing operational IT costs, the cloud may be a potential solution.
- **Are we getting them done well?**—Is the cloud initiative implemented effectively? Moving toward cloud services is a business decision that must be weighed. Once the decision to leverage the cloud is made, it is important that the transition be done according to determined processes. Governance and management are critical in leading the change in policy and business processes that will result. Additionally, metrics to report against are important to show implementation success.
- **Are we getting the benefits?**—Is the cloud delivering the expected benefits? Performance goals and objectives need to be determined before an enterprise has transitioned to the cloud. It is important to determine what is needed from business leaders in terms of availability, flexibility, scalability, auditability, etc., so that the client can measure these things to help determine success.

Figure 3.6—Val IT "Four Ares"



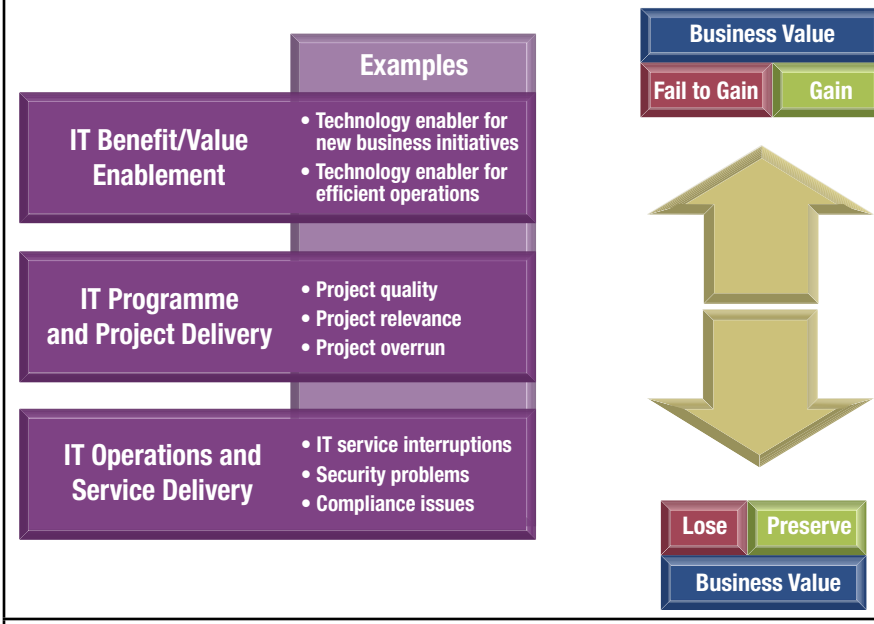
Source: ISACA, *Enterprise Value: Governance of IT Investments*, The Val IT Framework 2.0, USA, 2008, figure 3. Based on the "Four Ares" as described by John Thorp in his book, *The Information Paradox—Realizing the Business Benefits of Information Technology*, written jointly with Fujitsu, first published in 1998 and revised in 2003, McGraw-Hill, Canada.

Clearly, Val IT provides an enterprise's governance process with a thorough valuation of the results of a cloud program. As with Risk IT, Val IT requires IT governance managers to consider the strategic objectives of other effected groups within enterprises, ensuring that a cloud implementation aligns with the enterprise's true business needs.

Business Case Development

After the enterprise agrees on the business objectives for a new cloud program, these objectives must be further expanded and detailed into an overarching business case for the cloud. This entails the itemization of the specific sought-after cloud business advantages compared with known, but allowing for yet-to-be-determined, cloud risk. As shown in **figure 3.7**, IT risk in the cloud needs to be viewed from a variety of fronts. This includes IT benefit/value enablement, IT program and project delivery, and then IT operations and service delivery.

Figure 3.7—IT Risk Categories From Risk IT Framework



Source: ISACA, *The Risk IT Framework*, USA, 2009, figure 2

How and Why to Use COBIT

The use of proven frameworks can help enable an enterprise to realize expected benefits from the cloud.

ISACA's COBIT has evolved to be a well-recognized IT risk and controls framework. Extending its use to cloud governance is a logical step because COBIT is flexible and allows for innovation. The COBIT framework:
- Is platform-agnostic, both in type and complexity
- Has sufficient depth to address nearly all the technical aspects of cloud computing
- Provides clearly defined risk assessment measures—not just binary, but rather a maturity model scale of 1 through 5

COBIT addresses IT risk and controls throughout an entire program life cycle. Reflecting actual program implementations, these risk controls are interrelated. Controls are categorized in the following four domains:
- **Plan and Organize (PO)**—Provides direction to solution delivery (Acquire and Implement) and service delivery (Deliver and Support)
- **Acquire and Implement (AI)**—Provides the solutions and passes them on to be turned into services

- **Deliver and Support (DS)**—Receives the solutions, making them usable for end users
- **Monitor and Evaluate (ME)**—Monitors all processes to ensure that the direction provided is followed

These domains are distilled into 34 processes that are further refined by four to 15 control objectives each. The control objectives that are applicable to cloud computing are listed in appendix A.

IT risk managers, working with application and data owners and administrators, can develop a comprehensive IT-based risk assessment using:
- COBIT 4.1's 210 control objectives
- Detailed guidelines of the interrelationships of inputs and outputs to and from other COBIT 4.1 processes
- A Responsible, Accountable, Consulted and/or Informed (RACI) chart, which identifies likely risk assignments among organizational functions
- Specified risk assessment maturity model quantification

A COBIT-based assessment will provide the enterprise with a set of effective measures for gauging and controlling activities related to a cloud deployment or utilization. The seven COBIT information criteria reflect specific requirements for information:
- **Effectiveness**—Information is relevant and pertinent to the business process and is delivered in a timely, correct, consistent and usable manner.
- **Efficiency**—Information is provisioned through an optimal (most productive and economical) usage of resources.
- **Confidentially**—Sensitive information is protected from unauthorized disclosure.
- **Integrity**—Information is accurate and complete, and it is valid in accordance with an enterprise's sets of values and expectations.
- **Availability**—Information is available when required by the business process and is always maintained securely.
- **Compliance**—The enterprise is able to address compliance with applicable laws, regulations and contractual arrangements to which business processes are often subjected, i.e., externally imposed business criteria.
- **Reliability**—IT systems provide management with appropriate information to use in operating the entity, e.g., financial reporting to users of the financial information, and with information to report to regulatory bodies with regard to compliance with laws and regulations.

Governance Considerations

Establishing Business Goals for the Cloud

IT is most likely a strategic asset for an enterprise. When properly implemented, the cloud can be an extension of this asset. Proper implementation requires recognizing and establishing controls to offset known and future cloud risk. Before any of this can occur, the cloud governance committee needs to detail the enterprise's expected business objectives for the cloud program.

Figure 3.8 details a suggested process sequence to obtain consensus across the business. This governance process requires detailed interaction among all affected business groups. As noted in item 6 of this sequence, once the initial requested information is gathered from affected groups and assimilated, that information needs to be reviewed by other groups before adoption. It is entirely possible that one business group's intent for the cloud may impact another group, without understanding of the possible implications.

Figure 3.8—Establishing Business Goals for the Cloud Program

	Establishing Business Goals for a Cloud Program	COBIT 4.1	Risk IT	Val IT
1	Identify the desired business goals beyond capabilities of current IT.	PO1.3, PO3.1	Risk Evaluation (RE) 3.3	Investment Management (IM) 1.1, Portfolio Management (PM) 1.4
2	Define the opportunities envisioned for a cloud application.	PO1.4		IM 1.2, Value Governance (VG) 1.4
3	Quantify the gains envisioned in a cloud application.	PO5		IM1.3, IM4.1
4	Identify the required cloud application processes to achieve stated goals.	AI2.1	Risk Governance (RG) 3.3	IM2.2, IM4.2, PM1.2
5	Identify the applicable compliance regulations.	ME3		
6	Verify these values (for items 1 to 5) with all applicable stakeholders.			IM4.3
7	Compare these goals for the cloud vs. traditional IT.			IM2.2
8	Develop a detailed business case.	PO1.1		IM4.1, IM5.1

Linking IT and Business With COBIT

The business aspect of COBIT consists of linking business goals to IT goals, providing metrics and maturity models to measure their achievement, and identifying the associated responsibilities of business and IT process owners.

While the information criteria provide a generic method for defining the business requirements, defining a set of generic business and IT goals provides a business-related and more refined basis for establishing business requirements and developing the metrics that allow measurement against these goals. Every enterprise uses IT to enable business initiatives, and these can be represented as business goals for IT. COBIT provides a matrix of generic business goals (**figure 3.9**) and IT goals (**figure 3.10**) and shows how they map to the information criteria.

Figure 3.9—Linking Business Goals to IT Goals

		Business Goals	IT Goals								COBIT Information Criteria: Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
Financial Perspective	1	Provide a good return on investment of IT-enabled business investments.	24									✔					
	2	Manage IT-related business risk.	2	14	17	18	19	20	21	22			✔	✔	✔		
	3	Improve corporate governance and transparency.	2	18													✔
Customer Perspective	4	Improve customer orientation and service.	3	23							✔						
	5	Offer competitive products and services.	5	24							✔	✔					
	6	Establish service continuity and availability.	10	16	22	23					✔				✔		
	7	Create agility in responding to changing business requirements.	1	5	25						✔	✔					
	8	Achieve cost optimisation of service delivery.	7	8	10	24						✔					
	9	Obtain reliable and useful information for strategic decision making.	2	4	12	20	26				✔			✔			✔
Internal Perspective	10	Improve and maintain business process functionality.	6	7	11						✔	✔					
	11	Lower process costs.	7	8	13	15	24					✔					
	12	Provide compliance with external laws, regulations and contracts.	2	19	20	21	22	26	27				✔			✔	
	13	Provide compliance with internal policies.	2	13									✔			✔	
	14	Manage business change.	1	5	6	11	28				✔	✔					
	15	Improve and maintain operational and staff productivity.	7	8	11	13					✔	✔					
Learning and Growth Perspective	16	Manage product and business innovation.	5	25	28						✔	✔					
	17	Acquire and maintain skilled and motivated people.	9								✔	✔					

Source: ISACA, COBIT 4.1, USA, 2007, appendix I, page 169

Figure 3.10—Linking IT Goals to IT Processes

	IT Goals	Processes											COBIT Information Criteria						
													Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
1	Respond to business requirements in alignment with the business strategy.	PO1	PO2	PO4	PO10	AI1	AI6	AI7	DS1	DS3	ME1		P	P		S	S		
2	Respond to governance requirements in line with board direction.	PO1	PO4	PO10	ME1	ME4							P	P					
3	Ensure satisfaction of end users with service offerings and service levels.	PO8	AI4	DS1	DS2	DS7	DS8	DS10	DS13				P	P		S	S		
4	Optimise the use of information.	PO2	DS11											S		P			S
5	Create IT agility.	PO2	PO4	PO7	AI3								P	P		S			
6	Define how business functional and control requirements are translated in effective and efficient automated solutions.	AI1	AI2	AI6									P	P				S	
7	Acquire and maintain integrated and standardised application systems.	PO3	AI2	AI5									P	P				S	
8	Acquire and maintain an integrated and standardised IT infrastructure.	AI3	AI5										S	P					
9	Acquire and maintain IT skills that respond to the IT strategy.	PO7	AI5										P	P					
10	Ensure mutual satisfaction of third-party relationships.	DS2											P	P	S	S	S	S	S
11	Ensure seamless integration of applications into business processes.	PO2	AI4	AI7									P	P		S	S		
12	Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels.	PO5	PO6	DS1	DS2	DS6	ME1	ME4					P	P				S	S
13	Ensure proper use and performance of the applications and technology solutions.	PO6	AI4	AI7	DS7	DS8							P	S					
14	Account for and protect all IT assets.	PO9	DS5	DS9	DS12	ME2							S	S	P	P	P	S	S
15	Optimise the IT infrastructure, resources and capabilities.	PO3	AI3	DS3	DS7	DS9							S	P					
16	Reduce solution and service delivery defects and rework.	PO8	AI4	AI6	AI7	DS10							P	P		S	S		
17	Protect the achievement of IT objectives.	PO9	DS10	ME2									P	P	S	S	S	S	S
18	Establish clarity of business impact of risks to IT objectives and resources.	PO9											S	S	P	P	P	S	S
19	Ensure that critical and confidential information is withheld from those who should not have access to it.	PO6	DS5	DS11	DS12										P	P	S	S	S
20	Ensure that automated business transactions and information exchanges can be trusted.	PO6	AI7	DS5									P			P	S	S	
21	Ensure that IT services and infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster.	PO6	AI7	DS4	DS5	DS12	DS13	ME2					P	S		S	P		
22	Ensure minimum business impact in the event of an IT service disruption or change.	PO6	AI6	DS4	DS12								P	S		S	P		
23	Make sure that IT services are available as required.	DS3	DS4	DS8	DS13								P	P			P		
24	Improve IT's cost-efficiency and its contribution to business profitability.	PO5	DS6										S	P					S
25	Deliver projects on time and on budget, meeting quality standards.	PO8	PO10										P	P		S			S
26	Maintain the integrity of information and processing infrastructure.	AI6	DS5										P	P		P	P		S
27	Ensure IT compliance with laws, regulations and contracts.	DS11	ME2	ME3	ME4										S	S		P	S
28	Ensure that IT demonstrates cost-efficient service quality, continuous improvement and readiness for future change.	PO5	DS6	ME1	ME4								P	P					P

Source: ISACA, COBIT 4.1, USA, 2007, appendix I, page 170

A way to implement GEIT (internal controls) for the cloud is by selecting the business goals that are relevant for the enterprise when making use of cloud capabilities. Looking at COBIT's identified business goals, it is fair to identify business goals 1, 2, 6, 7, 8, 11, 14 and 16 as being of particular importance in a cloud environment. The example drawings in **figures 3.11** and **3.12** demonstrate the linkages for two key cloud business goals to IT goals and the IT goals to the COBIT IT processes that have to be implemented in a mature way to ensure the achievement of the goals.

Figure 3.11—Linking Business Goals With IT Goals

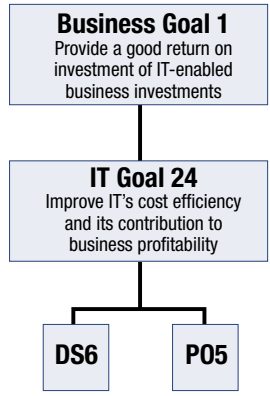
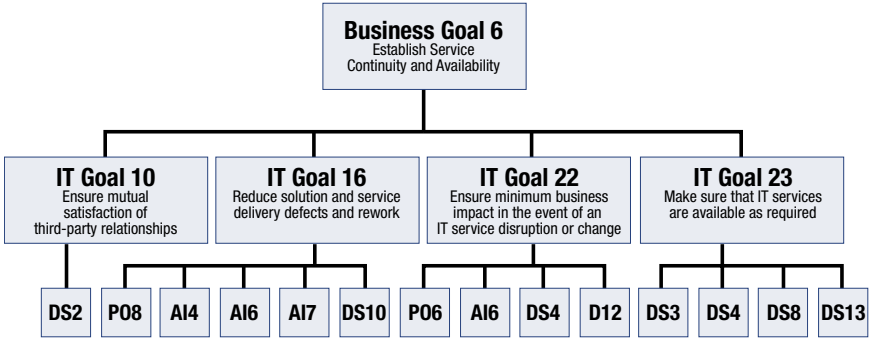


Figure 3.12—Linking IT Goals With IT Processes



Mapping Governance to the COBIT, Risk IT and Val IT Frameworks

Developing a risk assessment based solely on COBIT would be sufficient if the results were intended only to assist IT department governance decisions. However, moving to a cloud environment may cause a paradigm shift in business processes, so the IT business risk assessments must be shared, comprehended and jointly governed by all affected business managers (C-level to business line managers) from across the enterprise. The presentation of the cloud governance analysis needs

to be formatted in a manner that is easily internalized and readily and continually communicated to all affected departments.

This is where Risk IT and Val IT come into play. Risk IT supports cloud IT risk assessments based on COBIT 4.1 while adding its own guidelines into a governance process of the same style, depth and direction as current, best-of-breed enterprise risk management (ERM) business frameworks. Val IT provides a similar process view, but from the investment perspective. Risk IT and Val IT offer a governance process at the same level employed by other business programs, but also encompasses all salient IT issues.

Tactical Requirements
Enterprise governance of cloud projects requires acknowledgment of regulatory compliance requirements at both where the data are sourced and where the data are stored. New legal issues are already arising relative to the cloud. Detailed due diligence, an understanding of expected cloud client responsibilities, and review and negotiation of candidate CSP SLAs and contracts are strongly recommended.

Regulations
Online and computer-stored information faces a plethora of compliance regulations worldwide that vary by country or state. Since the cloud will contain data from many sources and from many locations, stored on servers across the world, regulation compliance will be a challenge. Most regulations apply to data relative to their source, but other regulations apply to the physical location of the data storage.

It is the cloud client's responsibility to ensure that its data and applications hosted by a CSP meet the various applicable local, national and international privacy, health data or financial accountability compliance laws. It is not uncommon to find various laws in contradiction or not aligned with the technical capabilities of the cloud.

This is another area in which Risk IT offers risk managers the means to drill down into the various personal privacy, health information or financial records regulations to assess each act's impact on the enterprise via the cloud. Since Risk IT is dynamic, it allows for changes to current law enforcement policies' risk impacts to propagate through the GRC program.

Legal Issues
Legal professionals are beginning to address newly recognized issues within the cloud computing industry using legal precedents from other areas of business law. Based on these precedents, legal professionals are providing advice to various legislatures worldwide for new potential cloud law enactments.

For example, in an attempt to update procedures to enforce PII laws in the UK, the Information Commission Office (ICO) has been accepting inputs from legal cloud specialists.

Many major CSPs offer clients SLA clauses that are primarily for the protection of the provider, offering limited legal assurances for the client. In addition, some basic, rudimentary concepts of business law are not clear in the cloud, for example:
- Who is the legal owner of client data once they are uploaded to the cloud?
- Are CSPs willing to accept certification responsibilities for compliance?
- What is a CSP willing to provide cloud clients as compensation for the loss or corruption of data entrusted to the CSP?

Due Diligence
While it may appear to be onerous, conducting research into the business backgrounds of potential CSPs is a critical facet of the cloud GRC process. Various cloud thought leaders have identified issues that need to be researched and assessed:
- **Know your provider**—The financial industry has long exercised due diligence in the form of "know your client" (KYC) to avoid accepting new business from terrorist organizations or clients recognized as money launderers for the illegal drug trade or engaged in other criminal activities. Similarly, prospective cloud clients need to be assured that their candidate CSP is a legitimate provider and not a front company for an organization that may use the client's data for illegal or cyberterrorism purposes.
- **Right to audit**—As is reflected in many current third-party provider security assurance programs, the client and the CSP need to agree in advance that the client has accessibility to the CSP to audit and verify the existence and effectiveness of security controls specified in the SLA. The pre-engagement security controls audit then becomes the benchmark for ongoing audits once the cloud contract is in place. For CSPs with very high volumes (hundreds) of cloud clients, this could become troublesome. That is why a broadly agreed industry standard, best-practice security certification will be a readily embraced tool, once available.
- **Assured continuity**—As in any new industry that shows signs of success, many enterprises have entered the CSP space. Sooner or later, there will be a shake-out in which the less effective or successful fall by the wayside. Enterprises should consider whether their prospective CSP has the financial stability to provide continual cloud services during the shake-out or whether the CSP will be able to transfer the enterprise's data and/or cloud-based applications back to the enterprise if it does cease operations.
- **Security policy and process transparency**—Clients should ascertain whether the prospective CSP is willing to share copies of its current security and disaster recovery/business continuity (DR/BC) policies. Enterprises should seek a CSP whose level of operational security appears to be at least as mature as, if not more mature than, the enterprise's level of security.

Undoubtedly, as business evolves in the cloud industry, more legal issues will arise.

Operational Activities
Once the higher-level risk assessment priorities are blocked out, COBIT 4.1, Risk IT and Val IT provide direction for enterprises' governance assessments

to become as granular as needed to quantify a complete picture of business risk vs. business opportunity available in the cloud. The next level of assessment incorporates benchmarking the required level of CSP services against what the enterprise needs and benchmarking current best CSP service offerings.

Additionally, potential CSP SLAs must be reviewed to determine whether the CSP's offering aligns technically and legally with the enterprise's requirements. Key considerations to reflect in a cloud contract may include:
- The CSP should provide clients with real-time performance, access management and security monitoring dashboards.
- The CSP's assured level of uptime for the enterprise's application should be determined.
- Records of application changes or IAM modifications should be available for client audit.
- The CSP should engage with clients on regular DR/BC exercises to practice for a potential real incident and improve DR/BC procedures as needed based on the exercise results.
- The CSP should provide reference contacts of existing clients, allowing the prospect to verify the CSP's service performance contentions.

CSP Contracts and Final SLA Review
It is always important to thoroughly review the potential CSP's contract terms, conditions and SLA. This is to assure the prospective client that the CSP can legally offer what it has verbally committed to and that the cloud risk from the CSP's service offerings is within the determined level of acceptable risk of the prospective client. Other considerations include:
- The potential CSP's security and service commitments meet client SLA requirements.
- Key cloud legal issues are detailed to the client's satisfaction in the CSP's contract or SLA.
- The CSP will allow the cloud client the right to audit the CSP's operations on a regular basis to verify that security controls are in place and effective.

Outcome of Good Governance
By initiating a governance program, enterprise leaders can identify, at a high level, cloud computing's benefits and risks. The COBIT, Risk IT and Val IT frameworks provide guidance on drilling down into the detailed aspects of each broad risk and value area, while allowing final analysis results to percolate back up to high-level issues.

When employing the described tools and methodologies, program decisions that were previously based on subjective rationales are better executed. These frameworks provide an excellent means to assess whether CSP offerings align with the enterprise's business expectations (valuations) and business risk tolerance levels.

Page intentionally left blank

4. Security and Cloud Computing

As discussed in chapter 2, among the many expected benefits from cloud computing are dynamic scalability, shorter development life cycles, reduction of IT CAPEX and the ability to outsource segments of an enterprise. However, as with any activity, risk is inherent to the cloud. It presents the very same issues found in the traditional IT world, but also introduces new threats and vulnerabilities that may be exaggerated due to the lack of physical visibility and the perceived loss of control over assets and information. Cloud risk includes:

- Cloud computing aggregates many enterprises' data into single files.
- Large volumes of data stored in a single location may be valuable targets for theft.
- A single unauthorized penetration may lead to the access of multiple enterprises' data.
- Many enterprises' information environments are transitioning to combinations of traditional physical systems coupled to the cloud computing platform.

The cloud brings some new threats that may increase an enterprise's overall risk posture, but as a general rule, it is still IT risk. What changes is the context. As enterprises make their way into cloud services, it will be critical that their IT leadership examine their risk from different perspectives. It is important for IT leaders to identify and assess both traditional and new risk and convey their assessments to their enterprise's decision makers prior to entering into a cloud computing application.

Beginning in 2008, many global economies entered a significant economic recession. In response, enterprises slowed their discretionary spending, resulting in a decrease in IT investments.

Businesses Are Ready for the Cloud

As enterprises continue to search for ways to reduce expenses, the cloud offers the opportunity to innovate in IT while saving on routinely incurred costs, yet this is not without risk.

Some analysts have indicated that unless an enterprise is comfortable with the level of risk it will assume by moving to cloud computing services, it should not consider moving critical applications and sensitive data to cloud environments. While this conservative statement may sound prudent and reasonable, a better approach is to consider the risk relative to the inherent risk in a given situation. This approach can help the enterprise to determine whether the business is ready for the cloud and whether the cloud is ready for the business.

The latter question leads to a series of specific key questions, the answers to which should be weighed before taking any action to move to a cloud service. Some of these questions include:

- What is the enterprise's expected availability?
- How are identity and access managed in the cloud environment?
- Where will the enterprise's data be located?
- What are the CSP's disaster recovery capabilities?
- How is the security of the enterprise's data managed?
- How is privileged user access to data managed?
- How is the enterprise's information protected from user abuse?
- What type of isolation can the enterprise expect?
- How is the enterprise's information secured on a virtualized environment?
- How is the entire system protected from Internet threats?
- How are activities monitored and audited?
- How will the enterprise ensure that no one has tampered with its data?
- What type of certification or assurances can the enterprise expect from the provider?

The answers to these questions may provide an enterprise with some important initial information that may guide decisions such as what type of data, if any, belong in the cloud.

Risk Considerations

As with any new technical solution, the cloud provides enterprises with opportunity and risk. For risk to exist, some factors need to be present: a valid threat with the opportunity to exploit a known vulnerability, a likelihood of such an exploitation occurring and a resulting impact. A threat is any event that, if it occurs, can cause harm to a system or individuals and create a loss of confidentiality, integrity and/or availability of information or the systems processing the information.

Many of the threats are not unique to the cloud environment; potential data loss, poor management by a service provider, service interruption and unauthorized access to sensitive data also are applicable to existing third-party initiatives. However, that does not mean there are no new security considerations. The cloud introduces new vulnerabilities, and unique idiosyncrasies to existing vulnerabilities, that call for thorough risk analysis and management.

From a business perspective, moving to the cloud may be taken with a "business as usual" attitude; however, for those responsible for operational or information risk management, there are many substantive considerations. Significant among these are unclear trust boundaries; ubiquitous logical, not physical, data separation; increased network security exposures; greater application security risks within the cloud stack; and the absence of an accepted and established governance model for the cloud environment.

Graduated Risk Responsibilities

Cloud computing risk varies among CSP service delivery models—SPI—and among the cloud computing deployment models—public, private, community or hybrid.

For example, a private cloud deployment model, using virtualized applications within an enterprise's data centers or on leased third-party servers, is similar to traditional IT enterprises and the risk is also most aligned with existing traditional IT enterprise risk.

Conversely, in a public cloud deployment model, many clients collectively utilize the same CSP resources, sharing servers, applications and data files as needed by each cloud client. The location of the cloud computing server(s) is continuously changing, and the amount of data stored and the cloud clients storing it are in flux.

The numbers of users, the shared levels of the operating stack, and the size and complexity of the virtual enterprise perimeter are much larger in the public cloud. As a result, risks from a public cloud deployment model are much more significant and different from traditional IT enterprise risks.

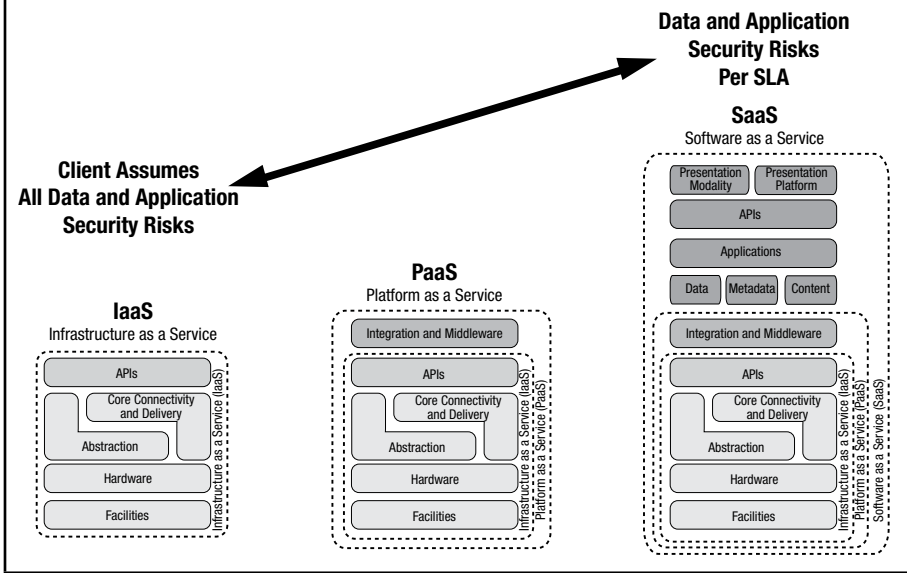
A large public cloud can be viewed like a large urban public transportation system. People are boarding and leaving trains, subways and buses continually, each with unique boarding points and end destinations. However, they all share the same system for their journey. They all bring personal data, valuables, PII and perhaps enterprise data on the notebook computers with which they travel.

Cloud computing clients maintain ultimate accountability for each security risk element. CSPs offer security risk administrative responsibilities on a graduated progression as their cloud services delivery model progresses, i.e., transitioning from an IaaS to a PaaS, then to an SaaS. In many cases, the immediate responsibilities of risk controls are shared between the CSP and its clients.

Demarcation lines between the CSP's and the cloud computing client's responsibilities for shared risks vary (**figure 4.1**). These variations can be attributed to the services delivery model used, the CSP vendor, the requirements of the prospective cloud computing client and the security classifications of the client data being migrated to the cloud computing platform.

In general, for the public cloud IaaS service delivery model, CSPs typically offer clients basic physical and administrative security provisions for their bare-bones cloud servers, i.e., physical security, intrusion detection systems (IDSs), intrusion prevention systems (IPSs), log management, and security information and event management (SIEM).

Figure 4.1—Varying Levels of Risk Management



Source: Universal Model, © Cloud Security Alliance. Used with permission.

If contracting a PaaS service delivery model in the public cloud deployment model, IAM application; configuration management; and governance, risk and management tools may be added as risk control services.

At the top of the service model stack, for SaaS offerings, CSPs may additionally offer performance monitoring, encryption and secure communication via virtual private networks (VPNs).

