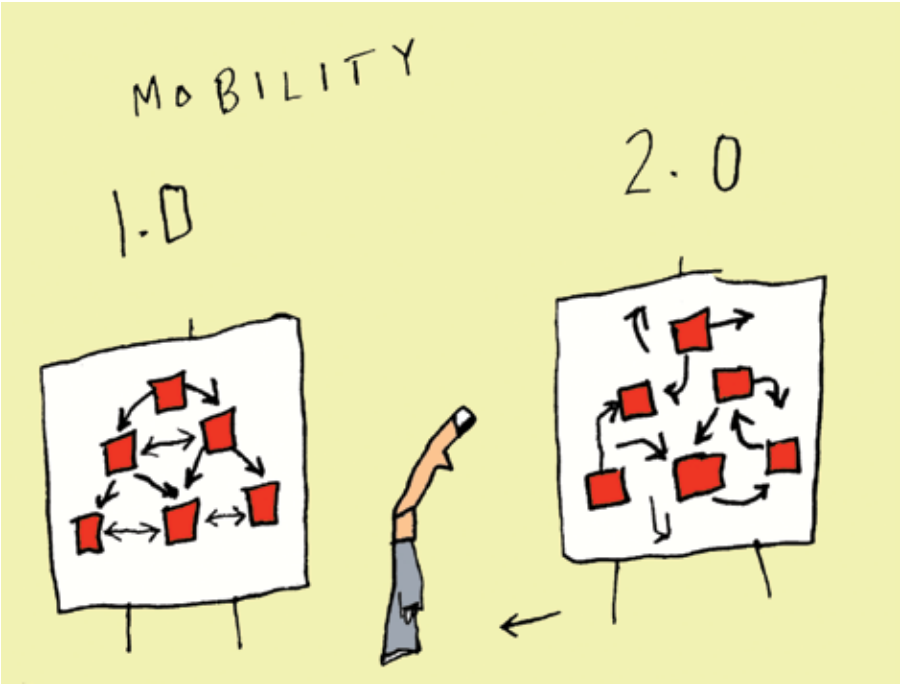
By Guy-Marie Joseph + Pascale Dominique

More mobility shift

Sound management and an understanding of risks and controls will help decision-makers benefit from new technologies



The world of information technology has seen many radical changes over the past few decades. In addition to the evolution of technology we have had to deal with the arrival of mobility, which goes beyond simply receiving messages on a personal digital assistant. That is in the past.

Innovations in the field of mobility, or mobility 2.0, impact internal controls and can create difficulties for systems auditors. The difficulties are often due to a lack of understanding of the technologies, which complicates the implementation of adequate controls.

In October's *CAmagazine*, "The mobility shift" (p. 44) examined convergence of voice and data, cloud computing and other factors that have hastened the implementation of wireless networks throughout organizations, all factors that have redefined the profile of the traditional mobile user.

Although the economic gains are clear, the risks associated with these new technologies continue to impede their implementation. The risks and the internal controls that can be applied to reduce them to an acceptable level, while reaping the benefits of these technologies, should also be examined.

Harmonizing information technology with corporate strategies, while ensuring that systems are adequately protected with an acceptable level of risk are constant challenges for IT teams. What's more, the emergence of technologies such as cloud computing reinforce the need for good governance.

Fewer and fewer critical systems, whether tangible or intangible, are being kept in house. As a result, it is important to define internal usage policies, evaluate mobility-associated risks and educate employees about risks and related controls. In addition, auditors must be familiar with new technologies, best practices and the tools that can reduce these risks.

MIKE CONSTABLE

While this is not an exhaustive analysis of these issues, the focus is on the risks and controls associated with each issue.

Portable units

Devices such as personal digital assistants (PDAs) run multiple operating systems that support a variety of tools and numerous applications configured specifically to the devices' environments. They can be synchronized to internal systems through wired, infrared and wireless infrastructures. Most of these devices accept Compact Flash and SmartCard memory cards, among others.

Physical risks

- loss of peripherals;
- theft and fraud arising from the use of stored data;
- damage that can adversely affect the company's reputation;
- data theft by shoulder surfing;
- clandestine monitoring of network traffic, resulting in attacks on these devices and illegal access to the company's network;
- often excluded from asset-management policies, the use of personal tools for business purposes forces managers to improvise; and
- consumer-oriented devices are not as well designed when it comes to security.

Application risks

- the complexity of these new technologies makes it difficult for IT teams to implement an adequate level of security;
- the high storage capacity of mostly unencrypted data increases risk;
- user-access authorizations are sometimes excessive, resulting in downloads of normally prohibited data; and
- security updates are not always managed or installed.

Controls

Plan to establish IT governance for mobility 2.0;
As regards physical risks:

- implement formal policies on the use of these devices that will differentiate between personal units included under these policies and those excluded;
- define an asset management and classification policy;
- ensure users read and comply with the policy;
- provide for the right, at the company's discretion, to audit these units; and
- educate users on prevention and make them aware of the risks, such as shoulder surfing, loss and theft.

