CHAPTER NINE

9

# Evolving Control Issues: Wireless Networks, Cloud Computing, and Virtualization

AN INFORMATION TECHNOLOGY (IT) auditor, working in the profession for any length of time, will understand that the IT technologies and their supporting processes are changing on a continuous basis. Some of these changes—such as the move to laptop computers from desktop devices tied to a network—do not have a significant internal controls impact for IT auditors. Others do. This chapter discusses three areas where IT is changing and where IT auditors may need to take somewhat different approaches in their internal controls reviews.

Our first example is the growth of wireless networks, both public and private. IT auditors often easily access their e-mail messages or get current business news from their laptop devices and the Internet. These facilities provide a massive convenience to all systems users, but they do present some control and security threats if an enterprise's network is not properly protected through firewalls and other security controls. An IT auditor may be happy to be able to access e-mail messages or change an airline flight reservation over a wireless network, but those connections should be secure. This chapter briefly looks at some wireless network security and internal control issues.

An IT configuration called cloud computing has been evolving rapidly in recent years. Although the term sounds almost exotic to many, cloud computing has become a significant concept today with our growing dependency on Web-based applications for many business processes rather than more traditional applications downloaded to home office servers. The concept known as Web services, service-oriented architecture (SOA), or software as a service (SaaS) was first largely promoted by Microsoft several years ago but has now been embraced by many others. Today, this concept has been

broadened and is known as cloud computing, a configuration where many different Internet applications supported by multiple vendors and operating on multiple servers operate together out of what looks like a large fuzzy Internet cloud. This chapter introduces some cloud computing concepts and discusses cloud-related security and controls concerns that may impact IT auditors in their assessments of IT general controls.

On a somewhat different level, storage management virtualization is another evolving IT infrastructure with general controls implications. The term *storage management virtualization* refers to the connections between a computer central processor unit (CPU) and connected or supporting mass storage drives or other devices. In past years, IT managers and auditors thought of a computer system in terms of its configuration—the disk drives and other peripheral devices that were connected to a computer's CPU. At one time, these were attached through an often complex network of hard-wired cables. However, starting around the year 2001, software tools were introduced to better manage these storage connections; this is called storage virtualization. They began as a tool for large server sites, but today virtualization concepts have been introduced on all levels of computer processors. File virtualization can introduce strong efficiencies to IT operations; however, there can also be some internal control risks if mass storage relationships are not properly managed and backed up. We will briefly introduce IT virtualization concepts important to IT auditors.

This chapter discusses these IT technical areas because they may impact IT auditors in their reviews and assessments of IT general controls. These three IT-related areas may not be familiar to many IT auditors and their managers today, but they will be control issues in many IT general controls audits going forward. Of course, the landscape is always changing, and IT auditors should always be aware of newer technology-driven internal control issues and should modify their reviews to accommodate and assess these and other new internal controls areas. IT auditors should always take a strong lead in their enterprises in understanding new technology-based processes and then translating them to reviews and assessments of internal controls.

## UNDERSTANDING AND AUDITING IT WIRELESS NETWORKS

Computer system components, such as terminals or printers, traditionally have been connected to their CPUs through cables or transmission wires. In earlier days, when an employee moved from one office to another, it was often necessary for a maintenance crew to string the necessary cables to the new office location. Although they originally could not transmit electronic data, radio-based wireless communications tools began to have a significant impact on the world during World War II. Through the use of wireless networks, information could be sent overseas or behind enemy lines easily, efficiently, and more reliably. Since then, transmission standards have been developed and wireless networks have grown significantly. Using local transmission stations, wireless networks first became common for local emergency services, such as the police or fire departments, which utilized wireless networks to communicate important information quickly.

By the late 1980s, local area networks (LANs) became very common, and many computer system configurations became to be based on a network of wired computer systems. In the early 1990s, processes and standards were developed for wireless LANs, where each system was a point in a local network.