Between the immaturity of this industry and a current lack of cloud delivery standards, there is a wide disparity in the quality and maturity level of CSPs' risk control offerings. Prospective cloud computing clients need to gain a complete comprehension of the scope and specific details of the security controls that the CSPs provide. Additionally, the expected risk responsibilities required of the prospective client must be specifically detailed. For shared risks, the specific hand-off points of risk control between the CSP and the client need to be detailed, down to the level of actual event scenarios. During the negotiations, the specific risk responsibilities and the CSP's actual risk control capabilities need to be determined and a decision made as to whether they are adequate for the prospective cloud client's risk control needs.

Tools and processes that are currently in place to improve enterprise efficiency and effectiveness—such as IAM, physical security controls, change management systems, systems and software development life cycles (SDLC), and disaster recovery—may be impacted by moving to the cloud. Also, current perimeter controls in place—such as data loss prevention (DLP), firewalls, IPSs and SIEM

systems—may not be as effective because data that were once monitored internally have been intentionally moved offsite. This shift requires changes in processes and procedures to ensure that security incidents are not occurring.

It is important that every enterprise considering moving to the cloud first understand what information it holds, where it is and what the impact of a breach of that data would be. Information inventory, classification and labeling are important for all enterprises because information that is uncontrolled has the potential to be transformed from an asset to a liability. It is particularly critical that data owners understand the sensitivity of data currently stored within the enterprise that may be relocated to a cloud environment.

The following initiatives have significant implications for cloud computing.

IAM

Users have always been, and continue to be, a threat to enterprise data. Intentional and unintentional actions carried out by humans can put the enterprise in harm's way.

One way to control access to information is to implement an IAM system. Such systems can control and manage access to data based on user role, data classification and data type, among other things. However, IAM systems are inherently vulnerable to the same threat that they are protecting against: insider attacks by employees or other trusted parties. For IAM to be an effective security measure, it must be updated regularly to avoid unnecessary accretion of privilege (violation of least privilege) and continuing access by individuals who no longer are entitled, such as terminated employees or contractors whose period of service has ended. Policies should exist and be followed for adding new users, changing existing user access and deleting users no longer needing access. This process holds true with cloud computing because unauthorized access to enterprise information resources is a prime cause for data theft or corruption of data integrity through modification or deletion.

The IAM risk consideration for a private cloud setting is similar to the consideration for traditional enterprise IT settings. Since the data are segregated from all other cloud data and are often managed by the organization owning the data, access is typically restricted to users within the enterprise, business partners and e-commerce customers. However, the public cloud setting includes authorized users employed by the CSP, thereby allowing more people to handle information assets and increasing potential egress points.

By definition, public cloud clients share databases, sandboxes and applications—the multitenancy of resources. Within the multitenant databases, CSPs' clients' data are commingled; there is no guarantee that an enterprise's data are not stored with the data of a competitor. In major public cloud SaaS offerings, stored data could remain unprotected if the client fails to apply an encryption solution before pushing the data to the cloud. Having commingled data in the public cloud environment

certainly highlights the need for secure access controls. Access privileges should be granted according to the concept of least privilege, allowing only the access to data and applications in the cloud and within traditional enterprise borders needed to complete job requirements.

It is important to control access to all identified data within the enterprise and in the cloud. As enterprises move to private and public clouds, the risk of unauthorized access does not change; however, the vulnerabilities and the likelihood of unauthorized access increase.

Physical Security

Physical access risks for private clouds that employ virtualization of applications on internal servers or exclusive use of servers within data farms remain relatively similar to the physical access risks of traditional enterprises. Public clouds change the landscape, and physical access risks are often viewed incorrectly as being delegated or transferred to the CSP.

From an IT audit perspective, a cloud server's physical location may become more relevant in many instances. Physical security also is a component in CSPs' DR/BC plans. Included within the physical considerations are a CSP's dual, but separate, access connections to the Internet and site locations that may be susceptible to natural disasters. If the cloud servers are located in such regions, the physical layout of the cloud server facilities needs to be designed appropriately and alternate sites should be documented and tested. Cloud clients need to be sure to document their SLA expected disaster recovery service levels in addition to day-to-day availability requirements.

Physical security has access control implications as well. Under a traditional content-hosting contract, clients are typically aware of where their data are stored and clients may have some control over the types of requirements that must be met by employees with access to the data center. In a public cloud environment, on the other hand, there may be no such assurance or protection provided unless specifically stipulated in the terms and conditions of the contract.

Operational Risk

Operational risk includes the risk of unsuccessful or untested patch management, logical intrusions and possible outages, DR/BC, and the risk that accrues to application and data backups. A competent, responsible CSP should be expected to address these operational risks.

The integration of cloud services with a traditional enterprise dynamically expands an organization's enterprise security risk perimeter and the scope of the computational operations stack. Thus, the number of users also expands, as do the number and nature of entry points, to both the cloud application itself and to the remaining traditional enterprise.

Security Concerns

Many security concerns have been addressed with tools and processes in the previous section addressing risk. These tools and processes include concepts such as privacy and access control, business process risk, and operational risk. There is also security-specific risk that is not necessarily unique to the cloud, but that is amplified by its use. The Cloud Security Alliance (CSA) conducted a survey,[7] which resulted in a report of likely cloud risks:

- **Abuse and nefarious use of cloud computing**—A problem for both the CSP and the cloud client, abuse of the cloud has the potential to monopolize resources and negatively impact cloud users. Providers offer customers unlimited computing, network and storage capacity, often through an easy-access registration process. Anyone with a valid credit card can register and immediately begin using these cloud services. Some providers even offer free limited trial periods. The lack of control in registration permits anonymity in the cloud. This has provided many with malicious intent a platform to conduct (with relative impunity) activities such as finding vulnerabilities and writing malicious code in the cloud. PaaS providers have traditionally suffered most from this kind of attack, although hackers have begun to target IaaS vendors as well.
- **Insecure APIs**—CSPs expose a set of APIs allowing customers to manage and interact with cloud services. Provisioning, management, orchestration and monitoring are all performed using these interfaces. The security and availability of general cloud services are dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy. Furthermore, enterprises and third parties often build on these interfaces to offer value-added services to their customers. Since this introduces the complexity of a new layered API, it also increases risk because enterprises may be required to relinquish their credentials to third parties.

  While most CSPs strive to integrate security into their service models, it is critical for client risk managers to understand fully the security implications associated with the usage, management, orchestration and monitoring of cloud services. Reliance on a weak set of APIs exposes enterprises to a variety of security issues related to confidentiality, integrity, availability and accountability.
- **Malicious insiders**—The threat of a malicious insider is well known to most enterprises. While it is a familiar risk in traditional IT enterprises, it is even further amplified for clients of cloud services. Instead of dealing with its own employees, who were likely screened and chosen by the enterprise, the client now has to trust the CSP and its employees. There is often little to no visibility into the hiring standards and practices for cloud employees. The impact that malicious insiders can have on an enterprise is considerable, given their level of access. Brand damage, financial impact and productivity losses are just some of the ways a malicious insider can affect an operation. As enterprises adopt cloud services, the human element takes on an even more profound importance.

[7] CSA, *Top Threats to Cloud Computing V1.0*, USA, 2010, *https://cloudsecuringalliance.org/topthreats/csathreats.v1.0.pdf*

- **Shared technology vulnerabilities**—IaaS vendors deliver their services in a scalable way, sharing infrastructure. Often, the underlying components making up this infrastructure (e.g., CPU caches, graphics processing units [GPUs]) are not designed to offer strong isolation properties for multitenant architectures. To address this gap, a virtualization hypervisor mediates access between guest OSs computers and the physical computer resources. Still, as noted previously, hypervisors have exhibited flaws, enabling guest OSs to gain inappropriate levels of control or influence on the underlying cloud platform.

  Attacks have surfaced in recent years that target the shared technology inside cloud computing environments. Disk partitions, CPU caches, GPUs and other shared elements were never designed for strong compartmentalization. As a result, attackers focus on how to impact the operations of other cloud customers and how to gain unauthorized access to data.
- **Data loss/leakage**—As in traditional IT operations, there are many ways for data to be compromised in the cloud. Deletion or alteration of records without a backup is an obvious example. For encrypted data in an IaaS cloud, the loss of an encoding key could effectively mean data destruction. Access in public cloud environments (again, multitenant environments) can result in hundreds or more of possible users just one level of security away from the sensitive data of other cloud clients.
- **Account, service and traffic hijacking**—Account or service hijacking is not new, but as it does with many types of risk, cloud computing adds new dimensions. When attackers gain access to cloud client user credentials, they are able to "eavesdrop" on activities and transactions, manipulate data, return falsified information, and redirect cloud client e-commerce customers to illegitimate sites.

  IaaS applications can become new bases for an attacker. From here, the attacker may leverage the use of the cloud client's brand recognition to launch attacks on the cloud client's unsuspecting e-commerce customers.
- **Unknown risk profiles**—A tenet of cloud computing is the reduction of expenses to cloud users of IT hardware, software and maintenance. The cloud is intended to allow enterprises to focus on their core competencies, remotely outsourcing a portion or most of their IT. The financial and operational benefits have been promoted by cloud promoters and IT experts since the emergence of this technology.

  With this promise of better, cheaper and faster IT, the security ramifications of virtual computing, outside the traditional physical IT enterprise, can become minimized. This is especially true as increasing numbers of organizational decision makers have personal virtual backgrounds (online social networking, shopping, entertainment, etc.). They see cloud computing as accepted and used extensively in culture and wonder why this is not the case for business and commerce as well.

  Data, which may be widely dispersed among many cloud-based servers, is often described as a security asset. Security by obscurity may result in unknown exposures. It definitely impairs the in-depth analysis required for highly controlled or regulated business process.

Secure Code

SPI delivery models are defined as implementations of SOA-based applications and are comprised by linking robust, proven applets together. However, in today's cloud, many traditionally designed web applications are still in use, often lacking sound security provisions. Identified risk is sourced to the initial web application designs, and many of these original designs have been "cut and pasted" into other web applications, further expanding the number of these "grandfathered" security risks.

Page intentionally left blank

5. Assurance in Cloud Computing

The Merriam-Webster dictionary defines assurance as "something that inspires or tends to inspire confidence."[8] ISACA defines assurance as an "objective examination of evidence for the purpose of providing an assessment on risk management, control or governance processes for the organization."[9]

The previous chapters of this book have examined the challenges and risk inherent in cloud computing—challenges made even more daunting by the plethora of cloud computing solutions that have arisen over a short period of time. Before moving ahead with the decision to roll out a cloud service or utilize cloud computing, there is a strong need for assurance mechanisms.

What is certain is that assurance, and ultimately "confidence," in the cloud will be different from a traditional outsourcing arrangement. Previously, assurance was much better understood because boundaries were established; frameworks, including certification and accreditation (C&A) by third parties, were defined and available from independent service providers; and assurance was usually provided by looking at historical transactions that could be aligned with the client or isolated to defined locations and facilities. With shared resourcing, multitenancy and geolocation, cloud computing requires an entirely new approach to providing assurance. In the cloud, boundaries are difficult to define and isolate and client-specific transactional information is difficult to obtain. Assurance needs to become more real-time, continuous and process-oriented vs. transactional in focus, while CSPs need to provide greater transparency to their clients regarding the movement of the clients' data. Security and assurance frameworks and certification and accreditation standards that are specific to CSPs must continue to evolve as clients seek confidence in the services of the CSPs.

What are the mechanisms available for obtaining assurance in the cloud computing space? Part of the answer depends on whether one is a CSP or a cloud user. For example, consumers want assurance over the accuracy of cloud usage metering and billing processes so that they are not overbilled; CSPs, on the other hand, need assurance about the quality of the technology infrastructure to help ensure maximum availability and avoid revenue loss that may result if the cloud service offered is less than what was promised to the user.

Therefore, various stakeholders within the cloud ecosystem are looking for assurance. The key stakeholders are the organizations that offer cloud services and the cloud users. Depending on the nature of the cloud deployment model, there could be other stakeholders interested in assurance, e.g., the Data Protection Authority (DPA) of a country whose citizens store data in the cloud.

[8] *www.merriam-webster.com/dictionary/assurance*
[9] *www.isaca.org/Pages/Glossary.aspx?tid=3880&char=A*

Assurance by CSP

CSPs have incentives and are challenged to establish, monitor and demonstrate *ongoing* compliance with a set of controls that meets their own and their customers' business and regulatory requirements. The greater the assurance, the more confidence a client will have in the CSP, which results in increased adoption and deployment of cloud solutions in the industry. The level and type of assurance should be driven by the type of cloud service model (i.e., SaaS, IaaS or PaaS), the cloud deployment model (i.e., public, private, community or hybrid) and the users of the cloud. For example, a CSP offering a community cloud utilized by US federal government agencies needs to consider the US Federal Risk and Authorization Management Program (FedRAMP) security framework (described later in this chapter).

As discussed in previous chapters, CSPs need to have a strong governance and risk management process in place. In alignment with the overall direction of the enterprise, the CSP must execute the appropriate activities within the context of a controls framework, balancing performance and compliance in achieving the governance objectives of value creation, risk management and resource optimization.

Although compliance is a strong driver for governance, users are also interested in understanding the CSP's checks and balances. Both users and the CSP itself have an interest in helping to ensure the long-term sustainability of the CSP. As governance and risk management systems are established, assurance must be obtained in those areas. CSPs need to determine the audit mandate and who will be involved in assurance and they need to respond to assurance issues at a strategic level.

The objective of the assurance process is to provide feedback to both the CSP and the users on the nature, scope and level of risk and compliance. The scope of the assurance refers to a specific subject matter, such as hardware and software acquisition, and can refer to a specific period of time. The scope of assurance can include reference to:

- Specific criteria, such as reliability, effectiveness, efficiency, availability and confidentiality
- Subject matter, such as technical standards, guidance and practices, examples of which include COSO, BITS Shared Assessment, ISO and COBIT
- Professional working standards, guidelines and practices, such as those from ISACA, PCI, FedRAMP, the CSA Control Matrix, the American Institute of Certified Public Accountants (AICPA) or NIST. (Appendix B provides a cloud computing assurance program that can be utilized by a CSP or a client.)

Assurance can also be provided for various perspectives or scopes within a CSP. It can be provided for specific objects or assets, such as internal control, data, patents, alliances, human resources, projects or programs. Assurance can be provided at various levels within the CSP—at the overall enterprise level or the level of a specific entity such as a geographic area, data center or service offering. Assurance

can also be provided for various functionalities, such as efficiency, effectiveness and security.[10]

Managing enterprise risk requires setting and articulating the company's risk appetite/risk tolerance and establishing risk limits. If this has not been done, there are no guidelines linked to the enterprise's strategy to indicate how much or how little risk to take. As CSPs evolve, developing a risk appetite/risk tolerance will become an increasing area of focus for cloud users.

The assurance strategy for new CSPs should start with implementing an ERM framework. However, if the company's cloud offerings are an extension of an existing lines of business (e.g., Amazon has traditionally been in the business of offering an online shopping platform; Amazon Web Services is an extension of its shopping platform into the CSP business), the CSP should revisit the key assumptions in the existing ERM framework (assuming there is one) in light of the new CSP business goals. Risks that apply to the CSP business will vary. An existing traditional web-hosting provider that is planning to expand its services into the CSP business may discover little new risk from that already in existence; enterprises that are not involved with computer hardware and software services, however, are likely to experience entirely new risk.

Many Requirements and Standards

The cloud creates multiple governance challenges related to regulatory and compliance requirements. Traditionally, web-hosting companies have focused on a horizontal service layer such as hosting ERP software. Business process outsourcing (BPO) companies focus on an industry vertical such as processing of insurance claims or other financial transactions. A side benefit of the specialization is that the assurance requirements are limited and better defined. For example, ERP-hosting providers that support the processing of financial transactions for US public companies must design and implement internal controls to help their CSP clients comply with the US Sarbanes-Oxley Act of 2002. Companies processing claims for nonpublic insurance companies, captive insurance companies, or nonprofit insurers or health plans need to help those entities comply with the Model Audit Rule (MAR) from the US National Association of Insurance Commissioners (NAIC).

However, for public CSPs or for private clouds of large diversified conglomerates, the assurance requirements can be quite broad and not well defined. In the case of public CSPs, there may not yet be enough critical mass to allow them to focus on a horizontal or vertical and meet a defined set of assurance requirements.

The same factor that makes the value proposition compelling for a public cloud (compared to traditional outsourced application-hosting services), i.e., the isolation of cloud service offerings from the end user, also leads to a lack of clear direction around what meets the assurance requirements of the cloud users. For community

[10] ITGI, "Taking Governance Forward," *www.takinggovernanceforward.org/PDFs/assurance.pdf*

clouds that are built with a specific horizontal or vertical in mind, there may be better definitions regarding the assurance requirements since the clouds are built for a predefined group of users. For example, prior to introducing IaaS products available through the US federal government's *Apps.gov* web site, CSPs must complete the C&A process at the Federal Information Security Management Act (FISMA) Moderate Impact Data security level, as administered by the US General Services Administration (GSA). Once authority to operate is granted, IaaS services can be made available for purchase by government entities through the *Apps.gov* storefront.[11]

For a diversified conglomerate that decides to implement a private cloud, the assurance challenges across multiple businesses pertaining to the private cloud might be similar to the public CSPs.

Public clouds face a multitude of requirements and standards such as PCI, the US Sarbanes-Oxley Act, internal audits, privacy protection laws, audits from service auditors and external auditors, ISO certification, and customer audits. Third-party service providers can become inundated with a multitude of compliance efforts such as processing requests for information from existing and potential clients related to information security practices, supporting client auditors that may not be satisfied with an independent service auditor's report, and completing detailed checklists.

These one-off audits and compliance efforts take away valuable time from other activities, and are expensive intrusions on the CSP. The answer to this problem lies in CSPs adopting a consistent suite of sound assurance and policy practices that cuts across horizontal service lines and industry verticals. Even after the decision is made to implement these practices, the challenge does not end because there are multitudes of assurance frameworks available, ranging from the very broad to the very narrow.

Many Assurance Frameworks

With the ever-changing environment and the number of cloud computing options, there is a need for a suitable assurance framework. Many enterprises have put time into customizing existing or creating new assurance frameworks for the cloud, but the environment is still evolving and the effort to create a consistent and broadly accepted framework remains a work in progress. At the time this document is being published, there is no single assurance framework that broadly meets the needs of every type of CSP and client.

The existing assurance frameworks can be classified into two broad categories:
1. Existing widely accepted frameworks customizable for the cloud (i.e., COBIT, ISO 2700x)
2. Frameworks built for the cloud (i.e., CSA Security Matrix, Jericho Forum® Self-Assessment Scheme)

[11] US General Services Administration (GSA), "Cloud-based Infrastructure as a Service Comes to Government," 19 October 2010, *www.gsa.gov/portal/content/193441*

The following is a short summary of various standards, certifications or assurance frameworks available:

- **COBIT**—Developed and maintained by ISACA, COBIT provides management a comprehensive framework for the control and governance of business-driven, IT-based projects and operations. COBIT also offers mappings to other frameworks such as NIST Special Publication (SP) 800-53, ISO 17799, ITIL, Capability Maturity Model Integration (CMMI) and Project Management Body of Knowledge (PMBOK). Appendix A maps the COBIT 4.1 control objectives to the cloud.
- **AICPA Service Organization Control (SOC) 1 Report**—An SOC report is an independent, third-party examination under the AICPA/Canadian Institute of Chartered Accountants (CICA) audit standards. Released under Statement of Standards for Attestation Engagements (SSAE) No. 16 and the International Standard on Assurance Engagements (ISAE) 3402, SOC reports replaced the previously used Statement on Auditing Standards (SAS) 70 third-party examination reports effective 15 June 2011. Under an SOC report, a CSP engages a CPA firm to perform an independent examination to provide the CSP clients and their internal and external auditors assurance regarding the understanding and reliance on controls that support the CSP client's processes and systems. There are three SOC report forms available. SOC 1 reports apply to financial reporting processes and are most consistent with prior Statement on Auditing Standards 70 reports. SOC 2 and SOC 3 reports are discussed in the following bullet as AICPA Trust Services. SOC reports provide the client with an understanding of the nature and significance of the services provided and the relevant impact in identifying and assessing the risks and assurances by the CSP.
- **AICPA/CICA Trust Services (SysTrust and WebTrust)**—Intended to provide assurance that an enterprise's systems controls meet one or more of the Trust Services principles and related criteria. Areas addressed by the principles include security, online privacy, availability, confidentiality and processing integrity. SysTrust is similar to an SOC 1 report, but with predefined principles and criteria. However, these principles, while of the proper intent needed for cloud risk assurance, may lack the specificity required to be effective in a cloud environment. IT auditors could insert within these overarching controls specific risk control points, but the responsibility is on the user auditors to properly determine these more detailed control points. Also, effective in 2011, Trust Service reports can be issued as SOC 2 or SOC 3 reports under the SSAE standard noted previously.
- **ISO 2700x**—This is the specification against which an enterprise's information security management system (ISMS) is evaluated and by which certification is granted. The objective of the standard is to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an ISMS." The ISO certification is not a one-off exercise: Maintaining the certificate requires reviewing and monitoring the ISMS on an ongoing basis. More than 1,000 certificates have been issued across the world. Additionally, CSA's Cloud Security Matrix has been identified an appropriate ISO controls subset for the cloud.[12]

[12] Cloud Security Alliance (CSA), *https://cloudsecurityalliance.org/cm.html*

- **Cloud Security Matrix**—Released by CSA in April 2010, this cloud security controls matrix is specifically designed to provide fundamental security principles to guide cloud vendors and assist prospective cloud clients in assessing overall security risks of a CSP. The foundation of CSA's controls matrix is other industry-accepted security standards, regulations and controls frameworks. CSA's matrix is an amalgam of controls from HIPAA, ISO/IEC 27001/27002, COBIT, PCI and NIST.
- **FedRAMP**—FedRAMP provides a framework for assessing and authorizing cloud computing services. FedRAMP is designed for federal agency use, but can be used for joint authorizations and continuous security monitoring services for both government and commercial cloud computing systems.
- **NIST SP 800-53**—The NIST IT security controls standards, much like ISO and COBIT, contain a controls framework required to address cloud security. Also similar to ISO and COBIT, the NIST IT security controls standards form an unspecified subset of the entire framework. Note: The current draft of NIST SP 800-146 contains additional guidance for using cloud service models.
- **Health Information Trust Alliance (HITRUST)**—HITRUST has developed an information controls framework specific to the health industry. It was created especially for the US HIPAA regulations and the new HITECH program that is moving all US patient information online, not unlike what already exists in other parts of the world.
- **BITS**—The BITS Shared Assessment Program contains the Standardized Information Gathering (SIG) questionnaire and Agreed Upon Procedures (AUP). They are used primarily by financial operations evaluating the IT controls their IT service providers have in place for security, privacy and business continuity. SIG is aligned with ISO/IEC 27002:2005, PCI Data Security Standard (PCI DSS), COBIT and NIST and is also aligned with US Federal Financial Institutions Examination Council (FFIEC) guidance, the AICPA/CICA Privacy Framework and a host of other privacy regulatory guidance organizations. Like the other frameworks mentioned, BITS covers most, but not all, security elements of cloud computing, with a subset of the entire questionnaire. BITS has also mapped its control framework for CSPs.

  (In 2010, Shared Assessments published *Evaluating Cloud Risk for the Enterprise*, a risk-based guidance to evaluating cloud computing for the enterprise, *sharedassessments.org/media/pdf-EnterpriseCloud-SA.pdf*.)
- **Jericho Forum® Self-Assessment Scheme (SAS)**—A guideline for vendors to self-assess the security aspects of their cloud offering and for prospective cloud clients to include into their requests for proposal (RFPs), Jericho Forum's Self-Assessment Scheme is based on the organization's "11 Commandments," released in 2006, which are design principles for effective security in deperimeterized environments. This Self-Assessment Scheme is designed to assess cloud security tools, either applications or devices.
- **European Network and Information Security Agency (ENISA)**—In November 2009, ENISA released a report titled "Cloud Computing—Benefits, Risks and Recommendations for Information Security." This report defines a multitude of risk points in the cloud, covering the various delivery and deployment models.

An industrious IT auditor could readily translate specific risk points into control points, then into IT audit tests. Obviously, the appropriate tests for the type of cloud service at hand would need to be identified.

Other standards and frameworks are also available and can be used; however, selecting the most appropriate assurance framework or combining portions from each framework requires careful planning and involvement of the relevant stakeholders. An external audit of the cloud service will likely be required for customers to gain comfort over the effectiveness of the CSP's controls. CSPs have been working diligently to provide transparency to clients regarding risks and controls to avoid onsite audits and build confidence with clients. Historically, enterprises have used a variety of assurance frameworks to assess the controls of outsourced services, including services provided by CSPs. **Figures 5.1** and **5.2** summarize some of the most common frameworks and their applicability to CSPs.

Figure 5.1—Common Framework CSP Applicability for Third-party Certification/Examination

Certification/Framework—Description	Benefits	Challenges
SOC 1 Examination—An independent, third-party examination under the AICPA/CICA attestation standards. Released under the Statement of Standards for Attestation Engagements (SSAE) No. 16 and the International Statement of Attestation Engagements (ISAE) 3402. CSPs can engage a CPA firm to perform an SOC 1 report to provide clients and their auditors assurance regarding the understanding and reliance on controls that support the CSP clients' financial reporting processes and systems. SOC 1 reports are the replacement to Statement on Auditing Standards 70 reports, which are well-known and understood third-party examinations.	• Independent third-party assurance on which CSP clients and their auditors may rely • Recognized and commonly known and accepted assurance framework • Potential third-party assurance tool, but will most likely need to be supplemented with other assurance methods	• An SOC 1 examination is not designed as, nor intended to be, a marketing document; and therefore, cannot be shared with prospective clients • May be limited in scope to financial systems and controls. CSP clients must be very careful to evaluate the scope of the SOC 1 that may or may not be applicable to the CSP services provided. • Not specifically designed as a framework/certification model for cloud environments

Figure 5.1—Common Framework CSP Applicability for Third-party Certification/Examination *(cont.)*		
Certification/Framework—Description	**Benefits**	**Challenges**
AICPA/CICA Trust Services Examination—An independent, third-party examination under the AICPA attestation standards. CSPs can engage a CPA firm to perform a Trust Services examination to provide the CSP's clients assurance that the CSP's system controls meet one or more of the Trust Services principles and related criteria (security, privacy, availability, confidentiality and processing integrity). Effective in 2011, Trust Service reports can be issued as SOC 2 or SOC 3 reports under the SSAE 16 standard.	• Independent, third-party assurance on which CSP clients may rely • Examination can be specifically targeted at area(s) relevant to the CSP client • Trust Services examination may be shared with prospective clients • May be more broadly focused than financial controls, e.g., operational processes and controls • Recognized and commonly known and accepted standard	• Not specifically designed as a framework/certification model for cloud environments
BITS—Used by financial institutions to evaluate the IT controls their IT service providers have in place for security, privacy and business continuity. Financial institutions can provide a Shared Assessments SIG questionnaire and may also provide a Shared Assessments AUP report.	• Has defined and specific criteria across a broad range of control areas (e.g., privacy, security, continuity) • Recently established, but commonly known framework for financial services enterprises • Has recently completed a white paper mapping the BITS criteria to relevant "delta" risk for CSPs • AUP report can provide an independent, third-party assurance on which users may rely	• Specifically designed for and focused on financial services industries
ISO/IEC 27001/27002—Established by ISO. ISO 2700x standards provide a security framework and process accreditation relative to the standards process.	• Can provide an independent, third-party certification on which CSP clients may rely • Well-known published standards and evaluation criteria. ISO standards are more commonly used and accepted in Europe than in other areas of the world. • Cover most security risk points of cloud computing, but applicable controls are a subset of the entire ISO 2700x control spectrum	• Few enterprises are ISO 2700x-certified or understand the certification process

Figure 5.2—Common Framework CSP Applicability for Assurance Frameworks		
Certification/Framework—Description	**Benefits**	**Challenges**
COBIT 4.1—ISACA's comprehensive framework for the control and governance of business-driven IT-based projects and operations	• Provides a comprehensive framework to evaluate cloud environments through the entire ecosystem (due diligence through delivery management) • Offers mapping to other frameworks such as NIST SP 800-53, ISO 17799, ITIL, CMMI and PMBOK • Commonly understood and accepted framework • Mapped to cloud risk and controls by ISACA	• Not originally created for cloud-specific risk.
NIST SP 800-53—Contains the controls required to address cloud security	• Provides a broad risk and security framework to evaluate cloud environments • Commonly understood guidance, highly respected standard-setting body	• Not specifically focused on unique cloud risk and standards • Does not provide independent, third-party assurance
Cloud Security Matrix—This cloud security controls matrix is specifically designed to provide fundamental security principles to guide cloud vendors and assist prospective cloud clients in assessing overall security risks of a CSP.	• Provides a framework that is specifically focused and targeted at cloud security controls • Based on other industry-accepted security standards, regulations and controls frameworks, including controls from HIPAA, ISO/IEC 27001/27002, COBIT, PCI and NIST • Focused on cloud security and risks and not across the broad ecosystem of cloud management risks	• Not yet commonly understood or consistently accepted as a framework for cloud security, but quickly gaining momentum and awareness
ENISA Information Assurance Framework for Cloud Computing—Defines multiple risk points in the cloud, covering the various delivery and deployment models. It is a detailed discussion regarding IT cloud risk.	• Provides broader guidance that is specifically focused and targeted on cloud risks and controls • Limited to risks, but an IT auditor could readily translate specific risk points into control points, then into IT audit tests	• Not yet commonly understood or consistently accepted as a framework for cloud risk • Limited to cloud risk and not focused on controls or tests of controls • Does not provide independent, third-party assurance

Figure 5.2—Common Framework CSP Applicability for Assurance Frameworks *(cont.)*		
Certification/Framework—Description	**Benefits**	**Challenges**
FedRAMP—Provides a framework for A&A cloud computing services. FedRAMP is designed for US federal agency use, but can be used for joint authorizations and continuous security monitoring services for both government and commercial cloud computing systems.	• Specifically designed for cloud computing services • Common security risk model that provides a consistent baseline for cloud-based technologies that can be leveraged across the US federal government and commercial cloud services • Provides assurance through A&A	• Currently limited to deployment within government agencies, but gaining momentum in awareness and across commercial industries
Jericho Forum® Self-Assessment Scheme—Recently released. The Jericho Forum's Self-Assessment Scheme is a guideline for vendors to self-assess the security aspects of their cloud offering and for prospective cloud clients to include in their RFPs.	• Provides a security framework that is specifically focused and targeted on cloud vendors to self-assess their cloud offering	• Not yet commonly understood or accepted as a framework for cloud vendors • Focused on cloud vendors and self-assessment • Does not provide independent, third-party assurance

Most products and services purchased today carry safety certifications or comply with regulations from governments or industry-standards commissions. A cloud security certification would provide assurance to clients that the CSP offering provides adequate security controls around client data. Cloud security certifications undoubtedly will make clients' transitions to the cloud more palatable; however, a cloud security certification cannot be viewed as a "be-all, end-all." Just as in PCI compliance, certifications will be only a minimum threshold—a starting point.