As regards application risks:

- identify and define a corporate standard for mobile units used and accepted in business;
- ensure these devices use recognized, tested and supported operating systems, since it is difficult to control emerging risks when multiple platforms are deployed;
- integrate security functions into the applications such as more complex passwords; a time-out system requiring users to re-enter their password after a certain period; and a password prompt when synchronizing or turning on the unit;
- strengthen and add security features to applications developed with tools sold by third parties, including biometrics (signature, voice, fingerprint- or pictogram-password recognition); tokens (two-factor authentication); data and application encryption (a minimum of 128 bits), and WPA2 wireless encryption and more, as recommend by the 802.11 standard; PKI infrastructure and the use of certificates (note that this type of infrastructure is complex and therefore difficult to set up and to manage); encryption between the units' data transmission and the access points; deployment of antivirus software and firewalls on the units; and policy ensuring security updates.

IP telephony (VoIP)

The telephone system is now merely an extension of the applications that use the Internet protocol (IP), leading to centralized and consolidated management. In addition, open standards allow for the integration of equipment from different suppliers, which is more cost effective.

Risks

Quality of service

- loss of packets;
- instability; and
- latency.

Security

- vulnerable to the same attacks as IP networks: viruses, DoS, packet spoofing (identity theft, disclosure of confidential information); and information travels out in the open;
- difficult to plan system downtime for preventive maintenance; and
- internal intruders are also a threat.

Controls

- physical security of the hardware;
- encryption of data transmissions (traffic encryption);
- network segmentation and voice and data separation on different VLANs;
- a separate server for telephony and data; and
- configuration of firewalls to filter unauthorized traffic.

Wireless networks

Information travels through the air by radio frequency. Such information includes critical application data as well as voice transmissions (VoWLAN). While these networks appear simple to deploy, installing and maintaining them require qualified personnel.

Risks

Wireless networks are exposed to the same risks as wired networks, but other significant vulnerabilities should be noted:

- eavesdropping;
- illegal access to the network;
- denial of service attacks (DoS); and
- use of nonapproved protocols.

Controls

- a multilayered approach is a recommended best practice for access control, authentication and wireless data encryption;
- network deployment and policies: deploy a minimum access port (AP) for adequate coverage; ensure that the AP transmits at the lowest level; ensure coverage of the building, both inside and outside; maintain installation policies for APs, network interface cards and WLAN user groups; and support authorized 802.11 protocols (e.g.: a/b/g/n);
- access control: configure in WPA or WPA2 mode for a high level of data encryption; change the SSID as often as possible (at least avoid a nomenclature displaying the nature of the SSID);
- control SSID distribution; verify the media access control addresses of all peripherals connected to the WLAN; and maintain access and denial policies for all unrecognized peripherals;
- security perimeter: install a firewall as well as intrusion detection and prevention systems; use VPNs to encrypt network traffic and route it through these servers; maintain and apply VPN access and routing policies; configure client accesses properly; and install a dedicated wireless intrusion protection system;
- application security: verify access privileges and user authentication for application purposes; maintain and apply access permissions and password management; and install patches from the manufacturer as soon they are released.

Cloud computing

An evolving field, cloud computing is a 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 (as defined by the National Institute of Standards and Technology).

Risks

The Cloud Security Alliance categorizes risks under governance and operational domains:

Governance:

- legal implications;
- contract content;
- financial viability of the supplier;
- crossborder considerations;
- compliance with current laws and regulations;
- audit and compliance;
- data security and protection;
- transfer of data to another supplier;
- Patriot Act for data stored in the US; and
- applicable privacy legislation.

Operations:

- authentication;
- integration with the company's other systems;
- system availability;
- business continuity ;
- disaster plan;
- incident management;
- accessibility.

Controls

- keep an inventory and classification of outsourced assets;
- ensure that a service-level agreement exists that meets the company's needs;
- ensure that the data does not come under the USA Patriot Act;
- ensure compliance with privacy legislation;
- plan an annual audit of suppliers' websites and a review of their policies on security, disaster planning, incident management, and skill and certification maintenance for technicians in charge of the systems.

Conclusion

New technologies offer many business opportunities. Every risk and internal control-related element cannot be covered in a brief article, but this is an overview of how to appropriately manage mobility risk and to show the importance of implementing internal controls. These controls may be similar to traditional methods, but IT auditors are required to thoroughly understand them. Understanding risks and controls, together with sound management, will help informed decision-makers benefit to the fullest extent from these new technologies.

Guy-Marie Joseph, MA, is president and head of the mobility, security and IT sector for ConnecTalk in Montreal (gjoseph@connectalk.com). Pascale Dominique, CA, CA•IT, CISA, is vice-president of finance and head of application development for ConnecTalk in Montreal (pdominique@connectalk.com)

Technical editor: Yves Godbout, CA•IT, CISA, director of IT services, Office of the Auditor General of Canada(godbouy@computrad.com)