Starting with these early 1990s standards, tools were developed to implement wireless LANs. These LANs originally required communications cards between a central computer and local terminals, but they expanded to broad networks with connections to remote transmission stations and the Internet.

Wireless systems have some vulnerability risks since their data is carried as radio signals subject to snooping. Wireless LANs, however, have their own problems. Connecting network elements by radio waves instead of wires presents many challenges. From a reliability standpoint, it is difficult to predict how dependable wireless network radio coverage inside a building will be because building construction features, such as steel beams and heavily plastered walls, severely weaken radio waves. Even outside of structures, predicting coverage accurately and dependably is difficult, owing to radio transmission propagation issues. Much more troubling is the fact that wireless LANs, by their very nature, broadcast their data into space, where the data can be intercepted by anyone with the ability to listen in at the appropriate frequency. These features also facilitate internal use of wireless LANs and enable interlopers to enter such networks with the same privileges as authorized users unless appropriate security controls are in place.

Not all networks, and certainly not all wired networks, are secure. However, when a traditional LAN operates over cables within a relatively secure physical perimeter, the level of security provided by the physical construction usually is sufficient. Adding wireless transmission capabilities adds security vulnerabilities and the need for additional systems controls, such as the need to authenticate every network user. An IT auditor should look these general control and security characteristics in all wireless applications:

- **Confidentiality.** An application should contain a level of protection against interception, or eavesdropping, to provide assurance that messages sent are readable only by the intended recipients.
- **Authenticity.** Protections against spoofing or impersonation controls should be in place to ensure that messages originate from the claimed entity.
- **Integrity.** Controls should provide protection from transmission errors and/or willful modification of messages to offer assurances that a message has not changed in transmission.
- **Availability.** Assurances should be in place that application data will be available when and where it is required, as a protection against denial of service or poor reliability.

Wireless networks and wireless LANs are important areas that should be included in any IT auditor's review of general controls. The next sections discuss some key internal control characteristics of wireless networks important for IT auditors as well as considerations for reviews of IT wireless systems general controls.

## Key Components of an IT Wireless System

A wireless IT system is almost a generic name, and there can be some confusion about the overall configuration of any such system. There are several basic ways to configure a wireless system. In an open system configuration, any entity that can pick up the wireless signal can potentially gain access. This is the type of wireless system, built around a wireless access point (WAP), that one encounters when accessing the Internet from a hotel room or coffee shop. For purposes of definition, a WAP is a device that allows communications connections to wireless networks using standards such as Wi-Fi, Bluetooth, or related standards. The WAP usually connects to a wired network and can relay data between the wireless devices (such as computers or printers) and wired devices on the network.

Many wireless systems in offices or homes are limited in their proximity to a WAP. Within their borders, however, they may connect to a variety of devices. Exhibit 9.1 shows such a wireless configuration with the wireless system existing inside a defined border, controlled by series of routers on the border edge. Routers are discussed in the next section; a large number of laptop computers, terminals, and other devices may be