CSPs will undoubtedly put great effort into obtaining a primary cloud security assurance certification. Perhaps industry-specific cloud security charters needed for certain markets will follow, be it PCI, BITS, HITRUST or other assessment packages. CSPs need to look at certification to upcoming finalized cloud security assurance standards as marketing tools—with certification comes greater market acceptance. Since the varied cloud security assurance programs typically attempt to cover the same or similar requirements, it may be that, once a CSP obtains one certification, others could readily fall into place.

CSPs that incorporate a standardized cloud assurance program will benefit from a reduction of client-requested operational CSP audits. CSPs can adopt a unified IT compliance approach to cover the multitude of requirements, provide a sound base for the various assurance frameworks and establish an effective compliance-monitoring program.

Unified IT Compliance Approach

Utilizing cloud computing services may introduce an enterprise to more regulatory compliance issues. Data may be stored or transported in different geographical regions that are subject to differing regulations. Since there could be a litany of compliance requirements, it may assist enterprises utilizing cloud services to adopt a unified IT compliance approach to more efficiently manage the compliance landscape.

The benefits of a unified compliance approach include:
- Reduced risk through a structured risk management approach
- Improved monitoring of compliance
- Improved security
- Rationalized compliance requirements and control assessment processes
- Reduced burden of compliance monitoring and testing

Key Elements of a Unified IT Compliance Program

The unified IT compliance approach includes the major components shown in **figure 5.3**.

Figure 5.3—Unified IT Compliance Components

Business function	Key Activities
Governance	• Provide executive oversight and visibility through ongoing status reporting based on key performance indicators (KPIs) and compliance activities.
Risk management	• Perform a periodic risk assessment. • Identify controls in a unified controls matrix to mitigate known risk. • Efficiently address applicable compliance requirements such as PCI, the US Sarbanes-Oxley Act, privacy/breach notifications, corporate policies and standards, and customer/business partner requirements. • Perform risk assessments of new projects and systems. • Periodically update the controls matrix to address changes/new risk.
Compliance	• Develop control testing/monitoring plans. • Perform control testing/monitoring procedures in a coordinated manner to reduce or eliminate duplication of efforts across the enterprise's compliance functions. • Monitor the status of risk mitigation activities for identified control gaps. • Provide support for external audit and certification activities to enable efficiencies.
Continuous improvement	• Identify and implement solutions to address aggregated control gaps. • Automate controls and monitoring activities where possible to drive efficiency.
Unified control processes	• Control activities should be executed by CSP personnel or other third parties; this includes in-house and outsourced activities.

There could be duplicity of assurance effort between the CSP and its clients, so it is important to coordinate activities to attain maximum leverage. For example, in the financial services industry, the BITS-Fiscal Operations Report and Application to Participate (FISAP) standards were formulated to produce a single consistent standard.

Assurance for Cloud Clients

Generally, there are two approaches a client may use to measure a CSP vendor:
1. Vendor management, including vendor risk assessment, vendor due diligence, vendor tiering based on the significance of the process outsourced, and contracting and SLAs as they apply to a CSP
2. Independent assurance by either the CSP's auditors or client personnel outside of vendor management (involves understanding the scope of services provided, obtaining and evaluating third-party assurance reports, evaluating residual risk, and determining whether an onsite visit to the service provider is required)

Assurance Through the Vendor Management Process

Users that outsource and intend to institute vendor governance should establish a vendor management office (VMO) or a specialized sourcing function. Effective vendor management programs include both a proactive (vendor governance) and reactive (vendor contract compliance review) strategy. Cloud computing requires continuous monitoring of compliance.

The key steps utilized as part of vendor management are:
1. Determine an opportunity assessment approach, and develop a business case for new business processes/IT functions to be sourced.
2. Select the process/components for a vendor-sourced delivery model.
3. Document at the as-is and to-be flows of the sourced process, including interfaces and hand-offs.
4. Develop a vendor short listing, conduct evaluations, carry out site visits, exercise due diligence, and make a final selection.
5. Engage in contract negotiations with selected vendor(s), and reach final acceptance, inclusive of legal, tax, security and regulatory factors and of a vendor(s) replacement/exit strategy. A response to the vendor risk assessment includes mechanisms to identify and evaluate vendor risk; based on these factors, select the contracts to evaluate further.
6. Exercise strategic vendor management based on governance requirements, audits (obtain independent assurance), risk and its mitigation, SLA trends, penalties or credits, etc. As part of strategic vendor management, enterprises with vendor management processes conduct vendor risk assessments and rank/tier vendors into different categories depending on the significance of the relationship and results of vendor due diligence efforts. Vendor risk assessment is based on a set of predefined risk categories, such as:
   – Nature and state of the relationship
   – Complexity of contract
   – Evidence of potential errors or manipulation
   – Taxation considerations
   – Strength of audit clause
7. Conduct day-to-day vendor management based on scope and change management, issue resolution and escalation, and communications. Use project management and earned value management (EVM) techniques to measure progress against goals.

8. Define agreed-on metrics for the vendors to measure and share.
9. Conduct periodic comprehensive reviews of vendors, covering all aspects of the relationship.

Traditional vendor due diligence may gain additional assurance by obtaining a third-party examination report (e.g., an SOC 1 audit report [previously Statement on Auditing Standards 70] or an ISO certificate). However, given the wide variety of potential uses for cloud computing, and its increasing complexity and diminishing transparency, an SOC 1 report or ISO certification may not be sufficient. The challenge remains that personnel assigned to perform vendor due diligence may not possess a comprehensive understanding of the risk involved in cloud computing and may end up accepting a certification that is irrelevant in meeting the vendor acceptance criteria. It is also possible that the CSP does not have the relevant certification; in certain cases, it may not be cost-effective for the CSP to obtain a specific certification to meet the needs of a single client or a small group of clients. From an assurance perspective, it is important to have a right-to-audit clause in such contracts.

In traditional vendor management, there is a lot of focus on fiscal and legal aspects related to vendors vs. a focus on emerging risk related to the business, e.g., reputational risk. The vendor manages security based on its risk profile and not necessarily on the client's risk model.

One of the key reasons that companies outsource is to provide better and faster service. Enterprises utilizing cloud computing migrate to an IT solution that responds to new business needs in real time by removing or streamlining the CSP clients' silos. Because SLAs provide the basis against which CSP clients manage performance in the outsourcing process, the SLAs must be specific and measurable, both of which present challenges in cloud computing as compared to traditional outsourcing. While there is limited precedent in the cloud computing space to provide sufficient benchmarks for SLAs, as cloud computing matures, there will be a need for benchmark data; independent, third-party intermediaries could have a role to play in this area.

As it pertains to measurability, experience with traditional IT hosting services has indicated that monitoring the quality of service (QoS) and challenging the SLA are the responsibilities of the cloud user. In addition to application processing time, network lag in external cloud computing arrangements is a factor in computing total processing time. To the end user, what matters is the total processing time, which cannot exceed certain thresholds.

A CSP client may not have a ready set of tools or human resources to track the QoS in a complex cloud computing environment. Some CSPs have one set of a standard contract, and clients must "take it or leave it." Unless the CSP client offers many potential business opportunities, the CSP may not be willing to negotiate the standard contractual terms and conditions. This can be challenging for large

enterprises because their needs are broader and require tighter clauses to ensure that the liability aspects are shared between the CSP and the enterprise. Furthermore, the very attraction of cloud's pay-as-you-go model is diluted if the cloud user needs to provide a large upfront commitment. In the cloud computing space, there is a need for well-defined SLAs related to various aspects of availability, response time, scalability and cost savings. Cloud computing is dynamic, and this dynamic nature must be accounted for in any system that tries to enforce SLAs. Further, due to a lack of standardization, it can be difficult to compare SLAs across multiple CSPs.

Vendor lock-in can be another problem when contracting with CSPs. With SaaS, the data reside with the CSP, so it is important to understand the format in which the data will be available if the CSP client decides to end the relationship. With PaaS, due to the lack of clarity, it is important to understand who owns the platform, process and data and to document the hand-offs as part of the contracting process. With IaaS, it is important to understand the virtual machine technology and whether the CSP has done significant customization to the virtual machine that would hinder it from utilizing an alternative CSP.

Assurance Provided by CSP Clients' Independent Auditors/Assessors

Third-party service providers are inundated with assurance requests; therefore, it is becoming increasingly common for CSPs to elect to undergo an audit/review/assessment from an independent auditor/assessor and share the report/certification. While C&A standards are evolving, the most commonly utilized reports are the SOC 1, ISO/IEC 27001, ISAE 3402 and AICPA/CICA Trust Services (SOC 2 and SOC 3) reports. Regardless of the form of report, users must determine the impact the CSP can have on them and evaluate the scope of the independent examination, including the completeness and adequacy of testing performed and results.

Appendix A. IT Control Objectives for Cloud Computing

Using the Cross-Reference for COBIT

COBIT was developed as a generic control framework. This document was designed to adapt COBIT to the cloud environment and identify those control objectives that are relevant to a cloud-based production environment.

All COBIT control objectives identified have some applicability to the cloud; however, some are higher priority than others.

The following provides guidance to using the document:

1. For each cloud delivery model (IaaS, PaaS and SaaS) three icons, a square, circle and triangle depict the three cloud deployment models: public cloud, private cloud and hybrid cloud, respectively.
2. Private cloud definition: For the purpose of this document, a private cloud is a cloud hosted by a third-party cloud service provider, exclusively for a single customer. The private cloud model that is hosted in the enterprise's own data center is not regarded as a private cloud for this purpose, since it is essentially a conventional in-house data center with a more flexible delivery approach.
3. In certain control objectives, a comment expounds briefly on the control objective in a cloud computing environment. In other instances, a comment explains why the control objective was not applicable in a cloud environment.
4. The COBIT control objective was omitted from the cross-reference where the control objective is generic to all IT (cloud and non-cloud), resulting in all corresponding icons being blank, and no comment is required.
5. The corresponding icons are solid where the COBIT control objective applies to one, two or three of the cloud service models.
6. PaaS is normally implemented as a development environment supporting software development activities, and generally includes hardware, compilers and other development tools. This document recognizes that for most organizations, COBIT controls do not apply to the PaaS environment. A major exclusion to this is the software development industry, where application development is the primary function and needs to be considered as an operational activity.

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Plan and Organise (PO)			
PO1 Define a Strategic IT Plan IT strategic planning is required to manage and direct all IT resources in line with the business strategy and priorities. The IT function and business stakeholders are responsible for ensuring that optimal value is realised from project and service portfolios. The strategic plan improves key stakeholders' understanding of IT opportunities and limitations, assesses current performance, identifies capacity and human resources requirements and clarifies the level of investment required. The business strategy and priorities are to be reflected in portfolios and executed by the IT tactical plan(s), which specifies concise objectives, action plans and tasks that are understood and accepted by both business and IT.			
PO1.1 IT Value Management Work with the business to ensure that the enterprise portfolio of IT-enabled investments contains programmes that have solid business cases. Recognise that there are mandatory, sustaining and discretionary investments that differ in complexity and degree of freedom in allocating funds. IT processes should provide effective and efficient delivery of the IT components of programmes and early warning of any deviations from plan, including cost, schedule or functionality, that might impact the expected outcomes of the programmes. IT services should be executed against equitable and enforceable SLAs. Accountability for achieving the benefits and controlling the costs should be clearly assigned and monitored. Establish fair, transparent, repeatable and comparable evaluation of business cases, including financial worth, the risk of not delivering a capability and the risk of not realising the expected benefits.	■ ● ▲	■ ● ▲	■ ● ▲
PO1.2 Business-IT Alignment Establish processes of bi-directional education and reciprocal involvement in strategic planning to achieve business and IT alignment and integration. Mediate between business and IT imperatives so priorities can be mutually agreed. ***Comment:*** *Identify issues where the business has contracted for CSP services without the knowledge of IT and vice versa.*	□ ○ △	□ ○ △	□ ○ △
PO1.3 Assessment of Current Capability and Performance Assess the current capability and performance of solution and service delivery to establish a baseline against which future requirements can be compared. Define performance in terms of IT's contribution to business objectives, functionality, stability, complexity, costs, strengths and weaknesses. ***Comment:*** *The current capability and performance can be used to evaluate the decision to utilise a cloud solution and the requirements of the CSP to satisfy the customer's requirements.*	■ ● ▲	■ ● ▲	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Plan and Organise (PO) ***(cont.)***			
PO1.4 IT Strategic Plan Create a strategic plan that defines, in co-operation with relevant stakeholders, how IT goals will contribute to the enterprise's strategic objectives and related costs and risks. It should include how IT will support IT-enabled investment programmes, IT services and IT assets. IT should define how the objectives will be met, the measurements to be used and the procedures to obtain formal sign-off from the stakeholders. The IT strategic plan should cover investment/operational budget, funding sources, sourcing strategy, acquisition strategy, and legal and regulatory requirements. The strategic plan should be sufficiently detailed to allow for the definition of tactical IT plans. ***Comment:*** *Cloud may be a component of the strategic plan and could affect budgetary planning.*	□ ○ △	□ ○ △	□ ○ △
PO1.5 IT Tactical Plans Create a portfolio of tactical IT plans that are derived from the IT strategic plan. The tactical plans should address IT-enabled programme investments, IT services and IT assets. The tactical plans should describe required IT initiatives, resource requirements, and how the use of resources and achievement of benefits will be monitored and managed. The tactical plans should be sufficiently detailed to allow the definition of project plans. Actively manage the set of tactical IT plans and initiatives through analysis of project and service portfolios.	■ ● ▲	■ ● ▲	■ ● ▲
PO1.6 Portfolio Management Actively manage with the business the portfolio of IT-enabled investment programmes required to achieve specific strategic business objectives by identifying, defining, evaluating, prioritising, selecting, initiating, managing and controlling programmes. This should include clarifying desired business outcomes, ensuring that programme objectives support achievement of the outcomes, understanding the full scope of effort required to achieve the outcomes, assigning clear accountability with supporting measures, defining projects within the programme, allocating resources and funding, delegating authority, and commissioning required projects at programme launch.	■ ● ▲	■ ● ▲	■ ● ▲
PO2 Define the Information Architecture The information systems function creates and regularly updates a business information model and defines the appropriate systems to optimise the use of this information. This encompasses the development of a corporate data dictionary with the organisation's data syntax rules, data classification scheme and security levels. This process improves the quality of management decision making by making sure that reliable and secure information is provided, and it enables rationalising information systems resources to appropriately match business strategies. This IT process is also needed to increase accountability for the integrity and security of data and to enhance the effectiveness and control of sharing information across applications and entities.			

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Plan and Organise (PO) *(cont.)*			
PO2.1 Enterprise Information Architecture Model Establish and maintain an enterprise information model to enable applications development and decision-supporting activities, consistent with IT plans as described in PO1. The model should facilitate the optimal creation, use and sharing of information by the business in a way that maintains integrity and is flexible, functional, cost-effective, timely, secure and resilient to failure. ***Comment:*** *SaaS applications that have been customised may require consideration.*	□ ○ △	□ ○ △	□ ○ △
PO2.2 Enterprise Data Dictionary and Data Syntax Rules Maintain an enterprise data dictionary that incorporates the organisation's data syntax rules. This dictionary should enable the sharing of data elements amongst applications and systems, promote a common understanding of data amongst IT and business users, and prevent incompatible data elements from being created. ***Comment:*** *This would apply to customisable processes within SaaS and with systems developed in PaaS.*	□ ○ △	■ ● ▲	■ ● ▲
PO2.3 Data Classification Scheme Establish a classification scheme that applies throughout the enterprise, based on the criticality and sensitivity (e.g., public, confidential, top secret) of enterprise data. This scheme should include details about data ownership; definition of appropriate security levels and protection controls; and a brief description of data retention and destruction requirements, criticality and sensitivity. It should be used as the basis for applying controls such as access controls, archiving or encryption.	■ ● ▲	□ ○ △	■ ● ▲
PO2.4 Integrity Management Define and implement procedures to ensure the integrity and consistency of all data stored in electronic form, such as databases, data warehouses and data archives. ***Comment:*** *Applies to SaaS, but the practicality of applying this control objective is questionable since, in general, the customer does not have access to this level of process detail.*	□ ○ △	□ ○ △	□ ○ △
PO3 Determine Technological Direction The information services function determines the technology direction to support the business. This requires the creation of a technological infrastructure plan and an architecture board that sets and manages clear and realistic expectations of what technology can offer in terms of products, services and delivery mechanisms. The plan is regularly updated and encompasses aspects such as systems architecture, technological direction, acquisition plans, standards, migration strategies and contingency. This enables timely responses to changes in the competitive environment, economies of scale for information systems staffing and investments, as well as improved interoperability of platforms and applications.			

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Plan and Organise (PO) ***(cont.)***			
PO3.1 Technological Direction Planning Analyse existing and emerging technologies, and plan which technological direction is appropriate to realise the IT strategy and the business systems architecture. Also identify in the plan which technologies have the potential to create business opportunities. The plan should address systems architecture, technological direction, migration strategies and contingency aspects of infrastructure components.	■ ● ▲	■ ● ▲	■ ● ▲
PO3.2 Technology Infrastructure Plan Create and maintain a technology infrastructure plan that is in accordance with the IT strategic and tactical plans. The plan should be based on the technological direction and include contingency arrangements and direction for acquisition of technology resources. It should consider changes in the competitive environment, economies of scale for information systems staffing and investments, and improved interoperability of platforms and applications. ***Comment:*** *The infrastructure plan will be limited to CSP capabilities vs. customer needs and customer interfaces to the CSP provided technology (IaaS) or software (SaaS).*	■ ● ▲	■ ● ▲	■ ● ▲
PO3.3 Monitor Future Trends and Regulations Establish a process to monitor the business sector, industry, technology, infrastructure, legal and regulatory environment trends. Incorporate the consequences of these trends into the development of the IT technology infrastructure plan. ***Comment:*** *Outside the scope of cloud computing, but is required for any strategic planning*	□ ○ △	□ ○ △	□ ○ △
PO4 Define the IT Processes, Organisation and Relationships An IT organisation is defined by considering requirements for staff, skills, functions, accountability, authority, roles and responsibilities, and supervision. This organisation is embedded into an IT process framework that ensures transparency and control as well as the involvement of senior executives and business management. A strategy committee ensures board oversight of IT, and one or more steering committees in which business and IT participate determine the prioritisation of IT resources in line with business needs. Processes, administrative policies and procedures are in place for all functions, with specific attention to control, quality assurance, risk management, information security, data and systems ownership, and segregation of duties. To ensure timely support of business requirements, IT is to be involved in relevant decision processes.			
PO4.2 IT Strategy Committee Establish an IT strategy committee at the board level. This committee should ensure that IT governance, as part of enterprise governance, is adequately addressed; advise on strategic direction; and review major investments on behalf of the full board. ***Comment:*** *Part of the organisation's approach to IT, this is not exclusively a cloud computing issue.*	□ ○ △	□ ○ △	□ ○ △

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Plan and Organise (PO) *(cont.)*			
PO4.3 IT Steering Committee Establish an IT steering committee (or equivalent) composed of executive, business and IT management to: • Determine prioritisation of IT-enabled investment programmes in line with the enterprise's business strategy and priorities • Track status of projects and resolve resource conflict • Monitor service levels and service improvements ***Comment:*** *Part of the organisation's approach to IT, this is not exclusively a cloud computing issue.*	□ ○ △	□ ○ △	□ ○ △
PO4.5 IT Organisational Structure Establish an internal and external IT organisational structure that reflects business needs. In addition, put a process in place for periodically reviewing the IT organisational structure to adjust staffing requirements and sourcing strategies to meet expected business objectives and changing circumstances. ***Comment:*** *The organisational structure will transition from an operational to a management-focused group of processes.*	■ ● ▲	□ ○ △	■ ● ▲
PO4.6 Establishment of Roles and Responsibilities Establish and communicate roles and responsibilities for IT personnel and end users that delineate between IT personnel and end-user authority, responsibilities and accountability for meeting the organisation's needs. ***Comment:*** *The organisational structure will transition from an operational to a management-focused group of processes.*	■ ● ▲	□ ○ △	■ ● ▲
PO4.7 Responsibility for IT Quality Assurance Assign responsibility for the performance of the quality assurance (QA) function and provide the QA group with appropriate QA systems, controls and communications expertise. Ensure that the organisational placement and the responsibilities and size of the QA group satisfy the requirements of the organisation. ***Comment:*** *QA, whether for cloud or non-cloud, remains the same.*	□ ○ △	□ ○ △	□ ○ △
PO4.9 Data and System Ownership Provide the business with procedures and tools, enabling it to address its responsibilities for ownership of data and information systems. Owners should make decisions about classifying information and systems and protecting them in line with this classification.	□ ○ △	□ ○ △	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Plan and Organise (PO) *(cont.)*			
PO4.10 Supervision Implement adequate supervisory practices in the IT function to ensure that roles and responsibilities are properly exercised, to assess whether all personnel have sufficient authority and resources to execute their roles and responsibilities, and to generally review key performance indicators. ***Comment:*** *Not cloud computing specific.*	□ ○ △	□ ○ △	□ ○ △
PO4.11 Segregation of Duties Implement a division of roles and responsibilities that reduces the possibility for a single individual to compromise a critical process. Make sure that personnel are performing only authorised duties relevant to their respective jobs and positions.	■ ● ▲	■ ● ▲	■ ● ▲
PO4.12 IT Staffing Evaluate staffing requirements on a regular basis or upon major changes to the business, operational or IT environments to ensure that the IT function has sufficient resources to adequately and appropriately support the business goals and objectives. ***Comment:*** *IT staffing requirements will change as the operational staff move to a more strategic, business focused and monitoring role in a production cloud environment.*	■ ● ▲	□ ○ △	■ ● ▲
PO4.13 Key IT Personnel Define and identify key IT personnel (e.g., replacements/backup personnel), and minimise reliance on a single individual performing a critical job function. ***Comment:*** *See PO4.12*	■ ● ▲	□ ○ △	■ ● ▲
PO4.14 Contracted Staff Policies and Procedures Ensure that consultants and contract personnel who support the IT function know and comply with the organisation's policies for the protection of the organisation's information assets such that they meet agreed-upon contractual requirements. ***Comment:*** *No difference to any outsourcing arrangement.*	■ ● ▲	■ ● ▲	■ ● ▲
PO4.15 Relationships Establish and maintain an optimal co-ordination, communication and liaison structure between the IT function and various other interests inside and outside the IT function, such as the board, executives, business units, individual users, suppliers, security officers, risk managers, the corporate compliance group, outsourcers and offsite management. ***Comment:*** *No difference to any outsourcing arrangement.*	■ ● ▲	■ ● ▲	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Plan and Organise (PO) *(cont.)*			
PO5 Manage the IT Investment A framework is established and maintained to manage IT-enabled investment programmes and that encompasses cost, benefits, prioritisation within budget, a formal budgeting process and management against the budget. Stakeholders are consulted to identify and control the total costs and benefits within the context of the IT strategic and tactical plans, and initiate corrective action where needed. The process fosters partnership between IT and business stakeholders; enables the effective and efficient use of IT resources; and provides transparency and accountability into the total cost of ownership, the realisation of business benefits and the ROI of IT-enabled investments.			
PO5.1 Financial Management Framework Establish and maintain a financial framework to manage the investment and cost of IT assets and services through portfolios of IT-enabled investments, business cases and IT budgets. ***Comment:*** *Standard operating procedures as with any other IT investment*	□ ○ △	□ ○ △	□ ○ △
PO5.3 IT Budgeting Establish and implement practices to prepare a budget reflecting the priorities established by the enterprise's portfolio of IT-enabled investment programmes, and including the ongoing costs of operating and maintaining the current infrastructure. The practices should support development of an overall IT budget as well as development of budgets for individual programmes, with specific emphasis on the IT components of those programmes. The practices should allow for ongoing review, refinement and approval of the overall budget and the budgets for individual programmes. ***Comment:*** *Standard operating procedures as with any other IT investment*	□ ○ △	□ ○ △	□ ○ △
PO5.4 Cost Management Implement a cost management process comparing actual costs to budgets. Costs should be monitored and reported. Where there are deviations, these should be identified in a timely manner and the impact of those deviations on programmes should be assessed. Together with the business sponsor of those programmes, appropriate remedial action should be taken and, if necessary, the programme business case should be updated. ***Comment:*** *Standard operating procedures as with any other IT investment*	□ ○ △	□ ○ △	□ ○ △

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Plan and Organise (PO) *(cont.)*			
PO5.5 Benefit Management Implement a process to monitor the benefits from providing and maintaining appropriate IT capabilities. IT's contribution to the business, either as a component of IT-enabled investment programmes or as part of regular operational support, should be identified and documented in a business case, agreed to, monitored and reported. Reports should be reviewed and, where there are opportunities to improve IT's contribution, appropriate actions should be defined and taken. Where changes in IT's contribution impact the programme, or where changes to other related projects impact the programme, the programme business case should be updated. ***Comment:*** *Standard operating procedures as with any other IT investment*	□ ○ △	□ ○ △	□ ○ △
PO6 Communicate Management Aims and Direction Management develops an enterprise IT control framework and defines and communicates policies. An ongoing communication programme is implemented to articulate the mission, service objectives, policies and procedures, etc., approved and supported by management. The communication supports achievement of IT objectives and ensures awareness and understanding of business and IT risks, objectives and direction. The process ensures compliance with relevant laws and regulations.			
PO6.2 Enterprise IT Risk and Control Framework Develop and maintain a framework that defines the enterprise's overall approach to IT risk and control and that aligns with the IT policy and control environment and the enterprise risk and control framework. ***Comment:*** *ERM must be updated to reflect specific risks introduced through cloud computing.*	■ ● ▲	■ ● ▲	■ ● ▲
PO6.3 IT Policies Management Develop and maintain a set of policies to support IT strategy. These policies should include policy intent; roles and responsibilities; exception process; compliance approach; and references to procedures, standards and guidelines. Their relevance should be confirmed and approved regularly. ***Comment:*** *Policies directly affecting cloud should be aligned with the CSP contract and the SLAs.*	■ ● ▲	■ ● ▲	■ ● ▲
PO7 Manage IT Human Resources A competent workforce is acquired and maintained for the creation and delivery of IT services to the business. This is achieved by following defined and agreed-upon practices supporting recruiting, training, evaluating performance, promoting and terminating. This process is critical, as people are important assets, and governance and the internal control environment are heavily dependent on the motivation and competence of personnel.			

