



# Leveraging Mobile & Remote Computing Technology

---

A Decision-Maker's Guide

*November 28, 2007*

*AICPA – IT Executive Committee*

*Mobile and Remote Computing Work Group*

# Leveraging Mobile & Remote Computing

---

## A Decision-Maker's Guide

November 28, 2007

### AICPA - IT Executive Committee Mobile & Remote Computing Work Group

© 2007 American Institute of Certified Public Accountants, Inc.

This discussion paper is part of a series of Content Suites created by the AICPA's IT Executive Committee to help Information Technology Section members and Certified Information Technology Professional (CITP) credential holders in their everyday technology life. Opinions of the authors and the AICPA staff involved are their own and do not necessarily reflect policies of the Institute or the Information Technology Section. Any hardware or software products mentioned do not in any way represent an endorsement by the Institute or Section.

All rights reserved. This document may be copied and distributed subject to the following conditions:

- (1) Copy all text without modification and include all pages.
- (2) All copies must contain the AICPA copyright notice and any other notices provided therein.
- (3) You may not distribute this document for profit.

# Leveraging Mobile & Remote Computing

## A Decision-Maker's Guide

---

### Table of Contents

<b>1. Introduction .....</b>	<b>3</b>
1.1. <i>Objective of this Discussion Paper</i> .....	3
1.2. <i>Who Should Be Reading This</i> .....	4
<b>2. Background and Relevancy.....</b>	<b>4</b>
<b>3. Mobile &amp; Remote Computing Decisions.....</b>	<b>6</b>
3.1. <i>Network Infrastructure</i> .....	6
3.1.1. <i>Internally Hosted Server-Client Solutions</i> .....	6
3.1.2. <i>Remote Control Solutions</i> .....	7
3.1.3. <i>Web-Based Applications</i> .....	8
3.2. <i>Mobile &amp; Remote Devices</i> .....	8
3.2.1. <i>Laptop Computers</i> .....	8
3.2.2. <i>Blackberries, Smartphones and PDAs</i> .....	9
3.3. <i>Mobile &amp; Remote Computing Peripherals</i> .....	9
3.3.1. <i>Portable USB Storage Devices</i> .....	9
3.3.2. <i>Printers</i> .....	10
3.3.3. <i>Scanners</i> .....	10
3.4. <i>Software</i> .....	10
3.4.1. <i>Secured Access Solutions</i> .....	10
3.4.2. <i>Collaboration Tools</i> .....	11
3.4.3. <i>Communication Applications</i> .....	12
3.5. <i>Policies and Security Considerations</i> .....	12
3.5.1. <i>Physical Loss</i> .....	13
3.5.2. <i>Unsecured Access</i> .....	14
3.5.3. <i>Unsafe User Behavior</i> .....	14
<b>4. Mobile &amp; Remote Computing Solutions .....</b>	<b>15</b>
4.1. <i>Flexible Work Arrangements &amp; Home-Based Workers</i> .....	16
4.2. <i>A Well Connected Mobile Workforce</i> .....	16
4.3. <i>Temporary Worker Accommodations</i> .....	17
4.4. <i>Disaster Recovery &amp; Business Continuity</i> .....	18
4.5. <i>Client Self-Service</i> .....	18
<b>5. Conclusion.....</b>	<b>19</b>
<b>6. Acknowledgements .....</b>	<b>20</b>
<b>7. Glossary of Terms.....</b>	<b>21</b>

# Leveraging Mobile & Remote Computing

## A Decision-Maker's Guide

---

### 1 Introduction

Business is no longer restricted to the office. Mobile computing, collaboration tools, remote access technologies and communication devices now make it possible for workers to remain in touch with the office from virtually anywhere, during the traditional workday and even after hours. As a result of extended office hours and increased flexibility, organizations have realized substantial gains in efficiency, and worker productivity. Checking company e-mail remotely via Blackberry or webmail application takes *seconds* – a small investment of time, but one that can take the surprise out of the employee's first few hours in the office, helping them keep project plans on track, and make better use of their day. In many cases, smaller organizations may be able to operate in an entirely virtual environment, with no need for physical offices at all.