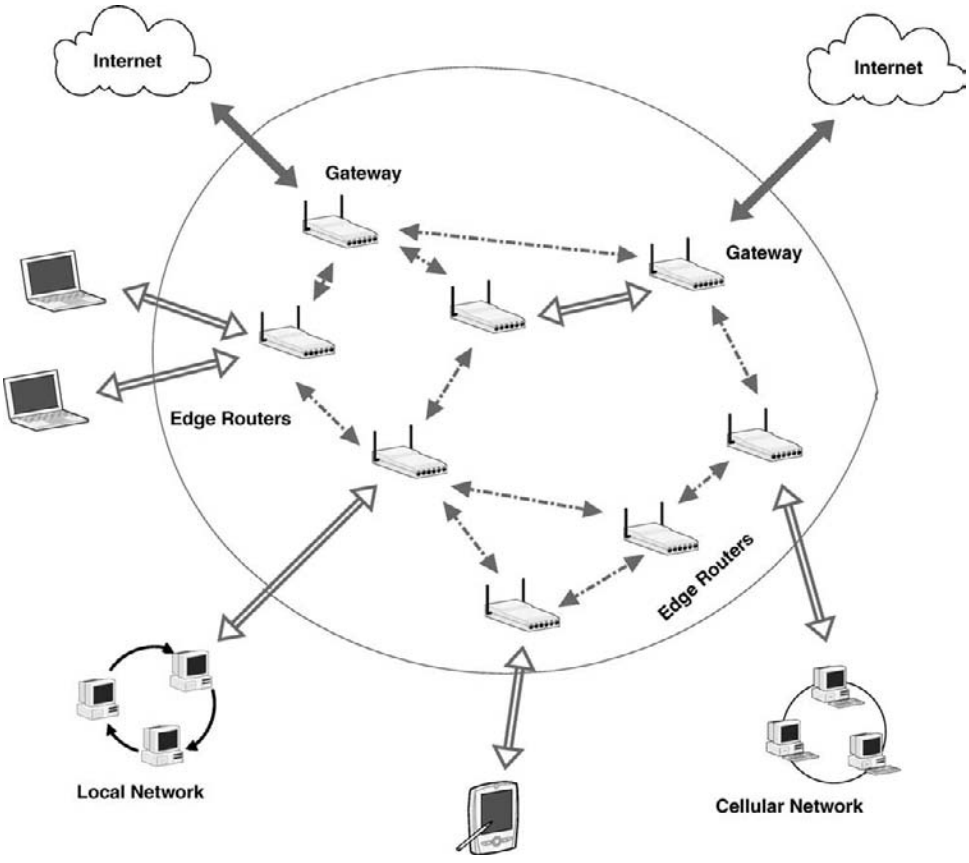


**EXHIBIT 9.1** Wireless Network Architecture

attached to each router. As the exhibit shows, the wireless network is connecting to the Internet through several service providers and to some other external systems outside of the network. In addition, there are connections to local LANs, a cell phone network, and personal handheld devices. Although at a very general and high level, this exhibit illustrates the type of wireless system found in many enterprises today. From an IT auditor's perspective, two key controls in this wireless system configuration are the placement of its routers and firewalls.

### *Wireless System Routers*

A key component of all networks, including wireless networks, a router is an electronic device used to connect two or more computers to the Internet by cable or wireless signals. A router allows several computers to communicate with each other and to the Internet at the same time. A wireless router performs the functions of a router but also acts as a wireless access point to allow access to the Internet or a computer network without the need for a cabled connection. It can function as a wired or a wireless LAN. Some routers also contain wireless antennae that allow connections from other wireless devices.

### *Wireless Firewalls*

A firewall is a type of one-way software door where transactions and activity can exit but cannot enter. It is a system, implemented in hardware, software, or a combination of both, that is designed to prevent unauthorized access to or from a private network. Firewalls frequently are used to prevent unauthorized Internet users from accessing private networks connected to the Internet, where all messages entering or leaving an internal network, the intranet, pass through an installed firewall. This important network control examines each message and blocks those that do not meet the specified security criteria. A firewall is considered a first line of defense in protecting private information.

### *Wireless Network Vulnerabilities and Risks*

There are a variety of control risks associated with any wireless network, including the risk of eavesdropping into system activities, illicit entry into the network enabled by a failure of user authentication, and denial of services. A major systems integrity concern here is the risk of eavesdropping. By their nature, wireless LANs intentionally radiate their radio signal network traffic into space, and once the signals are emitted, it is impossible to control who can receive them. The key control here is to encrypt all such messages. Wireless message standards allow for such encryption, but such standards are not always installed. When reviewing wireless applications, IT auditors should determine that encryption standards have been installed and that they have been applied to all critical applications.