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Plan and Organise (PO) ***(cont.)***			
PO7.1 Personnel Recruitment and Retention Maintain IT personnel recruitment processes in line with the overall organisation's personnel policies and procedures (e.g., hiring, positive work environment, orienting). Implement processes to ensure that the organisation has an appropriately deployed IT workforce with the skills necessary to achieve organisational goals. ***Comment:*** *Personnel needs will change. IaaS and SaaS platforms will require a focus on personnel who can manage the CSP relationship. Many IT tasks will move to the business units.*	■ ● ▲	■ ● ▲	■ ● ▲
PO7.2 Personnel Competencies Regularly verify that personnel have the competencies to fulfil their roles on the basis of their education, training and/or experience. Define core IT competency requirements and verify that they are being maintained, using qualification and certification programmes where appropriate. ***Comment:*** *IT competencies change as described in PO7.1.*	■ ● ▲	■ ● ▲	■ ● ▲
PO7.3 Staffing of Roles Define, monitor and supervise roles, responsibilities and compensation frameworks for personnel, including the requirement to adhere to management policies and procedures, the code of ethics, and professional practices. The level of supervision should be in line with the sensitivity of the position and extent of responsibilities assigned. ***Comment:*** *See PO7.1*	■ ● ▲	■ ● ▲	■ ● ▲
PO7.4 Personnel Training Provide IT employees with appropriate orientation when hired and ongoing training to maintain their knowledge, skills, abilities, internal controls and security awareness at the level required to achieve organisational goals. ***Comment:*** *Objective remains in place, however, some responsible organisations will move into the business.*	■ ● ▲	■ ● ▲	■ ● ▲
PO7.5 Dependence Upon Individuals Minimise the exposure to critical dependency on key individuals through knowledge capture (documentation), knowledge sharing, succession planning and staff backup. ***Comment:*** *Non-cloud specific process, but required. The transfer of responsibility to the business units may result in single points of failure.*	■ ● ▲	□ ○ △	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Plan and Organise (PO) *(cont.)*			
PO7.6 Personnel Clearance Procedures Include background checks in the IT recruitment process. The extent and frequency of periodic reviews of these checks should depend on the sensitivity and/or criticality of the function and should be applied for employees, contractors and vendors. ***Comment:*** *This is not a cloud specific process, but still required. Customers will have no control over CSP employees.*	□ ○ △	□ ○ △	□ ○ △
PO7.7 Employee Job Performance Evaluation Require a timely evaluation to be performed on a regular basis against individual objectives derived from the organisation's goals, established standards and specific job responsibilities. Employees should receive coaching on performance and conduct whenever appropriate. ***Comment:*** *Non-cloud specific process, but required. Customers will have no control over CSP employees.*	□ ○ △	□ ○ △	□ ○ △
PO7.8 Job Change and Termination Take expedient actions regarding job changes, especially job terminations. Knowledge transfer should be arranged, responsibilities reassigned and access rights removed such that risks are minimised and continuity of the function is guaranteed. ***Comment:*** *Non-cloud specific process, but required. Customers will have no control over CSP employees.*	□ ○ △	□ ○ △	□ ○ △
PO8 Manage Quality A quality management system (QMS) is developed and maintained that includes proven development and acquisition processes and standards. This is enabled by planning, implementing and maintaining the QMS by providing clear quality requirements, procedures and policies. Quality requirements are stated and communicated in quantifiable and achievable indicators. Continuous improvement is achieved by ongoing monitoring, analysis and acting upon deviations, and communicating results to stakeholders. Quality management is essential to ensure that IT is delivering value to the business, continuous improvement and transparency for stakeholders.			
PO8.3 Development and Acquisition Standards Adopt and maintain standards for all development and acquisition that follow the life cycle of the ultimate deliverable, and include sign-off at key milestones based on agreed-upon sign-off criteria. Consider software coding standards; naming conventions; file formats; schema and data dictionary design standards; user interface standards; interoperability; system performance efficiency; scalability; standards for development and testing; validation against requirements; test plans; and unit, regression and integration testing. ***Comment:*** *The management focus must be on approval of acquisitions and support for business cases and cost/benefits.*	□ ○ △	■ ● ▲	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Plan and Organise (PO) *(cont.)*			
PO9 Assess and Manage IT Risks A risk management framework is created and maintained. The framework documents a common and agreed-upon level of IT risks, mitigation strategies and residual risks. Any potential impact on the goals of the organisation caused by an unplanned event is identified, analysed and assessed. Risk mitigation strategies are adopted to minimise residual risk to an accepted level. The result of the assessment is understandable to the stakeholders and expressed in financial terms, to enable stakeholders to align risk to an acceptable level of tolerance.			
PO9.1 IT Risk Management Framework Establish an IT risk management framework that is aligned to the organisation's (enterprise's) risk management framework. ***Comment:*** *Cloud-specific risks must be included in the framework.*	□ ○ △	□ ○ △	□ ○ △
PO9.2 Establishment of Risk Context Establish the context in which the risk assessment framework is applied to ensure appropriate outcomes. This should include determining the internal and external context of each risk assessment, the goal of the assessment, and the criteria against which risks are evaluated. ***Comment:*** *See PO9.1*	□ ○ △	□ ○ △	□ ○ △
PO9.3 Event Identification Identify events (an important realistic threat that exploits a significant applicable vulnerability) with a potential negative impact on the goals or operations of the enterprise, including business, regulatory, legal, technology, trading partner, human resources and operational aspects. Determine the nature of the impact and maintain this information. Record and maintain relevant risks in a risk registry. ***Comment:*** *Address new risks that apply only to cloud.*	■ ● ▲	■ ● ▲	■ ● ▲
PO9.4 Risk Assessment Assess on a recurrent basis the likelihood and impact of all identified risks, using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk should be determined individually, by category and on a portfolio basis. ***Comment:*** *See PO9.3*	■ ● ▲	■ ● ▲	■ ● ▲
PO9.5 Risk Response Develop and maintain a risk response process designed to ensure that cost-effective controls mitigate exposure to risks on a continuing basis. The risk response process should identify risk strategies such as avoidance, reduction, sharing or acceptance; determine associated responsibilities; and consider risk tolerance levels. ***Comment:*** *See PO9.3*	■ ● ▲	■ ● ▲	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Plan and Organise (PO) ***(cont.)***			
PO10 Manage Projects A programme and project management framework for the management of all IT projects is established. The framework ensures the correct prioritisation and co-ordination of all projects. The framework includes a master plan, assignment of resources, definition of deliverables, approval by users, a phased approach to delivery, QA, a formal test plan, and testing and post-implementation review after installation to ensure project risk management and value delivery to the business. This approach reduces the risk of unexpected costs and project cancellations, improves communications to and involvement of business and end users, ensures the value and quality of project deliverables, and maximises their contribution to IT-enabled investment programmes.			
PO10.1 Program Management Framework Maintain the programme of projects, related to the portfolio of IT-enabled investment programmes, by identifying, defining, evaluating, prioritising, selecting, initiating, managing and controlling projects. Ensure that the projects support the programme's objectives. Co-ordinate the activities and interdependencies of multiple projects, manage the contribution of all the projects within the programme to expected outcomes, and resolve resource requirements and conflicts.	□ ○ △	■ ● ▲	■ ● ▲
PO10.2 Project Management Framework Establish and maintain a project management framework that defines the scope and boundaries of managing projects, as well as the method to be adopted and applied to each project undertaken. The framework and supporting method should be integrated with the programme management processes. ***Comment:*** *IaaS and SaaS would relate to the conversion; PaaS would be ongoing for each project.*	■ ● ▲	■ ● ▲	■ ● ▲
PO10.3 Project Management Approach Establish a project management approach commensurate with the size, complexity and regulatory requirements of each project. The project governance structure can include the roles, responsibilities and accountabilities of the programme sponsor, project sponsors, steering committee, project office and project manager, and the mechanisms through which they can meet those responsibilities (such as reporting and stage reviews). Make sure all IT projects have sponsors with sufficient authority to own the execution of the project within the overall strategic programme. ***Comment:*** *Iaas and SaaS would relate to the conversion; PaaS would be ongoing for each project.*	■ ● ▲	■ ● ▲	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Plan and Organise (PO) ***(cont.)***			
PO10.5 Project Scope Statement Define and document the nature and scope of the project to confirm and develop amongst stakeholders a common understanding of project scope and how it relates to other projects within the overall IT-enabled investment programme. The definition should be formally approved by the programme and project sponsors before project initiation.	■ ● ▲	■ ● ▲	■ ● ▲
PO10.6 Project Phase Initiation Approve the initiation of each major project phase and communicate it to all stakeholders. Base the approval of the initial phase on programme governance decisions. Approval of subsequent phases should be based on review and acceptance of the deliverables of the previous phase, and approval of an updated business case at the next major review of the programme. In the event of overlapping project phases, an approval point should be established by programme and project sponsors to authorise project progression.	■ ● ▲	■ ● ▲	■ ● ▲
PO10.7 Integrated Project Plan Establish a formal, approved integrated project plan (covering business and information systems resources) to guide project execution and control throughout the life of the project. The activities and interdependencies of multiple projects within a programme should be understood and documented. The project plan should be maintained throughout the life of the project. The project plan, and changes to it, should be approved in line with the programme and project governance framework.	■ ● ▲	■ ● ▲	■ ● ▲
PO10.8 Project Resources Define the responsibilities, relationships, authorities and performance criteria of project team members, and specify the basis for acquiring and assigning competent staff members and/or contractors to the project. The procurement of products and services required for each project should be planned and managed to achieve project objectives using the organisation's procurement practices.	■ ● ▲	■ ● ▲	■ ● ▲
PO10.9 Project Risk Management Eliminate or minimise specific risks associated with individual projects through a systematic process of planning, identifying, analysing, responding to, monitoring and controlling the areas or events that have the potential to cause unwanted change. Risks faced by the project management process and the project deliverable should be established and centrally recorded.	■ ● ▲	■ ● ▲	■ ● ▲
PO10.10 Project Quality Plan Prepare a quality management plan that describes the project quality system and how it will be implemented. The plan should be formally reviewed and agreed to by all parties concerned and then incorporated into the integrated project plan.	■ ● ▲	■ ● ▲	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Plan and Organise (PO) *(cont.)*			
PO10.11 Project Change Control Establish a change control system for each project, so all changes to the project baseline (e.g., cost, schedule, scope, quality) are appropriately reviewed, approved and incorporated into the integrated project plan in line with the programme and project governance framework.	■ ● ▲	■ ● ▲	■ ● ▲
PO10.12 Project Planning of Assurance Methods Identify assurance tasks required to support the accreditation of new or modified systems during project planning, and include them in the integrated project plan. The tasks should provide assurance that internal controls and security features meet the defined requirements.	■ ● ▲	■ ● ▲	■ ● ▲
PO10.13 Project Performance Measurement, Reporting and Monitoring Measure project performance against key project performance scope, schedule, quality, cost and risk criteria. Identify any deviations from the plan. Assess the impact of deviations on the project and overall programme, and report results to key stakeholders. Recommend, implement and monitor remedial action, when required, in line with the programme and project governance framework.	■ ● ▲	■ ● ▲	■ ● ▲
PO10.14 Project Closure Require that, at the end of each project, stakeholders ascertain whether the project delivered the planned results and benefits. Identify and communicate any outstanding activities required to achieve the planned results of the project and the benefits of the programme, and identify and document lessons learned for use on future projects and programmes.	■ ● ▲	■ ● ▲	■ ● ▲
COBIT Domain: Acquire and Implement (AI)			
AI1 Identify Automated Solutions The need for a new application or function requires analysis before acquisition or creation to ensure that business requirements are satisfied in an effective and efficient approach. This process covers the definition of the needs, consideration of alternative sources, review of technological and economic feasibility, execution of a risk analysis and cost-benefit analysis, and conclusion of a final decision to 'make' or 'buy'. All these steps enable organisations to minimise the cost to acquire and implement solutions whilst ensuring that they enable the business to achieve its objectives.			
AI1.1 Definition and Maintenance of Business Functional and Technical Requirements Identify, prioritise, specify and agree on business functional and technical requirements covering the full scope of all initiatives required to achieve the expected outcomes of the IT-enabled investment programme. ***Comment:*** *This is not a cloud specific step. However, it should be required prior to considering a cloud computing solution.*	■ ● ▲	■ ● ▲	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Acquire and Implement (AI) *(cont.)*			
AI1.2 Risk Analysis Report Identify, document and analyse risks associated with the business requirements and solution design as part of the organisation's process for the development of requirements. ***Comment:*** *This would be required for all projects. Cloud computing poses new risks requiring consideration.*	■ ● ▲	■ ● ▲	■ ● ▲
AI1.3 Feasibility Study and Formulation of Alternative Courses of Action Develop a feasibility study that examines the possibility of implementing the requirements. Business management, supported by the IT function, should assess the feasibility and alternative courses of action and make a recommendation to the business sponsor. ***Comment:*** *This is a standard step in all feasibility studies. Cloud computing is one alternative, with its own set of risks and rewards.*	■ ● ▲	■ ● ▲	■ ● ▲
AI1.4 Requirements and Feasibility Decision and Approval Verify that the process requires the business sponsor to approve and sign off on business functional and technical requirements and feasibility study reports at predetermined key stages. The business sponsor should make the final decision with respect to the choice of solution and acquisition approach. ***Comment:*** *IaaS and PaaS requires IT involvement, a process with which most IT organisations are familiar. SaaS decisions are often made outside the IT organisation. Focus should be on the business unit's evaluation of the proposal and alternative solutions.*	■ ● ▲	■ ● ▲	■ ● ▲
AI2 Acquire and Maintain Application Software Applications are made available in line with business requirements. This process covers the design of the applications, the proper inclusion of application controls and security requirements, and the development and configuration in line with standards. This allows organisations to properly support business operations with the correct automated applications.			

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Acquire and Implement (AI) ***(cont.)***			
AI2.1 High-level Design Translate business requirements into a high-level design specification for software acquisition, taking into account the organisation's technological direction and information architecture. Have the design specifications approved by management to ensure that the high-level design responds to the requirements. Reassess when significant technical or logical discrepancies occur during development or maintenance. ***Comment:*** *IaaS high-level design addresses the infrastructure requirements and whether the CSP can provide the technology and configurations necessary to host the applications. PaaS high-level design is the same as an internally developed design. SaaS design is limited, unless customisation is planned. However, entity interfaces and other internal customisations may be required.*	■ ● ▲	■ ● ▲	■ ● ▲
AI2.2 Detailed Design Prepare detailed design and technical software application requirements. Define the criteria for acceptance of the requirements. Have the requirements approved to ensure that they correspond to the high-level design. Perform reassessment when significant technical or logical discrepancies occur during development or maintenance. ***Comment:*** *Same as AI2.1, but focusing on detail design.*	■ ● ▲	■ ● ▲	■ ● ▲
AI2.3 Application Control and Auditability Implement business controls, where appropriate, into automated application controls such that processing is accurate, complete, timely, authorised and auditable. ***Comment:*** *IaaS will address operational controls, PaaS will address functional processes and automated controls, and SaaS will address the user interfaces with the CSP's application.*	■ ● ▲	■ ● ▲	■ ● ▲
AI2.4 Application Security and Availability Address application security and availability requirements in response to identified risks and in line with the organisation's data classification, information architecture, information security architecture and risk tolerance. ***Comment:*** *The scope is the same as AI2.3, but the focus is on security and availability.*	■ ● ▲	■ ● ▲	■ ● ▲
AI2.5 Configuration and Implementation of Acquired Application Software Configure and implement acquired application software to meet business objectives. ***Comment:*** *Since the software is 'effectively leased', standard configuration objectives would be consistent with any acquired software.*	□ ○ △	□ ○ △	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Acquire and Implement (AI) *(cont.)*			
AI2.6 Major Upgrades to Existing Systems In the event of major changes to existing systems that result in significant change in current designs and/or functionality, follow a similar development process as that used for the development of new systems. ***Comment:*** *Ensure that the CSP provides adequate lead time and details of changes prior to deployment.*	■ ● ▲	■ ● ▲	■ ● ▲
AI2.7 Development of Application Software Ensure that automated functionality is developed in accordance with design specifications, development and documentation standards, QA requirements, and approval standards. Ensure that all legal and contractual aspects are identified and addressed for application software developed by third parties. ***Comment:*** *PaaS would address typical system development controls. SaaS control objectives would focus on customisations, and rights and obligations of both parties.*	□ ○ △	■ ● ▲	■ ● ▲
AI2.8 Software Quality Assurance Develop, resource and execute a software QA plan to obtain the quality specified in the requirements definition and the organisation's quality policies and procedures. ***Comment:*** *Establish appropriate metrics to be used along with SLAs to ensure the quality of CSP delivery.*	■ ● ▲	■ ● ▲	■ ● ▲
AI2.9 Applications Requirements Management Track the status of individual requirements (including all rejected requirements) during the design, development and implementation, and approve changes to requirements through an established change management process.	■ ● ▲	■ ● ▲	■ ● ▲
AI2.10 Application Software Maintenance Develop a strategy and plan for the maintenance of software applications. ***Comment:*** *Ensure that the customer and the CSP has a notification process to provide sufficient notification of application software changes to allow the customer to modify any interfacing applications.*	□ ○ △	□ ○ △	■ ● ▲
AI3 Acquire and Maintain Technology Infrastructure Organisations have processes for the acquisition, implementation and upgrade of the technology infrastructure. This requires a planned approach to acquisition, maintenance and protection of infrastructure in line with agreed-upon technology strategies and the provision of development and test environments. This ensures that there is ongoing technological support for business applications.			

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Acquire and Implement (AI) *(cont.)*			
AI3.1 Technological Infrastructure Acquisition Plan Produce a plan for the acquisition, implementation and maintenance of the technological infrastructure that meets established business functional and technical requirements and is in accord with the organisation's technology direction. ***Comment:*** *IaaS is the primary focus, but PaaS may require supporting technology during development and as a precondition of implementation.*	■ ● ▲	■ ● ▲	□ ○ △
AI3.2 Infrastructure Resource Protection and Availability Implement internal control, security and auditability measures during configuration, integration and maintenance of hardware and infrastructural software to protect resources and ensure availability and integrity. Responsibilities for using sensitive infrastructure components should be clearly defined and understood by those who develop and integrate infrastructure components. Their use should be monitored and evaluated. ***Comment:*** *Private and hybrid delivery models require the customer to consider these control objectives. The CSP is solely responsible for public delivery of IaaS, PaaS and all SaaS.*	□ ● ▲	□ ● ▲	□ ○ △
AI3.3 Infrastructure Maintenance Develop a strategy and plan for infrastructure maintenance, and ensure that changes are controlled in line with the organisation's change management procedure. Include periodic reviews against business needs, patch management, upgrade strategies, risks, vulnerabilities assessment and security requirements. ***Comment:*** *In a private or hybrid delivery model, maintenance is the partial responsibility of the customer and a major focus of the CSP.*	□ ● ▲	□ ● ▲	□ ○ △
AI3.4 Feasibility Test Environment Establish development and test environments to support effective and efficient feasibility and integration testing of infrastructure components. ***Comment:*** *Since PaaS is a development platform, this is necessary. IaaS is limited to hardware configuration issues.*	□ ● ▲	□ ● ▲	□ ○ △
AI4 Enable Operation and Use Knowledge about new systems is made available. This process requires the production of documentation and manuals for users and IT, and provides training to ensure the proper use and operation of applications and infrastructure.			

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Acquire and Implement (AI) ***(cont.)***			
AI4.1 Planning for Operational Solutions Develop a plan to identify and document all technical, operational and usage aspects such that all those who will operate, use and maintain the automated solutions can exercise their responsibility. ***Comment:*** *PaaS is excluded here because it is a development platform not designed for operations processing.*	■ ● ▲	□ ○ △	□ ○ △
AI4.2 Knowledge Transfer to Business Management Transfer knowledge to business management to allow those individuals to take ownership of the system and data, and exercise responsibility for service delivery and quality, internal control, and application administration.	■ ● ▲	□ ○ △	■ ● ▲
AI4.3 Knowledge Transfer to End Users Transfer knowledge and skills to allow end users to effectively and efficiently use the system in support of business processes. ***Comment:*** *IaaS is included because, by definition, infrastructure can be provisioned by the user.*	■ ● ▲	□ ○ △	■ ● ▲
AI4.4 Knowledge Transfer to Operations and Support Staff Transfer knowledge and skills to enable operations and technical support staff to effectively and efficiently deliver, support and maintain the system and associated infrastructure.	■ ● ▲	■ ● ▲	■ ● ▲
AI5 Procure IT Resources IT resources, including people, hardware, software and services, need to be procured. This requires the definition and enforcement of procurement procedures, the selection of vendors, the setup of contractual arrangements, and the acquisition itself. Doing so ensures that the organisation has all required IT resources in a timely and cost-effective manner.			
AI5.1 Procurement Control Develop and follow a set of procedures and standards that is consistent with the business organisation's overall procurement process and acquisition strategy to acquire IT-related infrastructure, facilities, hardware, software and services needed by the business.	■ ● ▲	■ ● ▲	■ ● ▲
AI5.2 Supplier Contract Management Set up a procedure for establishing, modifying and terminating contracts for all suppliers. The procedure should cover, at a minimum, legal, financial, organisational, documentary, performance, security, intellectual property, and termination responsibilities and liabilities (including penalty clauses). All contracts and contract changes should be reviewed by legal advisors. ***Comment:*** *Cloud contract must be explicit in its definition of rights and obligations, and SLAs.*	■ ● ▲	■ ● ▲	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Acquire and Implement (AI) *(cont.)*			
AI5.3 Supplier Selection Select suppliers according to a fair and formal practice to ensure a viable best fit based on specified requirements. Requirements should be optimised with input from potential suppliers.	■ ● ▲	■ ● ▲	■ ● ▲
AI5.4 IT Resources Acquisition Protect and enforce the organisation's interests in all acquisition contractual agreements, including the rights and obligations of all parties in the contractual terms for the acquisition of software, development resources, infrastructure and services. ***Comment:*** *Refer to AI5.2*	■ ● ▲	■ ● ▲	■ ● ▲
AI6 Manage Changes All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment are formally managed in a controlled manner. Changes (including those to procedures, processes, system and service parameters) are logged, assessed and authorised prior to implementation and reviewed against planned outcomes following implementation. This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.			
AI6.1 Change Standards and Procedures Set up formal change management procedures to handle in a standardised manner all requests (including maintenance and patches) for changes to applications, procedures, processes, system and service parameters, and the underlying platforms. ***Comment:*** *This would be applicable to SaaS if the customer has implemented any customisation to the applications or manages interfaces to internal applications.*	■ ● ▲	■ ● ▲	■ ● ▲
AI6.2 Impact Assessment, Prioritisation and Authorisation Assess all requests for change in a structured way to determine the impact on the operational system and its functionality. Ensure that changes are categorised, prioritised and authorised. ***Comment:*** *See AI6.1*	■ ● ▲	■ ● ▲	■ ● ▲
AI6.3 Emergency Changes Establish a process for defining, raising, testing, documenting, assessing and authorising emergency changes that do not follow the established change process. ***Comment:*** *See AI6.1*	■ ● ▲	■ ● ▲	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Acquire and Implement (AI) ***(cont.)***			
AI6.4 Change Status Tracking and Reporting Establish a tracking and reporting system to document rejected changes, communicate the status of approved and in-process changes, and complete changes. Make certain that approved changes are implemented as planned. ***Comment:*** *Even though the CSP is providing much of the infrastructure and applications, it is critical that the customer maintains control over tracking and reporting. This will be useful in evaluating compliance with SLAs.*	■ ● ▲	■ ● ▲	■ ● ▲
AI6.5 Change Closure and Documentation Whenever changes are implemented, update the associated system and user documentation and procedures accordingly.	■ ● ▲	■ ● ▲	■ ● ▲
AI7 Install and Accredit Solutions and Changes New systems need to be made operational once development is complete. This requires proper testing in a dedicated environment with relevant test data, definition of rollout and migration instructions, release planning and actual promotion to production, and a post-implementation review. This assures that operational systems are in line with the agreed-upon expectations and outcomes.			
AI7.1 Training Train the staff members of the affected user departments and the operations group of the IT function in accordance with the defined training and implementation plan and associated materials, as part of every information systems development, implementation or modification project.	■ ● ▲	■ ● ▲	■ ● ▲
AI7.2 Test Plan Establish a test plan based on organisationwide standards that define roles, responsibilities, and entry and exit criteria. Ensure that the plan is approved by relevant parties.	■ ● ▲	■ ● ▲	■ ● ▲
AI7.3 Implementation Plan Establish an implementation and fallback/backout plan. Obtain approval from relevant parties.	■ ● ▲	■ ● ▲	■ ● ▲
AI7.4 Test Environment Define and establish a secure test environment representative of the planned operations environment relative to security, internal controls, operational practices, data quality and privacy requirements, and workloads. ***Comment:*** *The customer should be encouraged to provision its own test environment as required.*	■ ● ▲	■ ● ▲	■ ● ▲
AI7.5 System and Data Conversion Plan data conversion and infrastructure migration as part of the organisation's development methods, including audit trails, rollbacks and fallbacks.	□ ○ △	■ ● ▲	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Acquire and Implement (AI) *(cont.)*			
AI7.6 Testing of Changes Test changes independently in accordance with the defined test plan prior to migration to the operational environment. Ensure that the plan considers security and performance.	■ ● ▲	■ ● ▲	■ ● ▲
AI7.7 Final Acceptance Test Ensure that business process owners and IT stakeholders evaluate the outcome of the testing process as determined by the test plan. Remediate significant errors identified in the testing process, having completed the suite of tests identified in the test plan and any necessary regression tests. Following evaluation, approve promotion to production.	■ ● ▲	■ ● ▲	■ ● ▲
AI7.8 Promotion to Production Following testing, control the handover of the changed system to operations, keeping it in line with the implementation plan. Obtain approval of the key stakeholders, such as users, system owner and operational management. Where appropriate, run the system in parallel with the old system for a while, and compare behaviour and results. ***Comment:*** *SaaS will focus on changes and their effect on the functionality. PaaS will relate to standard development considerations.*	□ ○ △	■ ● ▲	□ ● ▲
AI7.9 Post-implementation Review Establish procedures in line with the organisational change management standards to require a post-implementation review as set out in the implementation plan.	■ ● ▲	■ ● ▲	■ ● ▲
COBIT Domain: Deliver and Support (DS)			
DS1 Define and Manage Service Levels Effective communication between IT management and business customers regarding services required is enabled by a documented definition of and agreement on IT services and service levels. This process also includes monitoring and timely reporting to stakeholders on the accomplishment of service levels. This process enables alignment between IT services and the related business requirements.			
DS1.1 Service Level Management Framework Define a framework that provides a formalised service level management process between the customer and service provider. The framework should maintain continuous alignment with business requirements and priorities and facilitate common understanding between the customer and provider(s). The framework should include processes for creating service requirements, service definitions, SLAs, OLAs and funding sources. These attributes should be organised in a service catalogue. The framework should define the organisational structure for service level management, covering the roles, tasks and responsibilities of internal and external service providers and customers. ***Comment:*** *Service levels are key to the effective administration of the contract and maintaining mutual expectations.*	■ ● ▲	■ ● ▲	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Deliver and Support (DS) ***(cont.)***			
DS1.2 Definition of Services Base definitions of IT services on service characteristics and business requirements. Ensure that they are organised and stored centrally via the implementation of a service catalogue portfolio approach. ***Comment:*** *The contract should define the business requirements and services explicitly, with metrics to facilitate SLA monitoring.*	■ ● ▲	■ ● ▲	■ ● ▲
DS1.3 Service Level Agreements Define and agree to SLAs for all critical IT services based on customer requirements and IT capabilities. This should cover customer commitments; service support requirements; quantitative and qualitative metrics for measuring the service signed off on by the stakeholders; funding and commercial arrangements, if applicable; and roles and responsibilities, including oversight of the SLA. Consider items such as availability, reliability, performance, capacity for growth, levels of support, continuity planning, security and demand constraints. ***Comment:*** *SLAs must be part of the contract, be measurable, and monitored by the customer.*	■ ● ▲	■ ● ▲	■ ● ▲
DS1.4 Operating Level Agreements Define OLAs that explain how the services will be technically delivered to support the SLA(s) in an optimal manner. The OLAs should specify the technical processes in terms meaningful to the provider and may support several SLAs.	■ ● ▲	■ ● ▲	■ ● ▲
DS1.5 Monitoring and Reporting of Service Level Achievements Continuously monitor specified service level performance criteria. Reports on achievement of service levels should be provided in a format that is meaningful to the stakeholders. The monitoring statistics should be analysed and acted upon to identify negative and positive trends for individual services as well as for services overall. ***Comment:*** *The CSP should report SLA metrics on a timely basis; the customer should maintain its own version of the SLA attainment for the purposes of comparison.*	■ ● ▲	■ ● ▲	■ ● ▲
DS1.6 Review of Service Level Agreements and Contracts Regularly review SLAs and underpinning contracts with internal and external service providers to ensure that they are effective and up to date and that changes in requirements have been taken into account.	■ ● ▲	■ ● ▲	■ ● ▲
DS2 Manage Third-party Services The need to assure that services provided by third parties (suppliers, vendors and partners) meet business requirements requires an effective third-party management process. This process is accomplished by clearly defining the roles, responsibilities and expectations in third-party agreements as well as reviewing and monitoring such agreements for effectiveness and compliance. Effective management of third-party services minimises the business risk associated with non-performing suppliers.			

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Deliver and Support (DS) ***(cont.)***			
DS2.1 Identification of All Supplier Relationships Identify all supplier services, and categorise them according to supplier type, significance and criticality. Maintain formal documentation of technical and organisational relationships covering the roles and responsibilities, goals, expected deliverables, and credentials of representatives of these suppliers.	■ ● ▲	■ ● ▲	■ ● ▲
DS2.2 Supplier Relationship Management Formalise the supplier relationship management process for each supplier. The relationship owners should liaise on customer and supplier issues and ensure the quality of the relationship based on trust and transparency (e.g., through SLAs).	■ ● ▲	■ ● ▲	■ ● ▲
DS2.3 Supplier Risk Management Identify and mitigate risks relating to suppliers' ability to continue effective service delivery in a secure and efficient manner on a continual basis. Ensure that contracts conform to universal business standards in accordance with legal and regulatory requirements. Risk management should further consider non-disclosure agreements (NDAs), escrow contracts, continued supplier viability, conformance with security requirements, alternative suppliers, penalties and rewards, etc.	■ ● ▲	■ ● ▲	■ ● ▲
DS2.4 Supplier Performance Monitoring Establish a process to monitor service delivery to ensure that the supplier is meeting current business requirements and continuing to adhere to the contract agreements and SLAs, and that performance is competitive with alternative suppliers and market conditions.	■ ● ▲	■ ● ▲	■ ● ▲
DS3 Manage Performance and Capacity The need to manage performance and capacity of IT resources requires a process to periodically review current performance and capacity of IT resources. This process includes forecasting future needs based on workload, storage and contingency requirements. This process provides assurance that information resources supporting business requirements are continually available.			
DS3.1 Performance and Capacity Planning Establish a planning process for the review of performance and capacity of IT resources to ensure that cost-justifiable capacity and performance are available to process the agreed-upon workloads as determined by the SLAs. Capacity and performance plans should leverage appropriate modelling techniques to produce a model of the current and forecasted performance, capacity and throughput of the IT resources. ***Comment:*** *Users must continue future capacity needs with respect to future requirements, e.g., acquisition. The time frame necessary to address additional capacity is much shorter in a cloud environment. Focus will be on the purchase of more licences.*	□ ○ △	□ ○ △	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Deliver and Support (DS) *(cont.)*			
DS3.2 Current Performance and Capacity Assess current performance and capacity of IT resources to determine if sufficient capacity and performance exist to deliver against agreed-upon service levels. ***Comment:*** *This objective changes focus—customer wants to be sure that internal resources exist to handle service levels. The CSP is responsible for addressing the infrastructure and processing needs.*	■ ● ▲	■ ● ▲	■ ● ▲
DS3.3 Future Performance and Capacity Conduct performance and capacity forecasting of IT resources at regular intervals to minimise the risk of service disruptions due to insufficient capacity or performance degradation, and identify excess capacity for possible redeployment. Identify workload trends and determine forecasts to be input to performance and capacity plans. ***Comment:*** *See DS3.2*	■ ● ▲	■ ● ▲	■ ● ▲
DS3.5 Monitoring and Reporting Continuously monitor the performance and capacity of IT resources. Data gathered should serve two purposes: • To maintain and tune current performance within IT and address such issues as resilience, contingency, current and projected workloads, storage plans, and resource acquisition • To report delivered service availability to the business, as required by the SLAs. Accompany all exception reports with recommendations for corrective action. ***Comment:*** *Monitoring and reporting focuses on internal performance/ capacity, and CSP's attainment of SLAs.*	■ ● ▲	■ ● ▲	■ ● ▲
DS4 Ensure Continuous Service The need for providing continuous IT services requires developing, maintaining and testing IT continuity plans, utilising offsite backup storage and providing periodic continuity plan training. An effective continuous service process minimises the probability and impact of a major IT service interruption on key business functions and processes.			

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Deliver and Support (DS) ***(cont.)***			
DS4.1 IT Continuity Framework Develop a framework for IT continuity to support enterprisewide business continuity management using a consistent process. The objective of the framework should be to assist in determining the required resilience of the infrastructure and to drive the development of disaster recovery and IT contingency plans. The framework should address the organisational structure for continuity management, covering the roles, tasks and responsibilities of internal and external service providers, their management and their customers, and the planning processes that create the rules and structures to document, test and execute the disaster recovery and IT contingency plans. The plan should also address items such as the identification of critical resources, noting key dependencies, the monitoring and reporting of the availability of critical resources, alternative processing, and the principles of backup and recovery. ***Comment:*** *Customer needs to address the internal IT continuity framework, which supports the CSP interface. Workstation and network considerations would address this issue.*	■ ● ▲	■ ● ▲	■ ● ▲
DS4.2 IT Continuity Plans Develop IT continuity plans based on the framework and designed to reduce the impact of a major disruption on key business functions and processes. The plans should be based on risk understanding of potential business impacts and address requirements for resilience, alternative processing and recovery capability of all critical IT services. They should also cover usage guidelines, roles and responsibilities, procedures, communication processes, and the testing approach. ***Comment:*** *Same as DS4.1*	■ ● ▲	■ ● ▲	■ ● ▲
DS4.3 Critical IT Resources Focus attention on items specified as most critical in the IT continuity plan to build in resilience and establish priorities in recovery situations. Avoid the distraction of recovering less-critical items and ensure response and recovery in line with prioritised business needs, while ensuring that costs are kept at an acceptable level and complying with regulatory and contractual requirements. Consider resilience, response and recovery requirements for different tiers, e.g., one to four hours, four to 24 hours, more than 24 hours and critical business operational periods. ***Comment:*** *Customers must define their critical internal IT resources, and processes to address the need for continuous service. This may include interfaces and internal automated processes. Alternate processing approaches may need to be considered if the servicer is incapable of restoring CSP in a timely manner. CSP is responsible for providing infrastructure to assure continuous service.*	■ ● ▲	■ ● ▲	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Deliver and Support (DS) ***(cont.)***			
DS4.4 Maintenance of the IT Continuity Plan Encourage IT management to define and execute change control procedures to ensure that the IT continuity plan is kept up to date and continually reflects actual business requirements. Communicate changes in procedures and responsibilities clearly and in a timely manner.	■ ● ▲	■ ● ▲	■ ● ▲
DS4.5 Testing of the IT Continuity Plan Test the IT continuity plan on a regular basis to ensure that IT systems can be effectively recovered, shortcomings are addressed and the plan remains relevant. This requires careful preparation, documentation, reporting of test results and, according to the results, implementation of an action plan. Consider the extent of testing recovery of single applications to integrated testing scenarios to end-to-end testing and integrated vendor testing.	■ ● ▲	■ ● ▲	■ ● ▲
DS4.6 IT Continuity Plan Training Provide all concerned parties with regular training sessions regarding the procedures and their roles and responsibilities in case of an incident or disaster. Verify and enhance training according to the results of the contingency tests.	■ ● ▲	■ ● ▲	■ ● ▲
DS4.7 Distribution of the IT Continuity Plan Determine that a defined and managed distribution strategy exists to ensure that plans are properly and securely distributed and available to appropriately authorised interested parties when and where needed. Attention should be paid to making the plans accessible under all disaster scenarios.	■ ● ▲	■ ● ▲	■ ● ▲
DS4.8 IT Services Recovery and Resumption Plan the actions to be taken for the period when IT is recovering and resuming services. This may include activation of backup sites, initiation of alternative processing, customer and stakeholder communication, and resumption procedures. Ensure that the business understands IT recovery times and the necessary technology investments to support business recovery and resumption needs. ***Comment:*** *The CSP is responsible for processing and infrastructure. The customer retains ultimate responsibility for interfaces and interim processing during outages.*	■ ● ▲	■ ● ▲	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Deliver and Support (DS) ***(cont.)***			
DS4.9 Offsite Backup Storage Store offsite all critical backup media, documentation and other IT resources necessary for IT recovery and business continuity plans. Determine the content of backup storage in collaboration between business process owners and IT personnel. Management of the offsite storage facility should respond to the data classification policy and the enterprise's media storage practices. IT management should ensure that offsite arrangements are periodically assessed, at least annually, for content, environmental protection and security. Ensure compatibility of hardware and software to restore archived data, and periodically test and refresh archived data. ***Comment:*** *The customer must contractually mandate appropriate backup storage policies and where possible, obtain physical control over copies of customer backup storage.*	□ ○ △	■ ● ▲	■ ● ▲
DS4.10 Post-resumption Review Determine whether IT management has established procedures for assessing the adequacy of the plan in regard to the successful resumption of the IT function after a disaster, and update the plan accordingly. ***Comment:*** *The post-resumption review needs to analyse the effectiveness of the CSP and customer staff and processes. In addition, it has to evaluate whether the CSP has the ability and resources to manage the customer's data and recovery needs.*	■ ● ▲	■ ● ▲	■ ● ▲
DS5 Ensure Systems Security The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards, and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimise the business impact of security vulnerabilities and incidents.			
DS5.1 Management of IT Security Manage IT security at the highest appropriate organisational level, so the management of security actions is in line with business requirements. ***Comment:*** *The customer's security focus must address those processes to which the customer is responsible: policy, standards and guidelines. In addition, the customer must focus on the CSP's IT security management specific to the platform and delivery method.*	■ ● ▲	■ ● ▲	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Deliver and Support (DS) ***(cont.)***			
DS5.2 IT Security Plan Translate business, risk and compliance requirements into an overall IT security plan, taking into consideration the IT infrastructure and the security culture. Ensure that the plan is implemented in security policies and procedures together with appropriate investments in services, personnel, software and hardware. Communicate security policies and procedures to stakeholders and users. ***Comment:*** *The customer must evaluate the risk associated with cloud computing against compliance and business risks. The security plan would be limited to the boundaries within the customer's site and administrative scope.*	■ ● ▲	■ ● ▲	■ ● ▲
DS5.3 Identity Management Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security-responsible person. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement authentication and enforce access rights. ***Comment:*** *Customer responsibility in an IaaS model would be the definition of and scope of access to the authorisation system. Whether the customer could specify the identity management features and processes would depend on the contract and infrastructure functional capabilities.* *In the PaaS model, the design of security within the application is the responsibility of the customer, the CSP would be responsible for access to CSP applicable libraries, etc.* *In the SaaS model, the customer would be responsible for access privileges, access controls, etc., but the CSP would be responsible for the IT management within the application and architecture delivering the application functions. Access to customer application programs and data through super user privileges is highly restricted and monitored.*	■ ● ▲	■ ● ▲	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Deliver and Support (DS) *(cont.)*			
DS5.4 User Account Management Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Perform regular management review of all accounts and related privileges. ***Comment:*** *The customer retains responsibility for user access provisioning. CSP personnel should be excluded from the user account management process. If any CSP personnel are permitted access, their activities should be monitored through logging and management review processes.*	■ ● ▲	■ ● ▲	■ ● ▲
DS5.5 Security Testing, Surveillance and Monitoring Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited in a timely manner to ensure that the approved enterprise's information security baseline is maintained. A logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed. ***Comment:*** *Detection and prevention are the primary responsibilities of the CSP, but the customer should have processes in place to test and monitor the detection and prevention activities.*	■ ● ▲	■ ● ▲	■ ● ▲
DS5.6 Security Incident Definition Clearly define and communicate the characteristics of potential security incidents so they can be properly classified and treated by the incident and problem management process. ***Comment:*** *Customers must maintain their own security incident definition processes to assure CSP compliance and follow-through of identified security incidents. The contract must require the CSP to report every customer-relevant incidence to the customer in detail and in a timely fashion.*	■ ● ▲	■ ● ▲	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Deliver and Support (DS) *(cont.)*			
DS5.8 Cryptographic Key Management Determine that policies and procedures are in place to organise the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorised disclosure. ***Comment:*** *The customer is responsible for key management to maintain the integrity and privacy of data. Where appropriate, key management can be shared between the customer and CSP, provided advanced key management procedures are in place.*	■ ● ▲	■ ● ▲	■ ● ▲
DS5.10 Network Security Use security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion detection) to authorise access and control information flows from and to networks. ***Comment:*** *When provisioning under IaaS, the customer is responsible to ensure that appropriate network security devices are in place. For PaaS and SaaS, the customer is responsible for the customer's internal network.*	■ ● ▲	■ ● ▲	■ ● ▲
DS5.11 Exchange of Sensitive Data Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin. ***Comment:*** *Same as DS5.10, but the regulators and compliance authorities would hold the customer responsible for data leakage. Any actions between the parties as a result of non-compliance would be based upon contractual agreements and penalties.*	■ ● ▲	■ ● ▲	■ ● ▲
DS6 Identify and Allocate Costs The need for a fair and equitable system of allocating IT costs to the business requires accurate measurement of IT costs and agreement with business users on fair allocation. This process includes building and operating a system to capture, allocate and report IT costs to the users of services. A fair system of allocation enables the business to make more informed decisions regarding the use of IT services.			
DS6.1 Definition of Services Identify all IT costs, and map them to IT services to support a transparent cost model. IT services should be linked to business processes such that the business can identify associated service billing levels. ***Comment:*** *Definition of services is a customer internal matter.*	■ ● ▲	■ ● ▲	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Deliver and Support (DS) ***(cont.)***			
DS6.2 IT Accounting Capture and allocate actual costs according to the enterprise cost model. Variances between forecasts and actual costs should be analysed and reported on, in compliance with the enterprise's financial measurement systems. ***Comment:*** *The CSP must provide a detailed report of resources used.*	■ ● ▲	■ ● ▲	■ ● ▲
DS6.3 Cost Modelling and Charging Establish and use an IT costing model based on the service definitions that support the calculation of chargeback rates per service. The IT cost model should ensure that charging for services is identifiable, measurable and predictable by users to encourage proper use of resources. ***Comment:*** *The CSP will provide billing based upon usage; the customer is responsible for defining and managing cost allocations and chargebacks.*	■ ● ▲	■ ● ▲	■ ● ▲
DS6.4 Cost Model Maintenance Regularly review and benchmark the appropriateness of the cost/recharge model to maintain its relevance and appropriateness to the evolving business and IT activities. ***Comment:*** *See DS6.3*	■ ● ▲	■ ● ▲	■ ● ▲
DS7 Educate and Train Users Effective education of all users of IT systems, including those within IT, requires identifying the training needs of each user group. In addition to identifying needs, this process includes defining and executing a strategy for effective training and measuring the results. An effective training programme increases effective use of technology by reducing user errors, increasing productivity and increasing compliance with key controls, such as user security measures.			
DS7.1 Identification of Education and Training Needs Establish and regularly update a curriculum for each target group of employees considering: • Current and future business needs and strategy • Value of information as an asset • Corporate values (ethical values, control and security culture, etc.) • Implementation of new IT infrastructure and software (i.e., packages, applications) • Current and future skills, competence profiles, and certification and/or credentialing needs as well as required reaccreditation • Delivery methods (e.g., classroom, web-based), target group size, accessibility and timing ***Comment:*** *Ensure that training is updated to reflect the CSP's functionality and technology.*	■ ● ▲	■ ● ▲	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Deliver and Support (DS) ***(cont.)***			
DS7.2 Delivery of Training and Education Based on the identified education and training needs, identify target groups and their members, efficient delivery mechanisms, teachers, trainers, and mentors. Appoint trainers and organise timely training sessions. Record registration (including prerequisites), attendance and training session performance evaluations.	■ ● ▲	■ ● ▲	■ ● ▲
DS7.3 Evaluation of Training Received Evaluate education and training content delivery upon completion for relevance, quality, effectiveness, the retention of knowledge, cost and value. The results of this evaluation should serve as input for future curriculum definition and the delivery of training sessions.	■ ● ▲	■ ● ▲	■ ● ▲
DS8 Manage Service Desk and Incidents Timely and effective response to IT user queries and problems requires a well-designed and well-executed service desk and incident management process. This process includes setting up a service desk function with registration, incident escalation, trend and root cause analysis, and resolution. The business benefits include increased productivity through quick resolution of user queries. In addition, the business can address root causes (such as poor user training) through effective reporting.			
DS8.1 Service Desk Establish a service desk function, which is the user interface with IT, to register, communicate, dispatch and analyse all calls, reported incidents, service requests and information demands. There should be monitoring and escalation procedures based on agreed-upon service levels relative to the appropriate SLA that allow classification and prioritisation of any reported issue as an incident, service request or information request. Measure end users' satisfaction with the quality of the service desk and IT services. ***Comment:*** *A CSP, in general, provides service desk functions. An organisation may direct all issues to its internal help desk, which will in turn record and forward the issue to the CSP.*	□ ○ △	□ ○ △	□ ○ △

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Deliver and Support (DS) ***(cont.)***			
DS8.2 Registration of Customer Queries Establish a function and system to allow logging and tracking of calls, incidents, service requests and information needs. It should work closely with such processes as incident management, problem management, change management, capacity management and availability management. Incidents should be classified according to a business and service priority and routed to the appropriate problem management team, where necessary. Customers should be kept informed of the status of their queries. ***Comment:*** *The service desk would generally be the responsibility of the CSP. However, the customer must register customer issues. This will be used as the primary record to reconcile customer requests to the CSP's problem reporting system, to ensure that all requests are addressed in a timely manner and according to the SLAs.*	■ ● ▲	■ ● ▲	■ ● ▲
DS8.3 Incident Escalation Establish service desk procedures, so incidents that cannot be resolved immediately are appropriately escalated according to limits defined in the SLA and, if appropriate, workarounds are provided. Ensure that incident ownership and life cycle monitoring remain with the service desk for user-based incidents, regardless which IT group is working on resolution activities.	■ ● ▲	■ ● ▲	■ ● ▲
DS8.4 Incident Closure Establish procedures for the timely monitoring of clearance of customer queries. When the incident has been resolved, ensure that the service desk records the resolution steps, and confirm that the action taken has been agreed to by the customer. Also record and report unresolved incidents (known errors and workarounds) to provide information for proper problem management.	■ ● ▲	■ ● ▲	■ ● ▲
DS8.5 Reporting and Trend Analysis Produce reports of service desk activity to enable management to measure service performance and service response times and to identify trends or recurring problems, so service can be continually improved. ***Comment:*** *The customer must develop an internal service desk summary based upon the CSP's metrics.*	■ ● ▲	■ ● ▲	■ ● ▲
DS10 Manage Problems Effective problem management requires the identification and classification of problems, root cause analysis and resolution of problems. The problem management process also includes the formulation of recommendations for improvement, maintenance of problem records and review of the status of corrective actions. An effective problem management process maximises system availability, improves service levels, reduces costs, and improves customer convenience and satisfaction.			

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Deliver and Support (DS) ***(cont.)***			
DS10.1 Identification and Classification of Problems Implement processes to report and classify problems that have been identified as part of incident management. The steps involved in problem classification are similar to the steps in classifying incidents; they are to determine category, impact, urgency and priority. Categorise problems as appropriate into related groups or domains (e.g., hardware, software, support software). These groups may match the organisational responsibilities of the user and customer base, and should be the basis for allocating problems to support staff. ***Comment:*** *The process must refer to the SLA and/or contract.*	■ ● ▲	■ ● ▲	■ ● ▲
DS10.2 Problem Tracking and Resolution Ensure that the problem management system provides for adequate audit trail facilities that allow tracking, analysing and determining the root cause of all reported problems considering: • All associated configuration items • Outstanding problems and incidents • Known and suspected errors • Tracking of problem trends Identify and initiate sustainable solutions addressing the root cause, raising change requests via the established change management process. Throughout the resolution process, problem management should obtain regular reports from change management on progress in resolving problems and errors. Problem management should monitor the continuing impact of problems and known errors on user services. In the event that this impact becomes severe, problem management should escalate the problem, perhaps referring it to an appropriate board to increase the priority of the request for change (RFC) or to implement an urgent change as appropriate. Monitor the progress of problem resolution against SLAs.	■ ● ▲	■ ● ▲	■ ● ▲
DS10.3 Problem Closure Put in place a procedure to close problem records either after confirmation of successful elimination of the known error or after agreement with the business on how to alternatively handle the problem.	■ ● ▲	■ ● ▲	■ ● ▲
DS10.4 Integration of Configuration, Incident and Problem Management Integrate the related processes of configuration, incident and problem management to ensure effective management of problems and enable improvements. ***Comment:*** *No or minimal configuration management*	■ ● ▲	■ ● ▲	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Deliver and Support (DS) ***(cont.)***			
DS11 Manage Data Effective data management requires identifying data requirements. The data management process also includes the establishment of effective procedures to manage the media library, backup and recovery of data, and proper disposal of media. Effective data management helps ensure the quality, timeliness and availability of business data.			
DS11.1 Business Requirements for Data Management Verify that all data expected for processing are received and processed completely, accurately and in a timely manner, and all output is delivered in accordance with business requirements. Support restart and reprocessing needs. ***Comment:*** *The customer must establish SLAs defining expectations and requirements. The customer must establish data management policy and procedures for interfacing data that remains within the confines of the customer's IT infrastructure. The customer may also need to establish transaction control mechanisms to ensure completeness of processing.*	□ ○ △	□ ○ △	■ ● ▲
DS11.4 Disposal Define and implement procedures to ensure that business requirements for protection of sensitive data and software are met when data and hardware are disposed or transferred. ***Comment:*** *The CSP will physically destroy any remaining data upon the expiration/termination of the contract.*	■ ● ▲	■ ● ▲	■ ● ▲
DS11.5 Backup and Restoration Define and implement procedures for backup and restoration of systems, applications, data and documentation in line with business requirements and the continuity plan. ***Comment:*** *A contract must define SLAs relevant to the backup and restoration of data.*	■ ● ▲	■ ● ▲	■ ● ▲
DS11.6 Security Requirements for Data Management Define and implement policies and procedures to identify and apply security requirements applicable to the receipt, processing, storage and output of data to meet business objectives, the organisation's security policy and regulatory requirements. ***Comment:*** *See DS11.1*	■ ● ▲	■ ● ▲	■ ● ▲
DS12 Manage the Physical Environment Protection for computer equipment and personnel requires well-designed and well-managed physical facilities. The process of managing the physical environment includes defining the physical site requirements, selecting appropriate facilities, and designing effective processes for monitoring environmental factors and managing physical access. Effective management of the physical environment reduces business interruptions from damage to computer equipment and personnel.			

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Deliver and Support (DS) *(cont.)*			
DS12.1 Site Selection and Layout Define and select the physical sites for IT equipment to support the technology strategy linked to the business strategy. The selection and design of the layout of a site should take into account the risk associated with natural and man-made disasters, whilst considering relevant laws and regulations, such as occupational health and safety regulations. ***Comment:*** *Contract requirements should specify whether the customer must comply with regulations or statutes on geographic location of data. This requirement may impact the CSP's site selection, or its ability to meet customer processing requirements.*	□ ○ △	□ ○ △	■ ● ▲
DS12.2 Physical Security Measures Define and implement physical security measures in line with business requirements to secure the location and the physical assets. Physical security measures must be capable of effectively preventing, detecting and mitigating risks relating to theft, temperature, fire, smoke, water, vibration, terror, vandalism, power outages, chemicals or explosives. ***Comment:*** *The CSP is responsible for physical security based upon contract provisions.*	□ ○ △	□ ○ △	■ ● ▲
DS13 Manage Operations Complete and accurate processing of data requires effective management of data processing procedures and diligent maintenance of hardware. This process includes defining operating policies and procedures for effective management of scheduled processing, protecting sensitive output, monitoring infrastructure performance and ensuring preventive maintenance of hardware. Effective operations management helps maintain data integrity and reduces business delays and IT operating costs.			
DS13.4 Sensitive Documents and Output Devices Establish appropriate physical safeguards, accounting practices and inventory management over sensitive IT assets, such as special forms, negotiable instruments, special purpose printers or security tokens. ***Comment:*** *Only applies to SaaS implementations where the CSP prints sensitive documents.*	□ ○ △	□ ○ △	■ ● ▲
COBIT Domain: Monitor and Evaluate (ME)			
ME1 Monitor and Evaluate IT Performance Effective IT performance management requires a monitoring process. This process includes defining relevant performance indicators, systematic and timely reporting of performance, and prompt acting upon deviations. Monitoring is needed to make sure that the right things are done and are in line with the set directions and policies.			

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Monitor and Evaluate (ME) ***(cont.)***			
ME1.1 Monitoring Approach Establish a general monitoring framework and approach to define the scope, methodology and process to be followed for measuring IT's solution and service delivery, and monitor IT's contribution to the business. Integrate the framework with the corporate performance management system.	■ ● ▲	□ ○ △	■ ● ▲
ME1.2 Definition and Collection of Monitoring Data Work with the business to define a balanced set of performance targets and have them approved by the business and other relevant stakeholders. Define benchmarks with which to compare the targets, and identify available data to be collected to measure the targets. Establish processes to collect timely and accurate data to report on progress against targets.	■ ● ▲	□ ○ △	■ ● ▲
ME1.3 Monitoring Method Deploy a performance monitoring method (e.g., balanced scorecard) that records targets; captures measurements; provides a succinct, all-around view of IT performance; and fits within the enterprise monitoring system.	■ ● ▲	■ ● ▲	■ ● ▲
ME1.4 Performance Assessment Periodically review performance against targets, analyse the cause of any deviations, and initiate remedial action to address the underlying causes. At appropriate times, perform root cause analysis across deviations. ***Comment:*** *Analyse actual performance against SLA requirements.*	■ ● ▲	□ ○ △	■ ● ▲
ME1.5 Board and Executive Reporting Develop senior management reports on IT's contribution to the business, specifically in terms of the performance of the enterprise's portfolio, IT-enabled investment programmes, and the solution and service deliverable performance of individual programmes. Include in status reports the extent to which planned objectives have been achieved, budgeted resources used, set performance targets met and identified risks mitigated. Anticipate senior management's review by suggesting remedial actions for major deviations. Provide the report to senior management, and solicit feedback from management's review. ***Comment:*** *This will depend upon the investment and the overall significance to the organisation.*	■ ● ▲	■ ● ▲	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Monitor and Evaluate (ME) *(cont.)*			
ME1.6 Remedial Actions Identify and initiate remedial actions based on performance monitoring, assessment and reporting. This includes follow-up of all monitoring, reporting and assessments through: • Review, negotiation and establishment of management responses • Assignment of responsibility for remediation • Tracking of the results of actions committed ***Comment:*** *This is a monitoring of the CSP's performance as well as the interface processes that are the responsibility of the customer.*	■ ● ▲	■ ● ▲	■ ● ▲
ME2 Monitor and Evaluate Internal Control Establishing an effective internal control programme for IT requires a well-defined monitoring process. This process includes the monitoring and reporting of control exceptions, results of self-assessments and third-party reviews. A key benefit of internal control monitoring is to provide assurance regarding effective and efficient operations and compliance with applicable laws and regulations.			
ME2.1 Monitoring of Internal Control Framework Continuously monitor, benchmark and improve the IT control environment and control framework to meet organisational objectives. ***Comment:*** *The customer is responsible for its control framework and how it relates to the CSP's performance.*	■ ● ▲	■ ● ▲	■ ● ▲
ME2.2 Supervisory Review Monitor and evaluate the efficiency and effectiveness of internal IT managerial review controls.	■ ● ▲	■ ● ▲	■ ● ▲
ME2.3 Control Exceptions Identify control exceptions, and analyse and identify their underlying root causes. Escalate control exceptions and report to stakeholders appropriately. Institute necessary corrective action. ***Comment:*** *Root cause analysis may be limited to what the CSP will provide. The fact that the CSP is addressing the issues and the customer's monitoring mechanism tracks repetition of issues would suffice.*	■ ● ▲	■ ● ▲	■ ● ▲
ME2.4 Control Self-assessment Evaluate the completeness and effectiveness of management's control over IT processes, policies and contracts through a continuing programme of self-assessment. ***Comment:*** *This relates to the customer's processes and responsibilities.*	□ ○ △	□ ○ △	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Monitor and Evaluate (ME) *(cont.)*			
ME2.5 Assurance of Internal Control Obtain, as needed, further assurance of the completeness and effectiveness of internal controls through third-party reviews. ***Comment:*** *This includes the receipt of SSAE16 (SAS70) third-party reports from CSPs for relevant processes, and the right to audit where third-party reviews are inadequate or not available.*	■ ● ▲	■ ● ▲	■ ● ▲
ME2.6 Internal Control at Third Parties Assess the status of external service providers' internal controls. Confirm that external service providers comply with legal and regulatory requirements and contractual obligations. ***Comment:*** *See ME2.5*	■ ● ▲	■ ● ▲	■ ● ▲
ME2.7 Remedial Actions Identify, initiate, track and implement remedial actions arising from control assessments and reporting.	■ ● ▲	■ ● ▲	■ ● ▲
ME3 Ensure Compliance With External Requirements Effective oversight of compliance requires the establishment of a review process to ensure compliance with laws, regulations and contractual requirements. This process includes identifying compliance requirements, optimising and evaluating the response, obtaining assurance that the requirements have been complied with and, finally, integrating IT's compliance reporting with the rest of the business.			
ME3.1 Identification of External Legal, Regulatory and Contractual Compliance Requirements Identify, on a continuous basis, local and international laws, regulations, and other external requirements that must be complied with for incorporation into the organisation's IT policies, standards, procedures and methodologies. ***Comment:*** *When considering the monitoring of compliance requirements, the customer must recognise that it is responsible for compliance with external regulations regardless of the CSP's actions or inactions*	■ ● ▲	□ ○ △	■ ● ▲
ME3.2 Optimisation of Response to External Requirements Review and adjust IT policies, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated.	■ ● ▲	□ ○ △	■ ● ▲
ME3.3 Evaluation of Compliance With External Requirements Confirm compliance of IT policies, standards, procedures and methodologies with legal and regulatory requirements.	■ ● ▲	□ ○ △	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Monitor and Evaluate (ME) *(cont.)*			
ME3.4 Positive Assurance of Compliance Obtain and report assurance of compliance and adherence to all internal policies derived from internal directives or external legal, regulatory or contractual requirements, confirming that any corrective actions to address any compliance gaps have been taken by the responsible process owner in a timely manner. ***Comment:*** *Refer to third party review or customer auditing of CSP processes.*	■ ● ▲	□ ○ △	■ ● ▲
ME3.5 Integrated Reporting Integrate IT reporting on legal, regulatory and contractual requirements with similar output from other business functions. ***Comment:*** *Integration is not necessarily desirable due to enforcement of SLAs.*	□ ○ △	□ ○ △	□ ○ △
ME4 Provide IT Governance Establishing an effective governance framework includes defining organisational structures, processes, leadership, roles and responsibilities to ensure that enterprise IT investments are aligned and delivered in accordance with enterprise strategies and objectives.			
ME4.1 Establishment of an IT Governance Framework Define, establish and align the IT governance framework with the overall enterprise governance and control environment. Base the framework on a suitable IT process and control model and provide for unambiguous accountability and practices to avoid a breakdown in internal control and oversight. Confirm that the IT governance framework ensures compliance with laws and regulations and is aligned with, and confirms delivery of, the enterprise's strategies and objectives. Report IT governance status and issues. ***Comment:*** *The IT governance framework includes CSP processes as well as any internal processes. Cloud processes should be addressed as any other third-party provider.*	□ ○ △	□ ○ △	□ ○ △

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Monitor and Evaluate (ME) ***(cont.)***			
ME4.2 Strategic Alignment Enable board and executive understanding of strategic IT issues, such as the role of IT, technology insights and capabilities. Ensure that there is a shared understanding between the business and IT regarding the potential contribution of IT to the business strategy. Work with the board and the established governance bodies, such as an IT strategy committee, to provide strategic direction to management relative to IT, ensuring that the strategy and objectives are cascaded into business units and IT functions, and that confidence and trust are developed between the business and IT. Enable the alignment of IT to the business in strategy and operations, encouraging co-responsibility between the business and IT for making strategic decisions and obtaining benefits from IT-enabled investments. ***Comment:*** *Whether IT resources are outsourced via cloud, traditional outsourced arrangement, or maintained internally, they must align with organisational strategies.*	□ ○ △	□ ○ △	□ ○ △
ME4.3 Value Delivery Manage IT-enabled investment programmes and other IT assets and services to ensure that they deliver the greatest possible value in supporting the enterprise's strategy and objectives. Ensure that the expected business outcomes of IT-enabled investments and the full scope of effort required to achieve those outcomes are understood; that comprehensive and consistent business cases are created and approved by stakeholders; that assets and investments are managed throughout their economic life cycle; and that there is active management of the realisation of benefits, such as contribution to new services, efficiency gains and improved responsiveness to customer demands. Enforce a disciplined approach to portfolio, programme and project management, insisting that the business takes ownership of all IT-enabled investments and IT ensures optimisation of the costs of delivering IT capabilities and services. ***Comment:*** *Whether IT resources are outsourced via cloud, traditional outsourced arrangement, or maintained internally, they must provide value delivery.*	□ ○ △	□ ○ △	□ ○ △

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Monitor and Evaluate (ME) *(cont.)*			
ME4.5 Risk Management Work with the board to define the enterprise's appetite for IT risk, and obtain reasonable assurance that IT risk management practices are appropriate to ensure that the actual IT risk does not exceed the board's risk appetite. Embed risk management responsibilities into the organisation, ensuring that the business and IT regularly assess and report IT-related risks and their impact and that the enterprise's IT risk position is transparent to all stakeholders. ***Comment:*** *Ensure that the C-suite is apprised of the risk associated with the adoption of cloud computing for critical functions.*	■ ● ▲	■ ● ▲	■ ● ▲
ME4.6 Performance Measurement Confirm that agreed-upon IT objectives have been met or exceeded, or that progress toward IT goals meets expectations. Where agreed-upon objectives have been missed or progress is not as expected, review management's remedial action. Report to the board relevant portfolios, programme and IT performance, supported by reports to enable senior management to review the enterprise's progress toward identified goals. ***Comment:*** *The SLA metrics will provide the basis for performance measurement and will include both CSP and customer internal SLAs.*	■ ● ▲	■ ● ▲	■ ● ▲
ME4.7 Independent Assurance Obtain independent assurance (internal or external) about the conformance of IT with relevant laws and regulations; the organisation's policies, standards and procedures; generally accepted practices; and the effective and efficient performance of IT. ***Comment:*** *Independent assurance will be limited to third-party reviews or internal audits within the contractual rights and obligations.*	■ ● ▲	□ ○ △	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Appendix B. Cloud Computing Management Audit/Assurance Program

This audit/assurance program is posted in Word for ISACA members at *www.isaca.org/Cloud-Audit-Program.aspx*. It is also available in the ISACA Bookstore.