The implementation of controls to ensure message integrity is also important for wireless systems. Network messages are transmitted in small packets of data that are then reassembled to deliver the correct message. Transmission software provides standards that should protect the integrity of all messages. Although the technical

details here may be beyond many readers, an IT auditor should meet with enterprise communications software specialists responsible for their enterprise's wireless networks and discuss the implemented software default standards that emphasize message integrity and provide controls over illicit network entry.

Our discussion here emphasizes the closed wireless networks that are more common for a business enterprise. Over time, the use of open wireless network connections, that are common in some public places to provide access to the Internet and other sites, will become more prevalent. Because these wireless systems are based on radio signal messages, we may see more perpetrators trying to get around security rules and attempting to gain improper accesses.

## Wireless Network Security Concerns

Security is a major issue with many enterprise wireless networks in general and wireless LANs in particular. Anyone equipped with proper tools within the geographical network range of an open, unencrypted wireless network can "sniff," or record, the network traffic, gain unauthorized access to internal network resources and to the Internet, and then possibly send spam messages or attempt other illegal actions using the wireless network's Internet addresses. Although these threats reflect issues that have long troubled many types of wired networks (e.g., individuals can plug their laptop computers into available Ethernet communication jacks within a site and get access to a local wired network), this improper access activity usually does not pose a significant problem, since many enterprises had reasonably good physical security. However, radio signals bleed or move outside of buildings and drift across property lines, making network physical security largely irrelevant.

Establishing effective wireless security procedures is a challenge to IT network administrators, enterprise management, and many IT auditors. There are strong and recognized standards to protect a wireless network, but many of those standards are defined in hardware routers—such as Cisco devices—that are wireless security options are set through controlling software with limited monitoring or controls.

Good IT processes and technology often are easily confused, and particularly so with wireless information security management issues. However, many of the same business processes that establish strong risk management practices for physical assets and wired networks also work to protect wireless resources. IT auditors can use the following cost-effective guidelines to enable enterprises to establish proper security protections as part of an overall wireless strategy. This list includes areas that represent good IT wireless internal control practices and objectives. An IT auditor can use these recommendations to better understand and evaluate enterprise wireless security processes.

- **Wireless security policy and architecture design.** Enterprise security policy, procedures, and best practices should include wireless networking as part of overall security management architecture to determine what is and is not allowed with wireless technology.
- **Treat all wireless access points as untrusted.** Access points need to be identified and evaluated on a regular basis to determine if they need to be quarantined as

untrusted devices before wireless clients can gain access to internal networks. This determination means the appropriate placement of firewalls, virtual private networks (VPNs), intrusion detection systems (IDSs), and authentication between access points or the Internet.

- **Access point configuration policies.** Enterprise administrators need to define their standard security settings before the wireless systems can be deployed. These settings include guidelines regarding IDs, wireless keys, and encryption.
- **Access point discovery.** Administrators should regularly search outward from a wired network to identify unknown access points. Such a search may identify rogue access points operating in the area—often a major concern in densely populated areas.
- **Access point security assessments.** An enterprise should perform regular security reviews and penetration assessments to identify poorly configured access points or defaults or easily guessed passwords.
- **Wireless client protection.** Wireless clients—typically user departments—should be examined regularly for good security practices. An enterprise IT function can establish good wireless procedures, but the actual users also should follow good practices.

The overall objective of this chapter is to highlight some evolving internal control areas that impact IT auditors. IT wireless systems are nothing new, but they are becoming almost standard components in many system configurations today. Chapter 26 provides more guidance on auditing IT telecommunication processes and wireless systems.

## UNDERSTANDING CLOUD COMPUTING

Cloud computing is a new and evolving concept that is important to many IT operations. Also closely related to the concepts of SaaS or SOA, cloud computing today is changing the way that many enterprises build and use IT applications.

A cloud symbol is often used today to refer to the Internet in this book and in other published references. The idea behind this Internet cloud is that users do not need knowledge of, expertise in, or control over the technology infrastructure ''in the cloud'' that supports them. This term originated in the telephone industry where, up until the 1990s, data and even early Internet circuits were hard-wired between destinations, but later long-haul telephone companies began offering wireless VPN service for data communications. The growth of these wireless networks and the Internet's World Wide Web concepts enhanced the way that we think of IT services.