I. Introduction

Overview

ISACA has developed the IT Assurance Framework (ITAF) as a comprehensive and good-practice-setting model. ITAF provides standards that are designed to be mandatory and that are the guiding principles under which the IT audit and assurance profession operates. The guidelines provide information and direction for the practice of IT audit and assurance. The tools and techniques provide methodologies, tools and templates to provide direction in the application of IT audit and assurance processes.

Purpose

The audit/assurance program is a tool and template to be used as a road map for the completion of a specific assurance process. ISACA has commissioned audit/assurance programs to be developed for use by IT audit and assurance practitioners. This audit/assurance program is intended to be utilized by IT audit and assurance professionals with the requisite knowledge of the subject matter under review, as described in ITAF section 2200—General Standards. The audit/assurance programs are part of ITAF section 4000—IT Assurance Tools and Techniques.

Control Framework

The audit/assurance programs have been developed in alignment with the ISACA COBIT framework—specifically COBIT 4.1—using generally applicable and accepted good practices. They reflect ITAF sections 3400—IT Management Processes, 3600—IT Audit and Assurance Processes, and 3800—IT Audit and Assurance Management.

Many organizations have embraced several frameworks at an enterprise level, including the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control Framework. The importance of the control framework has been enhanced due to regulatory requirements by the US Securities and Exchange Commission (SEC) as directed by the US Sarbanes-Oxley Act of 2002 and similar legislation in other countries. Enterprises seek to integrate control framework elements used by the general audit/assurance team into the IT audit and assurance framework. Since COSO is widely used, it has been selected for inclusion in this audit/assurance program. The reviewer may delete or rename these columns to align with the enterprise's control framework.

Governance, Risk and Control of IT

Governance, risk and control of IT are critical in the performance of any assurance management process. Governance of the process under review will be evaluated as part of the policies and management oversight controls. Risk plays an important role in evaluating what to audit and how management approaches and manages risk. Both issues are evaluated as steps in the audit/assurance program. Controls are the primary evaluation point in the process. The audit/assurance program identifies the control objectives and the steps to determine control design and effectiveness.

Responsibilities of IT Audit and Assurance Professionals

IT audit and assurance professionals are expected to customize this document to the environment in which they are performing an assurance process. This document is to be used as a review tool and starting point. It may be modified by the IT audit and assurance professional; it is *not* intended to be a checklist or questionnaire. It is assumed that the IT audit and assurance professional has the necessary subject matter expertise required to conduct the work and is supervised by a professional with the Certified Information Systems Auditor (CISA) designation and/or necessary subject matter expertise to adequately review the work performed.

II. Using This Appendix

This audit/assurance program was developed to assist the audit and assurance professional in designing and executing a review. Details regarding the format and use of the document follow.

Work Program Steps

The first column of the program describes the steps to be performed. The numbering scheme used provides built-in work paper numbering for ease of cross-reference to the specific work paper for that section. The physical document was designed in Microsoft® Word. The IT audit and assurance professional is encouraged to make modifications to this appendix to reflect the specific environment under review.

Step 1 is part of the fact-gathering and prefieldwork preparation. Because the prefieldwork is essential to a successful and professional review, the steps have been itemized in this plan. The first level steps, e.g., 1.1, are shown in **bold** type and provide the reviewer with a scope or high-level explanation of the purpose for the substeps.

Beginning in step 2, the steps associated with the work program are itemized. To simplify the use of the program, the audit/assurance program describes the audit/assurance objective—the reason for performing the steps in the topic area; the specific controls follow. Each review step is listed below the control. These steps may include assessing the control design by walking through a process, interviewing, observing or otherwise verifying the process and the controls that address that process. In many cases, once the control design has been verified,

specific tests need to be performed to provide assurance that the process associated with the control is being followed.

The maturity assessment, which is described in more detail later in this appendix, makes up the last section of the program.

The audit/assurance plan wrap-up—those processes associated with the completion and review of work papers, preparation of issues and recommendations, report writing, and report clearing—has been excluded from this appendix because it is standard for the audit/assurance function and should be identified elsewhere in the enterprise's standards.

COBIT Cross-reference

The COBIT cross-reference provides the audit and assurance professional with the ability to refer to the specific COBIT control objective that supports the audit/assurance step. The COBIT control objective should be identified for each audit/assurance step in the section. Multiple cross-references are not uncommon. Processes at lower levels in the work program are too granular to be cross-referenced to COBIT. The audit/assurance program is organized in a manner to facilitate an evaluation through a structure parallel to the development process. COBIT provides in-depth control objectives and suggested control practices at each level. As professionals review each control, they should refer to COBIT® 4.1 or the *IT Assurance Guide: Using COBIT®* for good-practice control guidance.

COSO Components

As noted in the introduction to this appendix, COSO and similar frameworks have become increasingly popular among audit/assurance professionals. This ties the assurance work to the enterprise's control framework. While the IT audit and assurance function uses COBIT as a framework, operational audit and assurance professionals use the framework established by the enterprise. Since COSO is the most prevalent internal control framework, it has been included in this document and is a bridge to align IT audit and assurance with the rest of the audit/assurance function. Many audit/assurance organizations include the COSO control components within their reports and summarize assurance activities to the audit committee of the board of directors.

For each control, the audit and assurance professional should indicate the COSO component(s) addressed. It is possible, but generally not necessary, to extend this analysis to the specific audit step level.

The original COSO internal control framework contained five components. In 2004, COSO was revised as the *Enterprise Risk Management (ERM) Integrated Framework* and extended to eight components. The primary difference between the two frameworks is the additional focus on ERM and integration into the business decision model. ERM is in the process of being adopted by large enterprises. The two frameworks are compared in **figure B.1**.

Figure B.1—Comparison of COSO Internal Control and ERM Integrated Frameworks	
Internal Control Framework	**ERM Integrated Framework**
Control Environment: The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, management's operating style, delegation of authority systems, as well as the processes for managing and developing people in the organization.	**Internal Environment:** The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
	Objective Setting: Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.
	Event Identification: Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.
Risk Assessment: Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, and, thus, risk assessment is the identification and analysis of relevant risks to achievement of assigned objectives. Risk assessment is a prerequisite for determining how the risks should be managed.	**Risk Assessment:** Risks are analyzed, considering the likelihood and impact, as a basis for determining how they could be managed. Risk areas are assessed on an inherent and residual basis.
	Risk Response: Management selects risk responses—avoiding, accepting, reducing or sharing risk—developing a set of actions to align risks with the entity's risk tolerances and risk appetite.

Figure B.1—Comparison of COSO Internal Control and ERM Integrated Frameworks *(cont.)*	
Internal Control Framework	**ERM Integrated Framework**
Control Activities: Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.	**Control Activities:** Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
Information and Communication: Information systems play a key role in internal control systems as they produce reports, including operational, financial and compliance-related information that make it possible to run and control the business. In a broader sense, effective communication must ensure information flows down, across and up the organization. Effective communication should also be ensured with external parties, such as customers, suppliers, regulators and shareholders.	**Information and Communication:** Relevant information is identified, captured and communicated in a form and time frame that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across and up the entity.
Monitoring: Internal control systems need to be monitored—a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities or separate evaluations. Internal control deficiencies detected through these monitoring activities should be reported upstream and corrective actions should be taken to ensure continuous improvement of the system.	**Monitoring:** The entirety of enterprise risk management is monitored and modifications are made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations or both.
Information for **figure B.1** was obtained from the COSO web site, *www.coso.org/aboutus.htm.*	

The original COSO internal control framework addresses the needs of the IT audit and assurance professional: control environment, risk assessment, control activities, information and communication, and monitoring. As such, ISACA has elected to utilize the five-component model for these audit/ assurance programs. As more enterprises implement the ERM model, the additional three columns can be added, if relevant. When completing the COSO component columns, consider the definitions of the components as described in **figure B.1**.

Reference/Hyperlink

Good practices require the audit and assurance professional to create a work paper that describes the work performed, issues identified and conclusions for each line item. The reference/hyperlink is to be used to cross-reference the audit/assurance step to the work paper that supports it. The numbering system of this document provides a ready numbering scheme for the work papers. If desired, a link to the work paper can be pasted into this column.

Issue Cross-reference

This column can be used to flag a finding/issue that the IT audit and assurance professional wants to further investigate or establish as a potential finding. The potential findings should be documented in a work paper that indicates the disposition of the findings (formally reported, reported as a memo or verbal finding, or waived).

Comments

The comments column can be used to indicate the waiving of a step or other notations. It is not to be used in place of a work paper that describes the work performed.

III. Controls Maturity Analysis

One of the consistent requests of stakeholders who have undergone IT audit/assurance reviews is a desire to understand how their performance compares to good practices. Audit and assurance professionals must provide an objective basis for the review conclusions. Maturity modeling for management and control over IT processes is based on a method of evaluating the enterprise so that it can be rated from a maturity level of nonexistent (0) to optimized (5). This approach is derived from the maturity model that the Software Engineering Institute (SEI) of Carnegie Mellon University defined for the maturity of software development.

IT Assurance Guide Using COBIT Appendix VII—Maturity Model for Internal Control, shown in **figure B.2**, provides a generic maturity model that shows the status of the internal control environment and the establishment of internal controls in an enterprise. It shows how the management of internal control, and an awareness of the need to establish better internal controls, typically develops from an ad hoc to an optimized level. The model provides a high-level guide to help COBIT users appreciate what is required for effective internal controls in IT and to help position their enterprise on the maturity scale.

Figure B.2—Maturity Model for Internal Control

Maturity Level	Status of the Internal Control Environment	Establishment of Internal Controls
0 Non-existent	There is no recognition of the need for internal control. Control is not part of the organization's culture or mission. There is a high risk of control deficiencies and incidents.	There is no intent to assess the need for internal control. Incidents are dealt with as they arise.
1 Initial/*ad hoc*	There is some recognition of the need for internal control. The approach to risk and control requirements is ad hoc and disorganized, without communication or monitoring. Deficiencies are not identified. Employees are not aware of their responsibilities.	There is no awareness of the need for assessment of what is needed in terms of IT controls. When performed, it is only on an *ad hoc* basis, at a high level and in reaction to significant incidents. Assessment addresses only the actual incident.

Figure B.2—Maturity Model for Internal Control *(cont.)*		
Maturity Level	**Status of the Internal Control Environment**	**Establishment of Internal Controls**
2 Repeatable but Intuitive	Controls are in place but are not documented. Their operation is dependent on the knowledge and motivation of individuals. Effectiveness is not adequately evaluated. Many control weaknesses exist and are not adequately addressed; the impact can be severe. Management actions to resolve control issues are not prioritized or consistent. Employees may not be aware of their responsibilities.	Assessment of control needs occurs only when needed for selected IT processes to determine the current level of control maturity, the target level that should be reached and the gaps that exist. An informal workshop approach, involving IT managers and the team involved in the process, is used to define an adequate approach to controls for the process and to motivate an agreed-upon action plan.
3 Defined	Controls are in place and adequately documented. Operating effectiveness is evaluated on a periodic basis and there is an average number of issues. However, the evaluation process is not documented. While management is able to deal predictably with most control issues, some control weaknesses persist and impacts could still be severe. Employees are aware of their responsibilities for control.	Critical IT processes are identified based on value and risk drivers. A detailed analysis is performed to identify control requirements and the root cause of gaps and to develop improvement opportunities. In addition to facilitated workshops, tools are used and interviews are performed to support the analysis and ensure that an IT process owner owns and drives the assessment and improvement process.
4 Managed and Measurable	There is an effective internal control and risk management environment. A formal, documented evaluation of controls occurs frequently. Many controls are automated and regularly reviewed. Management is likely to detect most control issues, but not all issues are routinely identified. There is consistent follow-up to address identified control weaknesses. A limited, tactical use of technology is applied to automate controls.	IT process criticality is regularly defined with full support and agreement from the relevant business process owners. Assessment of control requirements is based on policy and the actual maturity of these processes, following a thorough and measured analysis involving key stakeholders. Accountability for these assessments is clear and enforced. Improvement strategies are supported by business cases. Performance in achieving the desired outcomes is consistently monitored. External control reviews are organized occasionally.

Figure B.2—Maturity Model for Internal Control *(cont.)*		
Maturity Level	**Status of the Internal Control Environment**	**Establishment of Internal Controls**
5 Optimized	An enterprise-wide risk and control program provides continuous and effective control and risk issues resolution. Internal control and risk management are integrated with enterprise practices, supported with automated real-time monitoring with full accountability for control monitoring, risk management and compliance enforcement. Control evaluation is continuous, based on self-assessments and gap and root cause analyses. Employees are proactively involved in control improvements.	Business changes consider the criticality of IT processes and cover any need to reassess process control capability. IT process owners regularly perform self-assessments to confirm that controls are at the right level of maturity to meet business needs and they consider maturity attributes to find ways to make controls more efficient and effective. The organization benchmarks to external best practices and seeks external advice on internal control effectiveness. For critical processes, independent reviews take place to provide assurance that the controls are at the desired level of maturity and working as planned.

The maturity model evaluation is one of the final steps in the evaluation process. The IT audit and assurance professional can address the key controls within the scope of the work program and formulate an objective assessment of the maturity levels of the control practices. The maturity assessment can be a part of the audit/assurance report and can be used as a metric from year to year to document progression in the enhancement of controls. However, it must be noted that the perception of the maturity level may vary between the process/IT asset owner and the auditor. Therefore, an auditor should obtain the concerned stakeholder's concurrence before submitting the final report to management.

At the conclusion of the review, once all findings and recommendations are completed, the professional assesses the current state of the COBIT control framework and assigns it a maturity level using the six-level scale. Some practitioners utilize decimals (x.25, x.5, x.75) to indicate gradations in the maturity model. As a further reference, COBIT provides a definition of the maturity designations by control objective. While this approach is not mandatory, the process is provided as a separate section at the end of the audit/assurance program for those enterprises that wish to implement it. It is suggested that a maturity assessment be made at the COBIT control level. To provide further value to the client/customer, the professional can also obtain maturity targets from the client/customer. Using the assessed and target maturity levels, the professional can create an effective graphic presentation that describes the achievement or gaps between the actual and targeted maturity goals. A graphic is provided as the last page of the document (section VIII), based on sample assessments.

IV. Assurance and Control Framework

ISACA IT Assurance Framework and Standards

ITAF section 3630.6—Outsourced and Third-Party Activities—is of primary relevance to the audit and assurance of information security management. However, outsourcing, especially in a cloud environment (described later) is pervasive throughout the IT organization and its functional responsibility. Therefore, the subsections contained in ITAF section 3630—General IT Controls have varying levels of relevance, depending on the cloud computing design.

ISACA Controls Framework

COBIT is a framework for the governance of IT and is a supporting tool set that allows managers to bridge the gap among control requirements, technical issues and business risk. COBIT enables clear policy development and good practice for IT control throughout enterprises.

Utilizing COBIT as the control framework from which IT audit and assurance activities are based aligns IT audit and assurance with good practices as developed by the enterprise.

Cloud computing affects the entire IT and business unit functions. COBIT IT processes PO9 *Assess and manage IT risks* from the Plan and Organize (PO) domain; DS1 *Define and manage service levels*, DS2 *Manage third-party services*, DS4 *Ensure continuous service*, DS5 *Ensure systems security*, DS8 *Manage service desk and incidents*, DS9 *Manage the configuration*, and DS11 *Manage data* from the Deliver and Support (DS) domain; and ME2 *Monitor and evaluate internal control* and ME3 *Ensure compliance with external requirements* from the Monitor and Evaluate (ME) domain are the primary control frameworks and address good practices for managing third-party relationships. Secondary COBIT processes are cross-referenced within the audit/assurance program.

Cloud computing has touch points with the entire IT infrastructure. *Cloud Computing Management Audit/Assurance Program* cross-references numerous COBIT domains and processes. These sections appear in the COBIT cross-reference column of the audit/assurance program.

Refer to ISACA publication *COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*, published in 2007, for the related control practice value and risk drivers.

V. Executive Summary of Audit/Assurance Focus

Cloud Computing Management

The US National Institute of Standards and Technology (NIST) and the Cloud Security Alliance define cloud computing as a "model for enabling convenient, on-demand network access to a shared pool of configurable computing resources

(e.g., networks, servers, storage, applications, services) that can be provisioned and released with minimal management effort or service provider interactions."[13] In other words, IT services are delivered using a utility model.

Cloud computing uses three basic service models:
- **Infrastructure as a Service (IaaS)**—Capability to provision processing, storage, networks and other fundamental computing resources that offer 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. The primary difference between this approach and traditional outsourcing is that with cloud computing, access to the infrastructure is through the public or private networks and the assignment and payment for resources is based on usage.
- **Platform as a Service (PaaS)**—Capability to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages and tools supported by the provider
- **Software as a Service (SaaS)**—Capability to use the provider's applications that run on the 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).

Cloud computing utilizes the following deployment models:
- **Private cloud:**
  - Operated solely for an organization
  - May be managed by the organization or a third party
  - May exist on or off premise
- **Community cloud:**
  - Shared by several organizations
  - Supports a specific community that has a shared mission or interest
  - May be managed by the organizations or a third party
  - May reside on or off premise
- **Public cloud:**
  - Made available to the general public or a large industry group
  - Owned by an organization that sells cloud services
- **Hybrid cloud:**
  - Composed 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)

The key benefits to the customer include:
- Cost containment
- Immediate provisioning (setting up) of resources
- Servicer load balancing to maximize availability
- Ability to dynamically adjust resources according to demand with little notice

[13] ISACA, *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*, USA, 2009

- Ability of the customer to focus on core competencies instead of devoting resources to IT operations
- Mirrored solutions to minimize the risk of downtime

Business Impact and Risk

Applications processed in the cloud have similar implications for the business as traditional outsourcing. These include:

- Loss of business focus
- Solution failing to meet business and/or user requirements; not performing as expected; or not integrating with strategic IT plan, information architecture and technology direction
- Incorrect solution selected or significant missing requirements
- Contractual discrepancies and gaps between business expectations and service provider capabilities
- Control gaps between processes performed by the service provider and the organization
- Compromised system security and confidentiality
- Invalid transactions or transactions processed incorrectly
- Costly compensating controls
- Reduced system availability and questionable integrity of information
- Poor software quality, inadequate testing and high number of failures
- Failure to respond to relationship issues with optimal and approved decisions
- Insufficient allocation of resources
- Unclear responsibilities and accountabilities
- Inaccurate billings
- Litigation, mediation or termination of the agreement, resulting in added costs and/or business disruption and/or total loss of the organization
- Inability to satisfy audit/assurance charter and requirements of regulators or external auditors
- Reputation
- Fraud

Cloud computing has additional risk:

- Greater dependency on third parties:
  - Increased vulnerabilities in external interfaces
  - Increased risk in aggregated data centers
  - Immaturity of the service providers with the potential for service provider going concern issues
  - Increased reliance on independent assurance processes
- Increased complexity of compliance with laws and regulations:
  - Greater magnitude of privacy risk
  - Transborder flow of personally identifiable information
  - Affecting contractual compliance
- Reliance on the Internet as the primary conduit to the organization's data introduces:
  - Security issues with a public environment
  - Availability issues of Internet connectivity

- Due to the dynamic nature of cloud computing:
  - The location of the processing facility may change according to load balancing
  - The processing facility may be located across international boundaries
  - Operating facilities may be shared with competitors
  - Legal issues (liability, ownership, etc.) relating to differing laws in hosting countries may put data at risk

Objective and Scope

Objective—The cloud computing audit/assurance review will:

- Provide stakeholders with an assessment of the effectiveness of the cloud computing service provider's internal controls and security
- Identify internal control deficiencies within the customer organization and its interface with the service provider
- Provide audit stakeholders with an assessment of the quality of and their ability to rely on the service provider's attestations regarding internal controls

The cloud computing audit/assurance review is not designed to replace or focus on audits that provide assurance of specific application processes and excludes assurance of an application's functionality and suitability.

Scope—The review will focus on:

- The governance affecting cloud computing
- The contractual compliance between the service provider and customer
- Control issues specific to cloud computing

Since the areas under review rely heavily on the effectiveness of core IT general controls, it is recommended that audit/assurance reviews of the following areas be performed prior to the execution of the cloud computing review, so that appropriate reliance can be placed on these assessments:

- Identity management (if the organization's identity management system is integrated with the cloud computing system)
- Security incident management (to interface with and manage cloud computing incidents)
- Network perimeter security (as an access point to the Internet)
- Systems development (in which the cloud is part of the application infrastructure)
- Project management
- IT risk management
- Data management (for data transmitted and stored on cloud systems)
- Vulnerability management

Minimum Audit Skills

Cloud computing incorporates many IT processes. Since the focus is on information governance, IT management, network, data, contingency and encryption controls, the audit and assurance professional should have the requisite knowledge of these issues. In addition, proficiency in risk assessment, information security components of IT architecture, risk management, and the threats and vulnerabilities

of cloud computing and Internet-based data processing is required. Therefore, it is recommended that the audit and assurance professional conducting the assessment has the requisite experience and organizational relationships to effectively execute the assurance processes. Because cloud computing is dependent on web services, the auditor should have at least a basic understanding of Organization for the Advancement of Structured Information Standards (OASIS) Web Services Security (WS-Security or WSS) Standards (*www.oasis-open.org*).

VI. Audit/Assurance Program

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
1. PLANNING AND SCOPING THE AUDIT									
1.1 Define the audit/assurance objectives. The audit/assurance objectives are high level and describe the overall audit goals.									
1.1.1 Review the audit/assurance objectives in the introduction to this audit/assurance program.									
1.1.2 Modify the audit/assurance objectives to align with the audit/assurance universe, annual plan and charter.									
1.2 Define the boundaries of review. The review must have a defined scope. Understand the core business process and its alignment with IT, in its noncloud form and current or future cloud implementation.									
1.2.1 Obtain a description of all cloud computing environments in use and under consideration.									
1.2.2 Obtain a description of all cloud computing applications in use and under consideration.									
1.2.3 Identify the types of cloud services (IaaS, PaaS, SaaS) in use and under consideration, and determine the services and business solutions to be included in the review.									
1.2.4 Obtain and review any previous audit reports with remediation plans. Identify open issues, and assess updates to the documents with respect to these issues.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
1. PLANNING AND SCOPING THE AUDIT *(cont.)*									
1.3 Identify and document risk. The risk assessment is necessary to evaluate where audit resources should be focused. In most enterprises, audit resources are not available for all processes. The risk-based approach assures utilization of audit resources in the most effective manner.									
1.3.1 Identify the business risk associated with cloud computing of concern to business owners and key stakeholders.									
1.3.2 Verify that the business risk is aligned, rated or classified with cloud computing security criteria such as confidentiality, integrity and availability.									
1.3.3 Review previous audits of cloud computing.									
1.3.4 Determine if the risk identified previously has been appropriately addressed.									
1.3.5 Evaluate the overall risk factor for performing the review.									
1.3.6 Based on the risk assessment, identify changes to the scope.									
1.3.7 Discuss the risk with IT management, and adjust the risk assessment.									
1.3.8 Based on the risk assessment, revise the scope.									
1.4 Define the change process. The initial audit approach is based on the reviewer's understanding of the operating environment and associated risk. As further research and analysis are performed, changes to the scope and approach may result.									
1.4.1 Identify the senior IT assurance resource responsible for the review.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
1. PLANNING AND SCOPING THE AUDIT *(cont.)*									
1.4.2 Establish the process for suggesting and implementing changes to the audit/assurance program and the authorizations required.									
1.5 Define assignment success. The success factors need to be identified. Communication among the IT audit/assurance team, other assurance teams and the enterprise is essential.									
1.5.1 Identify the drivers for a successful review (this should exist in the assurance function's standards and procedures).									
1.5.2 Communicate success attributes to the process owner or stakeholder, and obtain agreement.									
1.6 Define the audit/assurance resources required. The audit/assurance resources required for a successful review need to be defined. (Refer to the Minimum Audit Skills section in section V.)									
1.6.1 Determine the audit/assurance skills necessary for the review.									
1.6.2 Estimate the total audit/assurance resources (hours) and time frame (start and end dates) required for the review.									
1.7 Define deliverables. The deliverable is not limited to the final report. Communication between the audit/assurance teams and the process owner about the number, format, timing and nature of deliverables is essential to assignment success.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
1. PLANNING AND SCOPING THE AUDIT *(cont.)*									
1.7.1 Determine the interim deliverables, including initial findings, status reports, draft reports, due dates for responses or meetings, and the final report.									
1.8 Communications The audit/assurance process must be clearly communicated to the customer/client.									
1.8.1 Conduct an opening conference to discuss: • Review objectives with the stakeholders • Documents and information security resources required to effectively perform the review • Timelines and deliverables									
2. GOVERNING THE CLOUD									
2.1 Governance and Enterprise Risk Management (ERM)									
2.1.1 Governance Audit/Assurance Objective: Governance functions are established to ensure effective and sustainable management processes that result in transparency of business decisions, clear lines of responsibility, information security in alignment with regulatory and customer organization standards, and accountability.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2. GOVERNING THE CLOUD *(cont.)*									
2.1.1.1 Governance Model Control: The organization has mechanisms in place to identify all providers and brokers of cloud services with which it currently does business and all cloud deployments that exist across the enterprise. The organization ensures that customer, IT, information security and business units actively participate in the governance and policy activities to align business objectives and information security capabilities of the service provider with those of the organization.	DS5.1 ME1.5 ME4.1 ME4.2	X		X	X	X			
2.1.1.1.1 Determine if the IT, information security and key business functions have defined integrated governance framework and monitoring processes.									
2.1.1.1.2 Determine if the IT, information security functions and key business units are actively involved in the establishment of SLAs and contractual obligations.									
2.1.1.1.3 Determine if the information security function has performed a gap analysis of the service provider's information security capabilities against the organization's information security policies and threat and vulnerabilities/IT risk emanating from the transition to cloud computing.									
2.1.1.1.4 Determine if the cloud provider has identified control objectives for the provided services.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2. GOVERNING THE CLOUD *(cont.)*									
2.1.1.1.5 Determine if the organization maintains an inventory of all services provided via the cloud.									
2.1.1.1.6 Determine that the business cannot procure cloud services without the involvement of IT and information security.									
2.1.1.2 Information Security Collaboration Control: Both parties define the reporting relationship and responsibilities.	PO4.5 PO4.6 PO4.14 DS2.2 ME2.1	x		x	x	x			
2.1.1.2.1 Determine if the responsibilities for governance are documented and approved by the service provider and customer.									
2.1.1.2.2 Determine if reporting relationships between the service provider and customer are clearly defined, identifying the responsibilities of both organizations' governance processes.									
2.1.1.3 Metrics and SLAs Control: SLAs that support the business requirements are defined, accepted by the service provider and monitored.	PO4.8 DS1.2 DS1.3 DS1.5 DS1.6 DS2.4	x		x		x			

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2. GOVERNING THE CLOUD *(cont.)*									
2.1.1.3.1 Obtain the SLAs; determine if the SLAs reflect the business requirements.									
2.1.1.3.2 Determine that the SLAs can be monitored using measurable metrics and that the metrics provide appropriate oversight and early warning of unacceptable performance.									
2.1.1.3.3 Determine if the SLA contains clauses that ensure services in case of vendor acquisition or changes in management.									
2.1.2 Enterprise Risk Management Audit/Assurance Objective: Risk management practices are implemented to evaluate inherent risk within the cloud computing model, identify appropriate control mechanisms, and ensure that residual risk is within acceptable levels.									
2.1.2.1 Identification of Risk Control: The risk management process provides a thorough assessment of the risk to the business by implementing the cloud processing model and is aligned to ERM if applicable.	PO9.3 PO9.5 ME4.2 ME4.5	X	X	X					
2.1.2.1.1 Determine if the organization has an ERM model.									
2.1.2.1.2 If an ERM model has been implemented, determine if the cloud computing risk assessment is in alignment with the enterprise ERM.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2. GOVERNING THE CLOUD *(cont.)*									
2.1.2.1.3 Determine if the services provided by the service provider and the processing model selected will limit the availability or execution of required information security activities, such as: • Restrictions on vulnerability assessments and penetration testing • Availability of audit logs • Access to activity monitoring reports • Segregation of duties									
2.1.2.1.4 Determine if the risk management approach includes the following: • Identification and valuation of assets and services • Identification and analysis of threats and vulnerabilities with their potential impact on assets • Analysis of the likelihood of events using a scenario approach • Documented management approval of risk acceptance levels and criteria • Risk action plans (control, avoid, transfer, accept)									
2.1.2.1.5 Determine if, during the risk assessment, the identified assets include both service-provider- and customer-owned assets and if the information security classifications used in the risk assessments are aligned.									
2.1.2.1.6 Determine if the risk assessment includes the service model and the service provider's capabilities and financial condition.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2. GOVERNING THE CLOUD *(cont.)*									
2.1.2.2 Integration of Risk and SLAs Control: SLAs are aligned and developed in conjunction with the results of the risk assessment.	PO9.3 PO9.4 DS1.1 DS1.2 DS1.3 DS1.4 DS1.5 DS2.3 DS2.4 DS2.5	x	x	x					
2.1.2.2.1 Determine if the results of the risk action plans are incorporated into the SLAs.									
2.1.2.2.2 Determine if a joint service provider/customer risk assessment was conducted to verify if all reasonable risk has been identified and if risk remediation alternatives were identified and documented.									
2.1.2.2.3 Where the risk assessment of the service provider has identified risk management that is either ineffective or not comprehensive, determine if the organization has performed an analysis of their compensating controls and if such controls will address the service provider's control shortcomings.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2. GOVERNING THE CLOUD *(cont.)*									
2.1.2.3 Acceptance of Risk Control: Risk acceptance is approved by a member of management with the authority to accept the risk on behalf of the organization and who understands the implications of the decision.	PO9.3 PO9.4 PO9.5 ME4.5	x	x						
2.1.2.3.1 Determine if management has performed an analysis of their quantification and acceptance of residual risk prior to implementing a cloud solution.									
2.1.2.3.2 Determine if the individual accepting such risk has the authority to make this decision.									
2.1.3 Information Risk Management Audit/Assurance Objective: A process to manage information risk exists and is integrated into the organization's overall ERM framework. Information risk management information and metrics are available for the information security function to manage risk within the risk tolerance of the data owner.									
2.1.3.1 Risk Management Framework and Maturity Model Control: A risk management framework and a maturity model have been implemented to quantify risk and assess the effectiveness of the risk model.	PO9.1 PO9.2 PO9.3 PO9.4 DS5.1 ME4.5	x	x	x					
2.1.3.1.1 Determine if a risk framework has been identified and approved.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2. GOVERNING THE CLOUD *(cont.)*									
2.1.3.1.2 Determine if a maturity model is used to assess the effectiveness.									
2.1.3.1.3 Review the results of the maturity model results, and determine if the lack of maturity materially affects the audit objectives.									
2.1.3.2 Risk Management Controls Control: Risk management controls are in effect to manage risk-based decisions.	PO9.3 PO9.4 PO9.5 PO9.6	x	x	x					
2.1.3.2.1 Identify the technology controls and contractual requirements necessary to make fact-based information risk decisions. Consider: • Information usage • Access controls • Security controls • Location management • Privacy controls									
2.1.3.2.2 For SaaS, determine that the organization has identified analytical information required from the service provider to support contractual obligations relating to performance, security and attainment of SLAs.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2. GOVERNING THE CLOUD *(cont.)*									
2.1.3.2.3 Obtain the analytical data requirements, and determine if the organization routinely monitors and evaluates the attainment of SLAs.									
2.1.3.2.4 For PaaS, determine that the organization has identified the information available and the control practices necessary to manage the application and development processes effectively that address availability, confidentiality, data ownership, concerns around e-discovery, privacy and legal issues.									
2.1.3.2.5 Determine if the organization has established monitoring practices to identify risk issues.									
2.1.3.2.6 For IaaS, determine that the organization has identified and monitors the control and security processes necessary to provide a secure operating environment.									
2.1.3.2.7 Determine if the service provider makes available metrics and controls to assist customers in implementing their information risk management requirements.									
2.1.4 Third-party Management Audit/Assurance Objective: The customer recognizes the outsourced relationship with the service provider. The customer understands its responsibilities for controls, and the service provider has provided assurances of sustainability of those controls.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2. GOVERNING THE CLOUD *(cont.)*									
2.1.4.1 Service Provider Procedures Control: The service provider makes available to customers independent third-party assessments, using generally accepted audit procedures, to describe the control practices in place at the service provider's operating locations.	DS2.2 ME2.5 ME2.6			X	X	X			
2.1.4.1.1 Determine if the service provider routinely has independent third-party assessments performed and issued.									
2.1.4.1.2 Determine if the scope of the third-party assessment includes descriptions of the following service provider processes: • Incident management • Business continuity and disaster recovery • Backup and co-location facilities									
2.1.4.1.3 Determine if the service provider routinely performs internal assessments of conformance to its own policies, procedures and availability of control metrics.									
2.1.4.2 Service Provider Responsibilities Control: The service provider has established processes to align its operations with requirements of the customer.	DS2.2 ME2.5 ME2.6	X		X					

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2. GOVERNING THE CLOUD *(cont.)*									
2.1.4.2.1 Determine if the service provider's information security governance, risk management and compliance processes are routinely assessed and include: • Risk assessments and reviews of facilities and services for control weaknesses • Definition of critical service and information security success factors and key performance indicators • Frequency of assessments • Mitigation procedures to ensure timely completion of identified issues • Review of legal, regulatory, industry and contractual requirements for comprehensiveness • Cloud service provider's oversight of risk from its own critical vendors • Terms of use due diligence to identify roles, responsibilities and accountability of the service provider • Legal review for local contract provisions, enforceability and laws pertaining to jurisdictional issues that are the responsibility of their service provider									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2. GOVERNING THE CLOUD *(cont.)*									
2.1.4.3 Customer Responsibilities Control: The customer performs due diligence processes to ensure sustainability and compliance with regulatory requirements.	DS4.2 DS4.4 DS4.5 ME2.6 ME3.1 ME3.3 ME3.4	x		x		x			
2.1.4.3.1 Determine if the customer has performed due diligence with respect to the service provider's information security governance, risk management and compliance processes as described under 2.1.4.2 Service Provider Responsibilities.									
2.1.4.3.2 Determine if the customer has prepared for the loss of service provider services including: • A business continuity and disaster recovery plan for various processing interruption scenarios • Tests of the business continuity and disaster plan • Inclusion of the business users and their business impact analysis in the continuity plan									
2.2 Legal and Electronic Discovery									
2.2.1 Contractual Obligations Audit/Assurance Objective: The service provider and customer establish bilateral agreements and procedures to ensure contractual obligations are satisfied, and these obligations address the compliance requirements of both the customer and service provider.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2. GOVERNING THE CLOUD *(cont.)*									
2.2.1.1 Contract Terms Control: A contract team representing the customer's legal, financial, information security and business units has identified and included required contractual issues in the contract from the customer's perspective, and the service provider's legal team has provided contractual assurance to the satisfaction of the customer.	DS1.6 DS2.2 DS2.4 ME2.5 ME2.6 ME3.1			X					
2.2.1.1.1 Determine if the contractual agreement defines both parties' responsibilities related to discovery searches, litigation holds, preservation of evidence and expert testimony.									
2.2.1.1.2 Determine that the service provider contract requires assurance to the customer that their data are preserved as recorded, including the primary data and secondary information (metadata and logs).									
2.2.1.1.3 Determine that service providers understand their contractual obligations to provide guardianship of the customer's data. Review contracts to determine this is specifically addressed.									
2.2.1.1.4 Determine that the customer's duty of care includes full scope of contract monitoring, including: • Precontract due diligence • Contract term negotiation • Transfer of data custodianship • Contract termination or renegotiation • Transition from processing									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2. GOVERNING THE CLOUD *(cont.)*									
2.2.1.1.5 Determine that the contract stipulates and both parties understand their obligations for both expected and unexpected termination of the relationship during and after negotiations and that the contract and/or precontract agreement provides for the orderly and timely return or secure disposal of assets.									
2.2.1.1.6 Determine that the contractual obligations specifically identify suspected data breach responsibilities of both parties and cooperative processes to be implemented during the investigation and any follow-up actions.									
2.2.1.1.7 Determine that the agreement provides for the customer to have access to the service provider's performance and tests for vulnerabilities on a regular basis.									
2.2.1.1.8 Determine that the contract establishes rights and obligations for both parties during transition at the conclusion of the relationship and after the contract terminates.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2. GOVERNING THE CLOUD *(cont.)*									
2.2.1.1.9 Determine if the contract establishes the following data protection processes: • Full disclosure of the service provider's internal security practices and procedures • Data retention policies in conformance with local jurisdiction requirements • Reporting on geographical location of customer data • Circumstances in which data can be seized and notification of any such events • Notification of subpoena or discovery concerning any customer data or processes • Penalties for data breaches • Protection against data contamination between customers (compartmentalization)									
2.2.1.1.10 Encryption requirements for data in transit, at rest and for backup are clearly identified in the cloud contractual agreement.									
2.2.1.2 Implementation of Contractual Requirements Control: The customer has implemented appropriate monitoring controls to ensure contractual obligations are satisfied.	DS1.5 DS1.6 DS2.4 ME2.5 ME2.6			x					

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2. GOVERNING THE CLOUD *(cont.)*									
2.2.1.2.1 Determine that the customer has considered and established controls within the contractual obligations to ensure retention of data and intellectual property ownership and the privacy of personal data contained within its data.									
2.2.1.2.2 Determine that the customer has developed appropriate issue monitoring processes to oversee the service provider's performance of contract requirements.									
2.2.1.2.3 Determine that the customer has established internal issue monitoring to identify customer contractual compliance deficiencies.									
2.2.2 Legal Compliance Audit/Assurance Objective: Legal issues relating to functional, jurisdictional and contractual requirements are addressed to protect both parties, and these issues are documented, approved and monitored.									
2.2.2.1 Legal Compliance Control: Legal compliance to local and cross-border laws are defined as a component of the contract.	DS1.6 ME3.1			x					
2.2.2.1.1 Determine if cross-border and local laws are defined and considered in the contract.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2. GOVERNING THE CLOUD *(cont.)*									
2.2.2.1.2 Determine if the service provider and customer have an agreed-upon unified process for responding to subpoenas, service of process, and other legal requests.									
2.3 Compliance and Audit									
2.3.1 Right to Audit Audit/Assurance Objective: The right to audit is clearly defined and satisfies the assurance requirements of the customer's board of directors, audit charter, external auditors and any regulators having jurisdiction over the customer.									
2.3.1.1 Audit Rights per Contract Control: The audit rights, as agreed in the contract, permit the customer to conduct professional control assessments.	ME2.5 ME2.6 ME3.1 ME3.3 ME3.4			X	X	X			
2.3.1.1.1 Review the audit rights in the contract, and determine if audit activities can be restricted or curtailed by the service provider.									
2.3.1.1.2 If audit rights issues are identified, prepare an appropriate summary of the findings and escalate to service provider relationship management. If necessary and appropriate, escalate to the audit committee.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2. GOVERNING THE CLOUD *(cont.)*									
2.3.1.2 Third-party Reviews Control: The service provider submits third-party reviews that satisfy the professional requirements of being performed by a recognized independent audit organization. The report describes the controls in place by the service provider and certifies that the controls have been tested using recognized selection criteria. A test period previously agreed upon provides a description of recommended customer and service provider responsibilities and controls.									
2.3.1.2.1 Obtain the third-party report.									
2.3.1.2.2 Determine that the report addresses the control environment utilized by the customer.									
2.3.1.2.3 Determine that the descriptions and processes are relevant to the service provider's customers.									
2.3.1.2.4 Determine that the report has described the key controls necessary for the reviewer to assess compliance with appropriate control objectives.									
2.3.1.2.5 Determine that the report and testing will satisfy the customer's assurance charter and compliance requirements of all regulators having jurisdiction over the customer.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2. GOVERNING THE CLOUD *(cont.)*									
2.3.1.2.6 Using the approved customer audit universe, compare the scope of the audit universe to the scope of the third-party report; identify gaps in the latter requiring additional assurance coverage.									
2.3.1.2.7 Determine if the service provider relationship crosses international boundaries and if this affects the ability to rely upon the third-party report.									
2.3.2 Auditability Audit/Assurance Objective: The service provider's operating environment should be subject to audit to satisfy the customer's audit charter, compliance requirements and good practice controls without restriction.									
2.3.2.1 Customer Assurance Reviews of Service Provider Processes Control: The customer performs appropriate reviews to supplement and/or replace third-party reviews as required by their audit universe and audit charter.	DS2.3 DS2.4 ME2.1 ME2.5 ME2.6 ME3.1 ME3.3 ME3.4	x		x	x	x			
2.3.2.1.1 Determine if supplementary assurance assessments (if a third-party review has been provided) or primary assurance assessments are required.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2. GOVERNING THE CLOUD *(cont.)*									
2.3.2.1.2 Generate appropriate requests to the service provider, and schedule reviews. Note: Utilize appropriate audit/assurance programs for these reviews.									
2.3.3 Compliance Scope Audit/Assurance Objective: The use of cloud computing does not invalidate or violate any customer compliance agreement.									
2.3.3.1 Feasibility of Data Security Compliance Control: Data regulations are identified by compliance topic and are mapped to the regulator's requirements. Gaps are evaluated to determine if the cloud computing platform will invalidate or breach compliance requirements.	ME3.1 ME3.2 ME3.3	x		x		x			
2.3.3.1.1 Determine if the customer has identified the legal and regulatory requirements of which it must comply (i.e., EU Data Directive, PCAOB AS5, PCI DSS, HIPAA).									
2.3.3.1.2 Determine if the customer has aggregated requirements to minimize duplication.									
2.3.3.1.3 Using the documentation assembled in the Governance and Enterprise Risk Management, Legal and Electronic Discovery, and Right to Audit sections, perform a gap analysis against the data regulations to determine if there are any regulatory requirements that cannot be satisfied by the cloud computing model.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2. GOVERNING THE CLOUD *(cont.)*									
2.3.3.2 Data Protection Responsibilities Control: The deployment scenario (IaaS, PaaS, SaaS) defines the data protection responsibilities between the customer and service provider, and these responsibilities are clearly established contractually.	DS2.2 DS5.1 DS11.6			x					
2.3.3.2.1 Determine that the responsibilities for data protection are based on the risk for the deployment scenario.									
2.3.3.2.2 Review the contract to determine the assignment of responsibilities.									
2.3.3.2.3 Based on the contract, determine if the customer and service provider each have established appropriate data protection measures within the scope of their responsibilities.									
2.3.4 ISO 27001 Certification Audit/Assurance Objective: Service provider security assurance is provided through ISO 27001 Certification.	DS5.1 ME2.6 ME2.7 ME3.4			x					
2.3.4.1 ISO Information Security Certification Control: ISO 27001 certification provides assurance of the service provider's adherence to best-practice security processes.									
2.3.4.1.1 Determine if the service provider has received ISO 27001 certification. If so, adjust the scope of the audit/assurance program to reflect this certification.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2. GOVERNING THE CLOUD *(cont.)*									
2.4 Portability and Interoperability									
2.4.1 Service Transition Planning Audit/Assurance Objective: Planning for the migration of data, such as formats and access, is essential to reducing operational and financial risk at the end of the contract. The transition of services should be considered at the beginning of contract negotiations.									
2.4.1.1 Portability Control: Procedures, capabilities and alternatives are established, maintained and tested, and a state of readiness has been established to transfer cloud computing operations to an alternate service provider in the event that the selected service provider is unable to meet contractual requirements or ceases operations.	PO2.1 PO4.1 PO4.2 PO4.4 PO4.5			X					
2.4.1.1.1 All cloud solutions									
2.4.1.1.1.1 Determine that the hardware and software requirements and feasibility for moving from the existing service provider (legacy provider) to another provider (new provider) have been documented for each cloud computing initiative.									
2.4.1.1.1.2 Determine that an alternate service provider for each legacy service provider has been identified and that the feasibility for transferring processes has been evaluated.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2. GOVERNING THE CLOUD *(cont.)*									
2.4.1.1.1.3 Determine if the feasibility analysis includes procedures and time estimates to move large volumes of data, if applicable.									
2.4.1.1.1.4 Determine if the portability process has been tested.									
2.4.1.1.2 IaaS cloud solutions									
2.4.1.1.2.1 Determine if the feasibility analysis of transferring from the IaaS legacy service provider involves any proprietary functions or processes that would preclude or delay the transferring of operations.									
2.4.1.1.2.2 Determine if the portability analysis includes processes to protect the intellectual property and data from the legacy service provider once the transfer has been completed.									
2.4.1.1.3 PaaS cloud solutions									
2.4.1.1.3.1 Determine if the feasibility analysis includes identification of application components and modules that are proprietary and would require special programming during transfer.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2. GOVERNING THE CLOUD *(cont.)*									
2.4.1.1.3.2 Determine if the portability analysis includes: • Translation functions to a new service provider • Interim processing until a new service provider is operational • Testing of new processes before promotion to a production environment at the new service provider									
2.4.1.1.4 SaaS cloud solutions									
2.4.1.1.4.1 Determine if the portability analysis includes: • A plan to back up the data in a format that is usable by other applications • Routine backup of data • Identification of custom tools required to process the data and plans to redevelop • Testing of the new service provider's application and due diligence before conversion									
3. OPERATING IN THE CLOUD									
3.1 Incident Response, Notification and Remediation Audit/Assurance Objective: Incident notifications, responses, and remediation are documented, timely, address the risk of the incident, escalated as necessary and are formally closed.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
3. OPERATING IN THE CLOUD *(cont.)*									
3.1.1 Incident Response Control: The contract SLAs describe specific definitions of incidents (data breaches, security violations) and events (suspicious activities) and the actions to be initiated by and the responsibilities of both parties.	DS1.5 DS1.6 DS2.2 DS2.4 DS5.6 DS8.1 DS8.2 DS8.3 DS8.4			X		X			
3.1.1.1 Obtain and review the SLAs per the contract to determine that incidents and events are clearly defined and responsibilities assigned.									
3.1.1.2 Review cooperation agreements, and evaluate the responsibilities for the investigation of incidents.									
3.1.1.3 Notification procedures according to local laws are incorporated into the incident and event process.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
3. OPERATING IN THE CLOUD *(cont.)*									
3.1.2 Service Provider Issue Monitoring Control: Issue monitoring processes are implemented and actively used by the service provider to document and report all defined incidents.	DS1.5 DS1.6 DS2.2 DS2.3 DS2.4 DS5.6 DS8.1 DS8.2 DS8.3 DS8.4		X	X		X			
3.1.2.1 Obtain and review the service provider's issue monitoring procedures.									
3.1.2.2 Determine if the monitored reporting requirements are aligned with the customer's incident reporting policy.									
3.1.2.3 Obtain the incident monitoring reports for a representative period of time.									
3.1.2.3.1 Determine that the: • Customer was notified of the incident within the SLA requirements • Remediation was timely based on the scope and risk of the incident • Remediation was appropriate • Issue was escalated, if appropriate • Issue was closed and the customer notified in a timely manner									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
3. OPERATING IN THE CLOUD *(cont.)*									
3.1.3 Customer Issue Monitoring Control: The customer has established an issue monitoring process to track internal and service provider incidents.	DS5.6 DS8.1 DS8.2 DS8.3 DS8.4 DS8.5 ME2.3			X		X			
3.1.3.1 Obtain the customer incident monitoring procedure.									
3.1.3.2 Determine if the incident monitoring procedure tracks both internal and service provider incidents.									
3.1.3.3 Select a sample of incidents, and determine that: • The service provider notified the customer on a timely basis within scope of the contract. • The remediation was timely based on the scope and risk of the incident. • The remediation was appropriate. • The issue was escalated within the service provider's hierarchy. • The issue was closed by the service provider. • The issue was monitored and reported to customer management. • Customer procedures were modified to recognize the increased risk. • Internal customer incidents were recorded by the customer, appropriately reported, remediated and closed.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
3. OPERATING IN THE CLOUD *(cont.)*									
3.2 Application Security									
3.2.1 Application Security Architecture Audit/Assurance Objective: Applications are developed with an understanding of the interdependencies inherent in cloud applications, requiring a risk analysis and design of configuration management and provisioning process that will withstand changing application architectures.									
3.2.1.1 Application Security Architecture Control: The design of cloud-based applications includes information security and application security architecture subject matter experts, and the process focuses on the interdependencies inherent in cloud applications.	AI2.4 DS5.1 DS5.2 DS5.7			X					
3.2.1.1.1 Obtain the application design documentation, and review the policies for subject matter expert involvement in the system design.									
3.2.1.1.2 Determine that information security and architecture specialists have been fully engaged during the planning and deployment of cloud applications.									
3.2.1.1.3 Select recent implementations, and review the project and development plans for evidence of information security and subject matter expert involvement.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
3. OPERATING IN THE CLOUD *(cont.)*									
3.2.1.2 Configuration Management and Provisioning Control: Configuration management and provisioning procedures are segregated from the service provider, limited to a security operations function within the customer's organization and provide audit trails to document all activities.	DS5.3 DS5.4 DS9.1 DS9.2 DS9.3			x					
3.2.1.2.1 Obtain the configuration management and provisioning security architecture.									
3.2.1.2.2 Determine if the service provider is prevented from configuring or provisioning users (both administrative and standard users), which may affect data integrity, access or security.									
3.2.1.2.3 Determine if logs and audit trails exist, and record these activities and how they are monitored and reviewed.									
3.2.2 Compliance Audit/Assurance Objective: Compliance requirements are an integral component of the design and implementation of the application security architecture.									
3.2.2.1 Compliance Control: The SDLC includes processes to ensure compliance requirements are identified, mapped to the cloud-based application, and included in the final product. Compliance gaps are escalated to appropriate senior management for waiver approval.	AI2.3 AI2.4 ME3.1 ME3.2			x					
3.2.2.1.1 Obtain the compliance analysis utilized as the basis for authorizing the initiation of a cloud-based application.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
3. OPERATING IN THE CLOUD *(cont.)*									
3.2.2.1.2 Determine if a formal compliance review is performed and if senior management authorization is required where internal information security policies require a waiver to allow the implementation of the cloud-based application.									
3.2.3 Tools and Services Audit/Assurance Objective: Use of development tools, application management libraries and other software are evaluated to ensure their use will not negatively impact the security of applications.									
3.2.3.1 Tools and Services Control: All tools and services used in the development, management and monitoring of applications are itemized and the ownership documented, and their effect on the security of the application is explicitly analyzed. High-risk tools and services are escalated to senior information management for approval.	AI2.5 AI3.2 AI3.3 DS5.1 DS9.1		x	x		x			
3.2.3.1.1 Obtain an analysis of tools and services in use.									
3.2.3.1.2 Determine if the ownership of each tool and service has been identified.									
3.2.3.1.3 Determine if information security risk has been evaluated for each tool and service. If one is deemed a security risk, determine the disposition (escalation, waiver to use or disallow use of software in a cloud environment).									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
3. OPERATING IN THE CLOUD *(cont.)*									
3.2.3.1.4 Examine examples of escalated requests, and determine the adherence to procedures.									
3.2.4 Application Functionality Audit/Assurance Objective: For SaaS implementations, the application outsourced to the cloud contains the appropriate functionality and processing controls required by the customer's control policies within the processing scope (financial, operational, etc.).									
3.2.4.1 Application Functionality Control: The application functionality is subject to an assurance review as part of the customer's application process assurance audit.	ME2.5 ME2.6	X		X		X			
3.2.4.1.1 Refer to a standard application audit program for specific steps.									
3.3 Data Security and Integrity									
3.3.1 Encryption Audit/Assurance Objective: Data are securely transmitted and maintained to prevent unauthorized access and modification.									
3.3.1.1 Data in Transit Control: Data in transit are encrypted over networks with private keys known only to the customer.	DS5.7 DS5.11 DS11.6			X					
3.3.1.1.1 Obtain the encryption policies and procedures for data in transit.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
3. OPERATING IN THE CLOUD *(cont.)*									
3.3.1.1.2 Evaluate if the encryption processes include the following: • Classification of data traversing cloud networks (top secret, confidential, company confidential, public) • Encryption technologies in use • Key management (see key management analysis in section 3.3.2) • A list of external organizations of the customer that have decryption keys to data in transit									
3.3.1.2 Data at Rest Control: Data stored in live production databases on cloud systems are encrypted, with knowledge of the decryption keys limited to the customer.	DS11.2 DS11.3 DS11.6			X					
3.3.1.2.1 Obtain the encryption policies and procedures for data stored on cloud systems.									
3.3.1.2.2 For SaaS implementations, determine if the service provider has implemented data at rest encryption.									
3.3.1.2.3 Determine if sensitive data need to be exclusively stored on customer systems to satisfy customer policy, regulatory or other compliance requirements.									
3.3.1.2.4 Evaluate if the encryption processes include the following: • Classification of data stored on cloud networks (top secret, confidential, company confidential, public) • Encryption technologies in use • Key management (see key management analysis section 3.3.2) • A list of external organizations of the customer that have decryption keys to data at rest									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
3. OPERATING IN THE CLOUD *(cont.)*									
3.3.1.3 Data Backup Control: Data backups are available encrypted.	DS11.2 DS11.3 DS11.5 DS11.6			x					
3.3.1.3.1 Obtain data backup policies and procedures for data backups of cloud-based data.									
3.3.1.3.2 Determine if data are encrypted to prevent unauthorized access and disclosure of confidential data.									
3.3.1.3.3 Determine if the encryption key structure provides adequate data confidentiality.									
3.3.1.3.4 Assess if backup processes provide the ability to restore configurations and data for a predetermined period to allow for forensic and other evaluation activities.									
3.3.1.3.5 Determine if tests of data restoration are performed on a routine basis.									
3.3.1.4 Test Data Confidentiality Control: Test data do not contain and are prohibited from using copies of any current or historical production data containing sensitive/confidential information.	AI7.4 DS11.6			x					
3.3.1.4.1 Obtain testing policies and standards.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
3. OPERATING IN THE CLOUD *(cont.)*									
3.3.1.4.2 Determine if policies specifically exclude the use of any current or historical production data.									
3.3.1.4.3 Perform sampling procedures to determine compliance with the test data prohibition policy.									
3.3.2 Key Management Audit/Assurance Objective: Encryption keys are securely protected against unauthorized access, separation of duties exists between the key managers and the hosting organization, and the keys are recoverable.									
3.3.2.1 Secure Key Stores Control: The key stores are protected during transmission, storage and back up.	DS5.7 DS5.8 DS5.11			x					
3.3.2.1.1 Obtain an understanding of how the key stores are protected.									
3.3.2.1.2 Evaluate access controls, transmission controls and backup to ensure that the key stores are in the possession of the key managers.									
3.3.2.1.3 Identify potential access breaches to key stores, and identify compensating controls.									
3.3.2.2 Access to Key Stores Control: Key stores access is limited to the key managers whose jobs are separated from the process the key stores protect.	DS5.7 DS5.8			x					
3.3.2.2.1 Identify the key store managers.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
3. OPERATING IN THE CLOUD *(cont.)*									
3.3.2.2.2 Perform a separation of duties analysis to determine the specific functional transactions to which the key store managers have access.									
3.3.2.2.3 Evaluate if the positions of key store managers and their access to key stores creates a vulnerability to data confidentiality or integrity.									
3.3.2.2.4 Determine if the service provider has access to the keys and has the procedures and oversight to ensure the confidentiality of customer data.									
3.3.2.2.5 Determine if appropriate controls protect the keys during generation and disposal.									
3.3.2.3 Key Backup and Recoverability Control: Key backup and recoverability have been established and tested to ensure continued access to data keys.	DS4.3 DS4.8 DS4.9 DS5.7 DS5.8			X					
3.3.2.3.1 Obtain the backup and recovery policies and procedures.									
3.3.2.3.2 Perform a risk assessment, with known vulnerabilities, to determine that the key backups would be available and recovery would be assured.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
3. OPERATING IN THE CLOUD *(cont.)*									
3.3.2.3.3 Determine if a key recovery test process exists and is routinely executed.									
3.3.2.3.4 Review recent key recovery tests. Evaluate the validity of each test, the analysis and remediation process used, and the preparedness for key restoration.									
3.4 Identity and Access Management									
3.4.1 Identity and Access Management Audit/Assurance Objective: Identity processes assure only authorized users have access to the data and resources, user activities can be audited and analyzed, and the customer has control over access management.									
3.4.1.1 Identity Provisioning Control: User provisioning (on-boarding), deprovisioning (termination) and job function changes of cloud-based applications and operating platforms are managed in a timely and controlled manner, according to internal user access policies.	DS5.3 DS5.4			X					
3.4.1.1.1 Obtain internal provisioning/deprovisioning policies.									
3.4.1.1.2 Analyze provisioning/deprovisioning policies in relation to the procedures implemented for cloud systems.									
3.4.1.1.3 Using the identity management section of the ISACA *Identity Management Audit/Assurance Program*, identify gaps in controls that require additional focus.									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
3. OPERATING IN THE CLOUD *(cont.)*									
3.4.1.2 Authentication Control: Responsibility for user authentication remains with the customer; single sign on and open authentication (as opposed to service provider proprietary authentication technologies) should be used.	PO3.4 DS5.3 DS5.4			x					
3.4.1.2.1 For SaaS and PaaS, determine if the customer can establish trust between the internal authentication system and the cloud system.									
3.4.1.2.2 Determine, where there is an option, that the nonproprietary authentication process has been implemented at the service provider.									
3.4.1.2.3 If a proprietary authentication process is the only option, determine if appropriate controls are in place to: • Prevent shared user IDs • Provide adequate separation of duties to prevent service provider staff from obtaining customer identities • Provide forensic and logging functions to provide history of activities • Provide monitoring functions to alert customer of unauthorized authentication activities									

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
3. OPERATING IN THE CLOUD *(cont.)*									
3.4.1.2.4 For IaaS: • If dedicated VPNs are implemented between the service provider and customer installations, determine if the users are authenticated at the customer network before passing transactions through the VPN. Dedicated VPNs are implemented between the service provider and customer installations to authenticate users at the customer network before passing transactions along through the VPN. • Where a dedicated VPN is not feasible, determine if recognized standard authentication formats are in use (e.g., SAML, WS-Federation) in conjunction with SSL.									
3.4.1.2.5 For IaaS and private, internal cloud deployments, verify that third-party access control solutions operate effectively in virtualized and cloud environments and that event data can be aggregated and correlated effectively for management review.									
3.4.1.2.6 Using the authentication section of the ISACA *Identity Management Audit/Assurance Program*, identify gaps in controls that require additional focus.									
3.5 Virtualization[14]									
3.5.1 Virtualization Audit/Assurance Objective: Virtualization operating systems are hardened to prevent cross-contamination with other customer environments.									