Cloud computing is more than just the Internet. It is the way we think of the services that Internet-resident applications provide. Because it is impossible to determine in advance precisely the paths of Internet traffic, the cloud symbol is used to describe that which were the responsibilities of the service providers as well as the network infrastructure. The concepts of software products or services on the Internet—SOA and SaaS—soon followed.

In the early 2000s, Microsoft extended this concept of SaaS through the development of what it calls Web Services. IBM also later released what it called the Autonomic

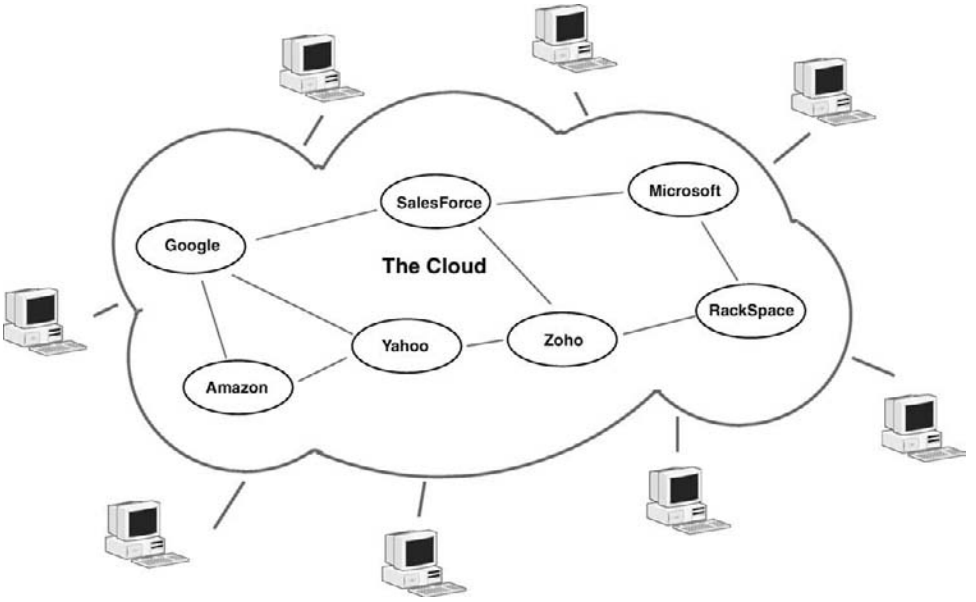


**EXHIBIT 9.2** Cloud Computing Concepts

Computing Manifesto, which described automation techniques such as self-monitoring, self-healing, self-configuring, and self-optimizing in the management of complex IT systems with heterogeneous storage, servers, applications, networks, security mechanisms, and other system elements that can be virtualized across an enterprise.

Software vendors are increasingly offering their products as services on the Internet rather than as applications that are resident on individual in-house servers. A good example of this trend—and an early product type leader—is the provider of customer relationship management (CRM) software, SalesForce (www.salesforce.com/crm/products.jsp). This supplier of customer and sales tracking software tools does not sell its products as a set of programs loaded on proprietary CDs for customer use. Rather, all of the SalesForce programs and documentation is found on the Internet, and customers pay for the software only when they use the product. The SalesForce applications are used as a service to customers.

Exhibit 9.2 shows this SaaS cloud computing concept. We have highlighted several vendors that currently offer SaaS products today, including Amazon, Google, Microsoft, and SalesForce. This is only a limited example of SaaS current applications, and certainly many more will follow. Some of the benefits of SaaS applications in a cloud computing environment are:

- Reduced infrastructure costs due to centralization. With the SaaS application in the cloud, there is no need to maintain application change management and other controls.
- Increased peak load capacities. Cloud providers, such as Amazon or Google, have massive server farms with massive capacities. Their load capacities are almost infinite.

- Efficiency improvements for systems that are often underutilized.
- Consistent performance that will be monitored by the service provider.
- Application and IT services resiliency. Cloud providers have mirrored solutions that can be utilized in a disaster scenario as well as for load-balancing traffic. Whether there is a natural disaster requiring a site in a different geographic area or just heavy traffic, cloud providers should have the resiliency and capacity to ensure sustainability during an unexpected event.

IT auditors will need to take a different approach in reviewing internal controls for SaaS applications and understanding IT security in a cloud computing environment. Web and other infrastructure services today are increasingly being delivered in a cloud environment, and there is a need to rethink some audit and control considerations.

## Reviewing Cloud Computing Application Controls

As any IT auditor should realize, even though an application is operating out of an SaaS environment, the need to assess and review its application internal controls does not go away. The SaaS-based application should continue to have the same audit trails, error-checking procedures, and other good practices that are found with any well-controlled IT application. An IT auditor can almost expect that a business application run under a major vendor, such as Google, has adequate internal controls.

Cloud computing represents a major change in the way applications are run and managed. Although only a limited number of vendors provide service-based software applications today, that number is expected to increase. Many vendors provide an implicit level of trust in the services they provide under the SaaS clouds, but an IT auditor should meet with their IT and business management to gain assurances that every SaaS application is well controlled.

An IT auditor should attempt to help demonstrate, to direct and indirect cloud computing users, that they can have a strong level of trust in the software services and infrastructure that make up the cloud for an enterprise. Some of the key assurance issues that should be addressed are:

- **Transparency.** Service providers must be able to demonstrate the existence of effective and robust security controls, assuring customers that their information is properly secured against unauthorized access, change, and destruction. Key questions for any service provider providing SaaS applications are:
  - What types of service provider employees have access to customer information?
  - Is a segregation of duties between provider employees maintained?
  - How are the files and data for different customers' information segregated?
  - What controls are in place to prevent, detect, and react to any security and control breaches?
- **Privacy.** Cloud computing service providers should provide assurances that privacy controls are in place that will prevent, detect, and react to breaches in a timely manner, with strong and periodically tested lines of communication.
- **Compliance.** In order to comply with various laws, regulations, and standards, there can be cloud computing concerns that the data may not be stored in one place

and may not be easily retrievable. It is critical to ensure that if authorities demand certain data, it can be provided without compromising other information. When using cloud services, there is no guarantee that an enterprise can get its information when needed or that a service provider may or may not claim a right to withhold information from authorities.

- **Transborder information flow.** With cloud-generated information potentially stored anywhere in the cloud, the physical location of the information can become an issue. This physical location dictates a jurisdiction and legal obligation. There are many legal issues here yet to be solved.
- **Certification.** Cloud computing service providers should assure their customers that they are doing the ''right'' things. In the future, independent third-party audits and/or service auditor reports will become a vital part of any cloud computing service provider assurance program. However, these facilities have not yet materialized.

Strong and effective standards are needed to help enterprises gain assurances regarding their cloud computing supplier's internal controls and security. At the time of this publication, there are no publicly available specific cloud computing standards.

As no defined set of standards exists, an IT auditor reviewing applications provided by a cloud computing service provider should look for strong assurances in three key areas:

1. **Events.** The service provider should regularly document and communicate changes and other factors that have affected SaaS system availability.
2. **Logs.** A service provider should provide comprehensive information about an enterprise's SaaS application and runtime environment.
3. **Monitoring.** Any such surveillance should not be intrusive and must be limited to what the cloud provider reasonably needs in order to run its facility.

Cloud computing represents a new and interesting opportunity to rework security and IT controls for a better tomorrow, and internal auditing standards should soon follow. The Information Systems Audit and Control Association (ISACA) has already provided some preliminary cloud computing audit and control guidance, and we expect to see much more in the future as SaaS applications and cloud computing grows and matures.