[14] ISACA offers an audit/assurance program on the topic of virtualization: VMware® Server Virtualization Audit/Assurance Program is available at *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/VMware-Server-Virtualization-Audit-Assurance-Program.aspx*.

VI. Audit/Assurance Program (cont.)

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyperlink	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
3. OPERATING IN THE CLOUD *(cont.)*									
3.5.1.1 Virtualization Control: Operating system isolation and security controls are implemented by the service provider to prevent unauthorized access and attacks.	DS2.4 DS5.5 DS9.2 DS9.3			X					
3.5.1.1.1 Identify the virtual machine configuration in place.									
3.5.1.1.2 Determine if additional controls have been implemented, including the following: • Intrusion detection • Malware prevention • Vulnerability scanning • Baseline management and analysis • Virtual machine image validation prior to placement in production • Preclude bypassing security mechanisms by the identification of security-related APIs in use • Separate production and testing environments • Internal organization identity management for administrative access • Timely isolation intrusion reporting									

VII. Maturity Assessment

The maturity assessment is an opportunity to assess the maturity of the processes reviewed. Based on the results of the audit/assurance review and the reviewer's observations, assign a maturity level to each of the following COBIT control practices. **The assessment should be limited to the control practices related directly to cloud computing implementation and should be applicable to the service provider and customer for the previously mentioned control criteria.**

COBIT Control Objectives	Assessed Maturity	Target Maturity	Reference Hyperlink	Comments
DS1 Define and Management Service Levels Effective communication between IT management and business customers regarding services required is enabled by a documented definition of and agreement on IT services and service levels. This process also includes monitoring and timely reporting to stakeholders on the accomplishment of service levels. This process enables alignment between IT services and the related business requirements. • DS1.1 *Service level management framework*—Define a framework that provides a formalised service level management process between the customer and service provider. The framework should maintain continuous alignment with business requirements and priorities and facilitate common understanding between the customer and provider(s). • DS1.2 *Definition of services*—Base definitions of IT services on service characteristics and business requirements. Ensure that they are organised and stored centrally via the implementation of a service catalogue portfolio approach. • DS1.3 *Service level agreements*—Define and agree to SLAs for all critical IT services based on customer requirements and IT capabilities. This should cover customer commitments; service support requirements; quantitative and qualitative metrics for measuring the service signed off on by the stakeholders; funding and commercial arrangements, if applicable; and roles and responsibilities, including oversight of the SLA. • DS1.5 *Monitoring and reporting of service level achievements*—Continuously monitor specified service level performance criteria. • DS1.6 *Review of service level agreements and contracts*—Regularly review SLAs and underpinning contracts (UCs) with internal and external service providers to ensure that they are effective and up to date and those changes in requirements have been taken into account.				

VII. Maturity Assessment (cont.)

COBIT Control Objectives	Assessed Maturity	Target Maturity	Reference Hyperlink	Comments
DS2 Manage Third-party Services The need to assure that services provided by third parties (suppliers, vendors and partners) meet business requirements requires an effective third-party management process. This process is accomplished by clearly defining the roles, responsibilities and expectations in third-party agreements as well as reviewing and monitoring such agreements for effectiveness and compliance. Effective management of third-party services minimises the business risk associated with non-performing suppliers. • DS2.2 *Supplier relationship management*—Formalise the supplier relationship management process for each supplier. The relationship owners should liaise on customer and supplier issues and ensure the quality of the relationship based on trust and transparency (e.g., through SLAs). • DS2.3 *Supplier risk management*—Identify and mitigate risks relating to suppliers' ability to continue effective service delivery in a secure and efficient manner on a continual basis. Ensure that contracts conform to universal business standards in accordance with legal and regulatory requirements. • DS2.4 *Supplier performance monitoring*—Establish a process to monitor service delivery to ensure that the supplier is meeting current business requirements and continuing to adhere to the contract agreements and SLAs, and that performance is competitive with alternative suppliers and market conditions.				

VII. Maturity Assessment (cont.)

COBIT Control Objectives	Assessed Maturity	Target Maturity	Reference Hyperlink	Comments
DS4 Ensure Continuous Service The need for providing continuous IT services requires developing, maintaining and testing IT continuity plans, utilising offsite backup storage and providing periodic continuity plan training. An effective continuous service process minimises the probability and impact of a major IT service interruption on key business functions and processes. • DS4.2 *IT continuity plans*—Develop IT continuity plans based on the framework and designed to reduce the impact of a major disruption on key business functions and processes. The plans should be based on risk understanding of potential business impacts and address requirements for resilience, alternative processing and recovery capability of all critical IT services. • DS4.4 *Maintenance of the IT continuity plan*—Encourage IT management to define and execute change control procedures to ensure that the IT continuity plan is kept up to date and continually reflects actual business requirements. • DS4.5 *Testing of the IT continuity plan*—Test the IT continuity plan on a regular basis to ensure that IT systems can be effectively recovered, shortcomings are addressed and the plan remains relevant. • DS4.8 *IT services recovery and resumption*—Plan the actions to be taken for the period when IT is recovering and resuming services. • DS4.9 *Offsite backup storage*—Store offsite all critical backup media, documentation and other IT resources necessary for IT recovery and business continuity plans.				
DS5 Ensure Systems Security The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards, and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents.				

VII. Maturity Assessment (cont.)

COBIT Control Objectives	Assessed Maturity	Target Maturity	Reference Hyperlink	Comments
DS5 Ensure Systems Security *(cont.)* • DS5.1 *Management of IT security*—Manage IT security at the highest appropriate organisational level, so the management of security actions is in line with business requirements. • DS5.2 *IT security plan*—Translate business, risk and compliance requirements into an overall IT security plan, taking into consideration the IT infrastructure and the security culture. Ensure that the plan is implemented in security policies and procedures together with appropriate investments in services, personnel, software and hardware. Communicate security policies and procedures to stakeholders and users. • DS5.3 *Identity management*—Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security-responsible person. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement authentication and enforce access rights. • DS5.4 *User account management*—Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. • DS5.5 *Security testing, surveillance and monitoring*—Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited in a timely manner to ensure that the approved enterprise's information security baseline is maintained.				

VII. Maturity Assessment (cont.)

COBIT Control Objectives	Assessed Maturity	Target Maturity	Reference Hyperlink	Comments
DS5 Ensure Systems Security *(cont.)* • DS5.6 *Security incident definition*—Clearly define and communicate the characteristics of potential security incidents so they can be properly classified and treated by the incident and problem management process. • DS5.7 *Protection of security technology*—Make security-related technology resistant to tampering, and do not disclose security documentation unnecessarily. • DS5.8 *Cryptographic key management*—Determine that policies and procedures are in place to organize the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorised disclosure. • DS5.10 *Network security*—Use security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion detection) to authorize access and control information flows from and to networks. • DS5.11 *Exchange of sensitive data*—Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin.				
DS8 Manage Service Desk and Incidents Timely and effective response to IT user queries and problems requires a well-designed and well-executed service desk and incident management process. This process includes setting up a service desk function with registration, incident escalation, trend and root cause analysis, and resolution. The business benefits include increased productivity through quick resolution of user queries. In addition, the business can address root causes (such as poor user training) through effective reporting. • DS8.1 *Service desk*—Establish a service desk function, which is the user interface with IT, to register, communicate, dispatch and analyze all calls, reported incidents, service requests and information demands. There should be monitoring and escalation procedures based on agreed-upon service levels relative to the appropriate SLA that allow classification and prioritization of any reported issue as an incident, service request or information request				

VII. Maturity Assessment (cont.)

COBIT Control Objectives	Assessed Maturity	Target Maturity	Reference Hyperlink	Comments
DS8 Manage Service Desk and Incidents *(cont.)* • DS8.2 *Registration of customer queries*—Establish a function and system to allow logging and tracking of calls, incidents, service requests and information needs. It should work closely with such processes as incident management, problem management, change management, capacity management and availability management. Incidents should be classified according to a business and service priority and routed to the appropriate problem management team, where necessary. • DS8.3 *Incident escalation*—Establish service desk procedures, so incidents that cannot be resolved immediately are appropriately escalated according to limits defined in the SLA and, if appropriate, workarounds are provided. • DS8.4 *Incident closure*—Establish procedures for the monitoring of timely clearance of customer queries. When the incident has been resolved, ensure that the service desk records the resolution steps, and confirm that the action taken has been agreed to by the customer. Also record and report unresolved incidents (known errors and workarounds) to provide information for proper problem management. • DS8.5 *Reporting and trend analysis*—Produce reports of service desk activity to enable management to measure service performance and service response times and to identify trends or recurring problems, so service can be continually improved.				
DS9 Manage the Configuration Ensuring the integrity of hardware and software configurations requires the establishment and maintenance of an accurate and complete configuration repository. This process includes collecting initial configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository as needed. • DS9.1 *Configuration repository and baseline*—Establish a supporting tool and a central repository to contain all relevant information on configuration items. Monitor and record all assets and changes to assets. Maintain a baseline of configuration items for every system and service as a checkpoint to which to return after changes. • DS9.2 *Identification and maintenance of configuration items*—Establish configuration procedures to support management and logging of all changes to the configuration repository. Integrate these procedures with change management, incident management and problem management procedures.				

VII. Maturity Assessment (cont.)

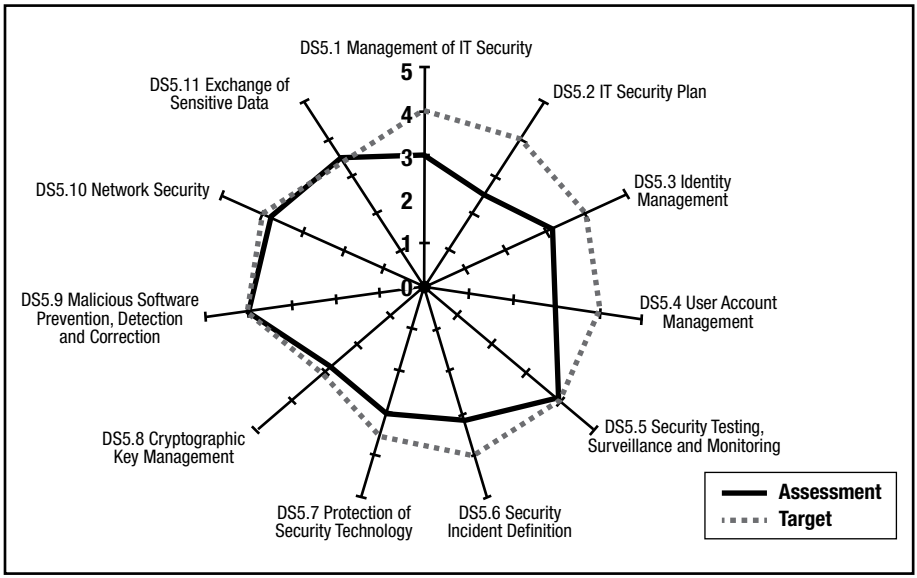
COBIT Control Objectives	Assessed Maturity	Target Maturity	Reference Hyperlink	Comments
DS11 Manage Data Effective data management requires identifying data requirements. The data management process also includes the establishment of effective procedures to manage the media library, backup and recovery of data, and proper disposal of media. • DS11.2 *Storage and retention arrangements*—Define and implement procedures for effective and efficient data storage, retention and archiving to meet business objectives, the organization's security policy and regulatory requirements. • DS11.3 *Media library management system*—Define and implement procedures to maintain an inventory of stored and archived media to ensure their usability and integrity. • DS11.4 *Disposal*—Define and implement procedures to ensure that business requirements for protection of sensitive data and software are met when data and hardware are disposed or transferred. • DS11.5 *Backup and restoration*—Define and implement procedures for backup and restoration of systems, applications, data and documentation in line with business requirements and the continuity plan. • DS11.6 *Security requirements for data management*—Define and implement policies and procedures to identify and apply security requirements applicable to the receipt, processing, storage and output of data to meet business objectives, the organisation's security policy and regulatory requirements.				
ME2 Monitor and Evaluate Internal Control Establishing an effective internal control program for IT requires a well-defined monitoring process. This process includes the monitoring and reporting of control exceptions, results of self-assessments and third-party reviews. • ME2.5 *Assurance of internal control*—Obtain, as needed, further assurance of the completeness and effectiveness of internal controls through third-party reviews. • ME2.6 *Internal control at third parties*—Assess the status of external service providers' internal controls. Confirm that external service providers comply with legal and regulatory requirements and contractual obligations.				

VII. Maturity Assessment (cont.)

COBIT Control Objectives	Assessed Maturity	Target Maturity	Reference Hyperlink	Comments
ME3 Ensure Compliance With External Requirements Effective oversight of compliance requires the establishment of a review process to ensure compliance with laws, regulations and contractual requirements. This process includes identifying compliance requirements, optimising and evaluating the response, obtaining assurance that the requirements have been complied with and, finally, integrating IT's compliance reporting with the rest of the business. • ME3.1 *Identification of external legal, regulatory and contractual compliance requirements*—Identify, on a continuous basis, local and international laws, regulations, and other external requirements that must be complied with for incorporation into the organisation's IT policies, standards, procedures and methodologies. • ME3.3 *Evaluation of compliance with regulatory requirements*—Confirm compliance of IT policies, standards, procedures and methodologies with legal and regulatory requirements. • ME3.4 *Positive assurance of compliance*—Obtain and report assurance of compliance and adherence to all internal policies derived from internal directives or external legal, regulatory or contractual requirements, confirming that any corrective actions to address any compliance gaps have been taken by the responsible process owner in a timely manner.				

VIII. Assessment Maturity vs. Target Maturity

This spider graph is an example of the assessment results and maturity target for a specific company.



Glossary

Acronym	Term	Definition
A6	The Automated Audit, Assertion, Assessment and Assurance application programming interface (API)	A cross-industry work group attempting to develop a common interface allowing cloud service providers (CSPs) to automate the audit, assertion, assessment and assurance of their cloud infrastructures
AICPA	American Institute of Certified Public Accountants	US national professional organization of CPAs
API	Application programming interface	A set of routines, protocols and tools referred to as "building blocks" used in business application software development **Scope note:** A good API makes it easier to develop a program by providing all the building blocks related to functional characteristics of an operating system that applications need to specify; for example, when interfacing with the operating system (OS) (e.g., provided by Microsoft Windows, different versions of UNIX). A programmer would utilize these APIs in developing applications that can operate effectively and efficiently on the platform chosen.
ASP	Application service provider	Also known as managed service provider (MSP); deploys, hosts and manages access to a packaged application to multiple parties from a centrally managed facility **Scope note:** The applications are delivered over networks on a subscription basis.
BCP	Business continuity plan	A plan used by an enterprise to respond to disruption of critical business processes. Depends on the contingency plan for restoration of critical systems.

Acronym	Term	Definition
(none)	BITS (formerly stood for "Banking Industry Technology Secretariat")	A nonprofit, chief executive officer (CEO)-driven financial service industry consortium made up of 100 of the largest financial institutions in the US. BITS works to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions.
BMIS	Business Model for Information Security	An ISACA model providing an in-depth explanation of a holistic business model that examines security issues from a systems perspective
CAPEX	Capital expense	An expenditure that is recorded as an asset because it is expected to benefit more than the current period. The asset is then depreciated or amortized over the expected useful life of the asset.
CAPTCHA	Completely Automated Public Touring test to tell Computers and Humans Apart	A type of challenge-response test used in computing to ensure that the response is not generated by a computer. An example is the site request for web site users to recognize and type a phrase posted using various challenging-to-read fonts.
CICA	Canadian Institute of Chartered Accountants	Canadian national professional organization of CAs
CM	Change management	A holistic and proactive approach to managing the transition from a current to a desired organizational state, focusing specifically on the critical human or "soft" elements of change **Scope note:** Change management includes activities such as culture change (values, beliefs and attitudes), development of reward systems (measures and appropriate incentives), organizational design, stakeholder management, human resource policies and procedures, executive coaching, change leadership training, team building, and communications planning and execution.

Acronym	Term	Definition
(none)	COBIT® (formerly stood for "Control Objectives for Information and related Technology")	A complete, internationally accepted process framework for IT that supports business and IT executives and management in their definition and achievement of business goals and related IT goals by providing a comprehensive IT governance, management, control and assurance model. COBIT describes IT processes and associated control objectives, managememt guidelines (activities, accountabilities, responsibilities and performace metrics) and maturity models. COBIT supports enterprise management in the development, implementation, continuous improvement and monitoring of good IT-related practices. **Scope note:** Adoption and use of the COBIT framework are supported by guidance for executives and management (e.g., *Board Briefing on IT Governance, 2nd Edition*), IT governance implementers (e.g., *COBIT® Quickstart™, 2nd Edition*; *Implementing and Continually Improving IT Governance; COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*), and IT assurance and audit professionals (e.g., *IT Assurance Guide: Using COBIT®*). Guidance also exists to support its applicability for certain legislative and regulatory requirements (e.g., *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition*; *IT Control Objectives for Basel II*) and its relevance to information security (*COBIT® Security Baseline™, 2nd Edition*). COBIT is mapped to other frameworks and standards to illustrate complete coverage of the IT management life cycle and support its use in enterprises using multiple IT-related framework and standards.
CPU	Central processing unit	Computer hardware that houses the electronic circuits that control/direct all operations of the computer system.

Acronym	Term	Definition
CSA	Cloud Security Alliance	A nonprofit organization designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.
CSP	Cloud services provider	A provider of Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) (SPI) services.
CSRF	Cross-site request forgery	A type of malicious exploit of a web site whereby unauthorized commands are transmitted from a user that the web site trusts (also known as a one-click attack or session riding); acronym pronounced “sea-surf”
CSS	Cross-site scripting	A type of computer security vulnerability typically found in web applications that enables malicious attackers to inject client-side script into web pages viewed by other users
DDoS	Distributed denial of service (DoS)	A denial-of-service (DoS) assault from multiple sources
DMTF	Distributed Management Task Force	An industry organization that develops, maintains and promotes standards for systems management in enterprise IT environments
DR	Disaster recovery	Activities and programs designed to return the enterprise to an acceptable condition. The ability to respond to an interruption in services by implementing a DRP to restore an enterprise’s critical business functions.
DRP	Disaster recovery plan	A set of human, physical, technical and procedural resources to recover, within a defined time and cost, an activity interrupted by an emergency or disaster.
(none)	Dynamic partitioning	The variable allocation of central processing unit (CPU) processing and memory to multiple applications and data on a server
ENISA	European Network and Information Security Agency	An agency of the European Union chartered to improve network and information security

Acronym	Term	Definition
ERM	Enterprise risk management	The discipline by which an enterprise in any industry assesses, controls, exploits, finances and monitors risk from all sources for the purpose of increasing the enterprise's short- and long-term value to its stakeholders
ERP	Enterprise resource planning	A packaged business software system that allows an enterprise to automate and integrate the majority of its business processes; to share common data and practices across the entire enterprise; and to produce and access information in a real-time environment
GRC	Governance, risk and compliance	Organizational activities including corporate governance, enterprise risk management (ERM) and corporate compliance with applicable laws and regulations
HIPAA	Health Insurance Portability and Accountability Act	US law that regulates the use and disclosure of patient information held by "covered entities" (generally, healthcare clearinghouses, employer-sponsored health plans, health insurers and medical service providers that engage in certain transactions)
HITECH	Health Information Technology for Economic and Clinical Health Act	A stimulus package passed by the US Congress aimed at inducing more medical service providers and physicians to adopt patient electronic health records (EHR).
HITRUST	Health Information Trust Alliance	An information security consortium formed in 2008 in response to the often confusing array of security mandates, guidelines and rules that affect US healthcare providers, pharmacies, payers, service providers and other organizations affected by healthcare regulatory requirements
(none)	Hypervisor	The computer tool allowing various software applications running on different operating systems (OSs) to coexist on the same server at the same time. This means 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.

Acronym	Term	Definition
I/O	Input/output	The process of input or output, encompassing the devices, techniques, media and data used
IaaS	Infrastructure as a Service	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 operating systems (OSs) and applications
IAM	Identity access management	Encapsulates people, processes and products to identify and manage the data used in an information system to authenticate users and grant or deny access rights to data and system resources. The goal of IAM is to provide appropriate access to enterprise resources.
(none)	Intrusion detection	The process of monitoring the events occurring in a computer system or network to detect signs of unauthorized access or attack
IDS	Intrusion detection system	Inspects network and host security activity to identify suspicious patterns that may indicate a network or system attack
IEEE	Institute of Electrical and Electronics Engineers	An organization composed of engineers, scientists and students; acronym pronounced "I-triple-E" **Scope note:** IEEE is best known for developing standards for the computer and electronics industry.
IM	Investment Management	A Val IT domain
IPS	Intrusion prevention system	An extension of IDS that can prevent/block detection intrusions
ISP	Internet service provider	A third party that provides individuals and enterprises access to the Internet and a variety of other Internet-related services
ITGI	IT Governance Institute	Founded by ISACA and its affiliated foundation in 1998; strives to assist enterprise leadership in ensuring long-term, sustainable enterprise success and increase stakeholder value by expanding awareness
J-SOX	Japanese "Sarbanes-Oxley Act"	The Japanese government's equivalent to the US Sarbanes-Oxley Act

Acronym	Term	Definition
K-SOX	Korean "Sarbanes-Oxley Act"	The Korean government's equivalent to the US Sarbanes-Oxley Act
LPAR	Logical partitioning	The IBM definition of dynamic partitioning
NIST	National Institute for Standards and Technology	Agency of the US Department of Commerce whose mission is to promote US innovation and industrial competitiveness by advancing measurement science, standards and technology *www.nist.gov/public_affairs/general_information.cfm*
OASIS	Organization for the Advancement of Structured Information Standards	A nonprofit consortium that drives the development, convergence and adoption of open standards for the global information society
OPEX	Operating expense	An ongoing cost of performing daily business activity, e.g., utilities, insurance, maintenance, office supplies
OS	(Computer) operating system	A master control program that runs the computer and acts as a scheduler and traffic controller. **Scope note:** The OS is the first program copied into the computer's memory after the computer is turned on and must reside in memory at all times. It is the software that interfaces between the computer hardware (disk, keyboard, mouse, network, modem, printer) and the application software (word processor, spreadsheet, e-mail), and it also controls access to the devices, is partially responsible for security components and sets the standards for the application programs that run in it.
OWASP	Open Web Application Security Project	An open-source application security project. The OWASP community includes corporations, educational organizations and individuals from around the world.

Acronym	Term	Definition
PaaS	Platform as a Service	Offers the capability to deploy onto the cloud infrastructure customer-created or -acquired applications that are created using programming languages and tools supported by the provider
PC	Personal computer	An electronic data processor for use by an individual
PCI DSS	Payment Card Industry Data Security Standards	Worldwide information security standards defined by the Payment Card Industry Security Standards Council
PDA	Personal digital assistant	Handheld devices that provide computing, Internet, networking and telephone characteristics; also known as "palmtop" and "pocket computer"
PII	Personally identifiable information	Information that can be used alone or with other sources to uniquely identify, contact or locate a single individual
PIPEDA	Personal Information Protection and Electronic Documents Act	Canadian law relating to data privacy
PM	Portfolio Management	A Val IT domain
RFI	Remote file inclusion	A type of vulnerability most often found on web sites, allowing an attacker to include a remote file usually through a script on the web server
RPO	Recovery point objective	Determined based on the acceptable data loss in case of a disruption of operations. It indicates the earliest point in time to which it is acceptable to recover the data. The RPO effectively quantifies the permissible amount of data loss in case of interruption.
RTO	Recovery time objective	The amount of time allowed for the recovery of a business function or resource after a disaster occurs

Acronym	Term	Definition
SaaS	Software as a Service	Offers the 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).
SDLC	Software/system development life cycle	The phases deployed in the development or acquisition of a software system **Scope note:** This is an approach used to plan, design, develop, test and implement an application system or a major modification to an application system. Typical phases of the SDLC include feasibility study, requirements study, requirements definition, detailed design, programming, testing, installation and postimplementation review, but not the service delivery or benefits realization activities.
SEIM	Security event and incident management	A prepared defense plan to manage and document an enterprise's response to a security incident
SLA	Service level agreement	An agreement, preferably documented, between a service provider and the customer(s)/user(s) that defines minimum performance targets for a service and how they will be measured
SNIA	Storage Networking Industry Association	International organization for storing information
SOA	Service-oriented architecture	A cloud-based library of proven, functional software applets that are able to be connected together to become a useful online application
SoD	Segregation/ separation of duties	A basic internal control that prevents or detects errors and irregularities by assigning responsibility for initiating and recording transactions and custody of assets to separate individuals **Scope note:** SoD is commonly used in large IT organizations so that no single person is in a position to introduce fraudulent or malicious code without detection.

Acronym	Term	Definition
SOX	Sarbanes-Oxley Act of 2002	A US law enacted as a reaction to a number of major corporate and accounting scandals. Its intent is to ensure that publicly traded companies in the US maintain open transparency in their accounting procedures and have controls in place to prevent any manipulation of financial data.
SPI	Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS)	The acronym used to refer to the three cloud delivery models
SQL	Structured Query Language	A database computer language designed for managing data in relational database management systems (RDBMSs)
TCO	Total cost of ownership	Includes original cost of the computer and software, hardware and software upgrades, maintenance, technical support, training, and certain activities performed by users
URL	Uniform resource locator	Specifies where an identified online resource is available and the mechanism for retrieving it
VG	Value Governance	A Val IT domain
VPN	Virtual private network	A secure private network that uses the public telecommunications infrastructure to transmit data **Scope note:** In contrast to a much more expensive system of owned or leased lines that can only be used by one company, VPNs are used by enterprises for both extranets and wide areas of intranets. Using encryption and authentication, a VPN encrypts all data that pass between two Internet points, maintaining privacy and security
(none)	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

Acronym	Term	Definition
XACML	Extensible Access Control Markup Language	A declarative online software application user access control policy language implemented in Extensible Markup Language (XML)
XML	Extensible Markup Language	Promulgated through the World Wide Web Consortium, XML is a web-based application development technique that allows designers to create their own customized tags, thus, enabling the definition, transmission, validation and interpretation of data between applications and enterprises

Additional Resources and Feedback
Visit *www.isaca.org/itcocloud* for additional resources and use the feedback function to provide your comments and suggestions on this document. Your feedback is a very important element in the development of ISACA guidance for its constituents and is greatly appreciated.

ISACA Professional Guidance Publications

Many ISACA publications contain detailed assessment questionnaires and work programs that provide valuable guidance. Please visit *www.isaca.org/bookstore* or e-mail *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, 2nd 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®, 2nd 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™, 2nd Edition*, 2007
- *COBIT® Security Baseline™, 2nd 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, 2nd 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, 2nd Edition*, 2004
- Technical and Risk Management Reference Series:
  - *Security, Audit and Control Features Oracle® Database, 3rd Edition*, 2009
  - *Security, Audit and Control Features Oracle® E-Business Suite, 3rd Edition*, 2010
  - *Security, Audit and Control Features PeopleSoft, 2nd Edition*, 2006
  - *Security, Audit and Control Features SAP® ERP, 3rd 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

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*
Web site: *www.isaca.org*

ISBN 978-1-60420-185-7
90000>
9 781604 201857