## Cloud Computing Security and Privacy Challenges

The use of SaaS applications operating in cloud computing environment shifts a wide range of challenges and responsibilities primarily from an enterprise's IT function to an environment where some responsibilities are assumed by the cloud computing service provider while others remain the responsibility of the enterprise IT function. This is a challenge for IT auditors as well, who must understand the security and privacy components of their selected service providers.

Cloud computing and the use of SaaS applications is a new trend and an increasing number of vendors are offering suites of SaaS applications. Vendors such as Google and Amazon are building huge, multiserver cloud computer complexes, but today no established set of recognized best practices exists across these various service providers.

In some respects, the trend of enterprises shifting some their in-house IT resources to cloud service providers has some elements similar to the move to IT service bureaus in the early 1980s.

In the mid- to late 1970s, an increasing number of enterprises decided to move from their manual or unit-record punched-card processes to the new mainframe computer systems. Many had added systems development programming staffs and installed mainframe computer systems, but often with very disappointing results. A frequent problem was that these new systems did not have the capacity to process the volumes of enterprise data; when they did, often the systems experienced computer system maintenance or downtime problems.

A solution for many at that time was to convert enterprise computer systems operations to what was called a service bureau—a large centralized computer systems resource that collected input materials for many clients, processed using common systems, and delivered the output reports. These service bureaus, however, did not work well for everyone. Many firms subscribed without fully realizing what they would be getting in terms of services and integrity and internal control monitoring for the enterprise processes. Most service bureau computer operations disappeared well before the demise of the mainframe. However, some of the same things are happening today with enterprises converting some conventional applications to a cloud environment. A major problem is that enterprises do not always ask the right questions from their service providers.

When making a decision to select a service provider as part of a move to cloud computing, an enterprise should ask competing service providers some hard questions about their operations and standards. An IT auditor can take a lead in suggesting that its management should gain assurances in some of these areas when selecting a cloud computing service provider:

- **Privileged user access.** Sensitive data processed outside an enterprise and in a cloud brings with it an inherent level of risk, because outsourced services in the cloud bypass conventional physical, logical, and personnel IT controls that an IT organization would exert over its in-house systems programs. Service providers should provide thorough information about the people who manage an enterprise's data and systems in the cloud. They should supply specific information on the hiring and oversight of privileged administrators and the controls over their access.
- **Regulatory compliance.** An enterprise is ultimately responsible for the security and integrity of its own data, even when that data is held by a service provider. Cloud computing service providers should supply detailed information on their security governance policies and the results of recent external audits and security certifications. In addition, they should agree to update the enterprise on these activities on a regular basis.
- **Data location.** When an enterprise uses the cloud, it probably will not know exactly where data is hosted—not even the country. Because of data ownership laws, service providers should identify the specific jurisdictions where they will be storing and processing an enterprise's data. Service providers also should make a contractual commitment to obey local privacy requirements on behalf of their customers.

- **Data segregation.** Data in the cloud typically is stored in a shared environment alongside data from other customers. Cloud providers should provide detailed information on what is done to segregate enterprise data at rest or separate from other users and provide evidence that their security encryption schemes were designed and tested by experienced specialists. Encryption accidents can make data totally unusable and can complicate availability.
- **Recovery.** Even if an enterprise does not know the location of its cloud data, cloud providers should document what will happen to data and services in case of a disaster. They should provide evidence, including test results, that their recovery methods will replicate the data and application infrastructure across multiple sites. The services should assert whether they have the ability to do a complete restoration, and how long it will take.
- **Investigative support.** Investigating inappropriate or illegal activity may be impossible in cloud computing. Cloud services are especially difficult to investigate, because logging and data for multiple customers may be collocated and/or spread across an ever-changing set of hosts and data centers. Service providers should provide a contractual commitment to support specific forms of investigation, along with evidence that they have already successfully supported such activities.
- **Long-term viability.** An enterprise has no guarantee that cloud computing providers will never go broke or be acquired and swallowed up by a larger company. However, current providers such as Amazon, Google, IBM, and Microsoft will almost certainly continue to be around for a while. An enterprise should nevertheless gain assurances that its data will remain available even after such an event. All service providers should provide assurances that users will get their data back in a format that they can import into a replacement application.

Cloud computing and SaaS applications are new and evolving areas as this book goes to press. We can expect to see established standards and recognized best practices in future years. Companies learned enough lessons years ago when using IT service bureaus to recognize how *not* to select a cloud service provider. Cloud computing and SaaS are the wave of the future, and IT auditors should see much more of them in the years going forward.

## STORAGE MANAGEMENT VIRTUALIZATION

*Virtualization* is the concept of pooling IT physical storage resources from multiple network storage devices into what appears to be a single storage device that is managed from a central console. Storage virtualization helps an IT storage administrator perform the tasks of backup, archiving, and recovery more easily, and in less time, by disguising the actual complexity of the overall network of IT storage devices. This author was first introduced to storage management virtualization in 2002 when he was as part of a small consulting group for EMC Corporation helping to launch an Information Technology Infrastructure Library (ITIL) consulting practice. (ITIL best practices are discussed in Chapter 7.) At that time, EMC was a leader in storage management devices,

and its virtualization concepts were a major technology innovation. Virtualization has since become a widely used and important IT resource management process.

To understand IT virtualization, one should visit the earlier days of computer systems—particularly the mainframes of old. Those computers had operating systems (OSs) that controlled various attached peripheral devices, including printers, tape drives, and mass storage devices. Although earlier mainframe computer systems initially made massive use of relatively inexpensive magnetic tape drives to store data, technology quickly moved to rotating magnetic drum and then to disk drive storage devices. Although they were much more expensive in the early days of IT, disk and drum drives quickly became popular. The limitation with tape drives was that to read the 100,000th record on a tape, the drive had to pass through the first 99,999 records to find that record. Tape drives and then drum drives quickly became almost historical anecdotes, and technology moved to rotating disk drives, which were much faster and had indexing schemes that located that 100,000th record almost instantaneously.

As every IT auditor with a packed C drive on his or her laptop, full of records and other materials, can attest, there is strong need for mass storage space on all computers. Enterprises of all sizes need ways to manage and control their stored data. With enterprises creating so much information, IT operations have stored their data on multiple storage units or drives but also need to consolidate storage and get the most out of each storage unit. Schemes for managing all those devices soon become a headache. A solution has been storage virtualization, a technique to combine all storage drives into one centrally manageable resource.

Virtualization in general is the separation of a device's functions from its physical elements. With storage virtualization, a unit's physical drive is separated from its functions to store data, and multiple physical disks will appear to be a single unit. Virtualization is a very efficient method to manage and control separate physical units using specialized virtualization software. With the proper software, virtualization techniques can be used with IT hardware devices beyond storage management, network components, servers, operating systems, or even applications. In such systems, the hardware application diagrams that IT auditors had to request as part of a review of general IT controls are no longer applicable. Virtualization software assumes these unit-by-unit responsibilities.

Virtualization concepts were, in some respects, the forerunner of cloud computing. We have only mentioned virtualization here as a new concept, with little supporting detail, that IT auditors will encounter in their general controls reviews. Although IT storage management virtualization was first introduced by just one company, many hardware and storage management vendors have picked up the concept. When an IT auditor encounters an environment in which virtualization is used heavily, he or she should meet with members of the IT staff to gain an understanding of the nature of the implementation, to ensure that it has been implemented in a manner that emphasizes IT internal controls, and that IT appears to be realizing benefits from the software tools or features. Similar to cloud computing, virtualization is a software product or concept offered by many major vendors. It is a growing and still evolving concept and IT auditors should increase their understanding of it as an evolving trend in IT operations.