Mobile & remote computing lends flexibility to even the most rigid business environments. Employees are able to access e-mail, customer and client databases, and most other critical systems through secure Internet-based connections, using portals to store and share information, and virtual private networks to keep prying eyes away from sensitive data. Mobile technology solutions can also increase the accuracy of workers in the field, reduce the costs of managing an IT infrastructure and help organizations get the most out of their staff, regardless of where they happen to work or reside.

“Going mobile” is not a one-step process. It is not something organizations simply “decide” to do. Mobile & remote computing implementations involve a series of important decisions regarding infrastructure, security, software, device deployment, document management and much more. Instead of allowing the technology to *drive* the process, organizations need to determine their business objectives, review their existing IT infrastructure, and determine which mobile & remote computing technologies would be most appropriate given their stated objectives, business needs, available resources and budget.

Years ago, mobile & remote computing and its supporting technologies were familiar to only a few early adopters and large organizations with substantial IT budgets and healthy appetites for innovation. Today, networked-enabled laptops with remote access capabilities have become standard issue for many organizations, and the adoption of mobile handheld devices, web-deployed applications and services, and telecommuting initiatives continues to grow. Given the trends, the potential benefits and today's competitive business environment, no organization, regardless of size or focus, can afford to ignore the benefits of mobile & remote computing.

#### 1.1 Objectives of this Discussion Paper

The AICPA Information Technology Section's discussion paper *Leveraging Mobile & Remote Computing: A Decision-Maker's Guide*, is intended to provide a contextual framework in which to discuss mobile & remote computing technologies and how organizations of various sizes, including CPA firms and other businesses can leverage them to derive significant value. It is also intended to communicate the basic information necessary to begin planning and implementing a mobile & remote computing initiative into a firm, business or other type of organization.

# Leveraging Mobile & Remote Computing

## A Decision-Maker's Guide

---

There are many resources available to learn more about mobile & remote computing – many of which are located on [AICPA's IT Center](#). In addition, because this topic has appeared numerous times on the AICPA's Top Technology Initiatives list, the AICPA's IT Executive Committee created this discussion paper as one component of the [Remote & Mobile Computing Content Suite](#) which also contains:

- **Mobile & Remote Computing Case Study: Project Balance** - A case study demonstrating how one CPA firm, KAF Financial, has employed mobile and remote computing technologies and flexible work arrangements to increase productivity, improve customer service, enhance recruitment efforts and further work-life balance.
- **Glossary of Mobile & Remote Computing Terms** - A glossary of mobile and remote computing technologies and terms intended to provide a primer for those new to mobile and remote computing, or good refresher for those in-the-know.
- **Mobile & Remote Computing Sample IT Policies (Template)** - A sample IT policy document that can be modified to help formalize and articulate IT policies to employees, which incorporates specific policies crucial to any organization implementing mobile and remote computing initiatives.
- **Mobile & Remote Computing Sample IT Policies (Annotated)** - An annotated version of the Sample IT policies document with notes explaining the rationale for various policies, as well as practical implementation advice.
- **Top Technology Initiatives Podcast** - A podcast featuring IT thought leaders Jim Bourke, CPA.CITP, John Seale, CPA.CITP, and David Ryan, CPA.CITP discussing the mobile and remote computing technologies and how organizations are leveraging these technologies to maximize efficiency, productivity, customer service and work-life balance.
- **Mobile and Remote Computing Case Studies (Web Seminar)** - A web seminar hosted by Robert Gaby, CPA, CITP of Arxis Technology Group, Inc. during which he introduces CPA firm technology leaders John Seale, CPA, CITP; Barry MacQuarrie, CPA, CITP; and Jim Bourke, CPA, CITP, and moderates a discussion about mobile & remote computing technologies, and how their firms have been able to leverage them to achieve substantial benefits.

### 1.2 Who Should Be Reading This

This document is intended to assist IT decision-makers in public practice and business and industry, and those who influence IT decisions. Because mobile & remote computing is pervasive throughout the business marketplace, the actual audience may be wider and more varied.

Intended audiences include:

- **Managing partners and shareholders** of small- to mid-sized firms who are considering an implementation or expansion of mobile & remote computing capabilities, and are looking to explore available options.
- **CIOs, IT Managers and Consultants** looking to “sell the case” for expansion of mobile & remote computing capabilities to the stakeholder(s).

## 2 Background and Relevancy

In 2007, the AICPA included Mobile & Remote Computing (MRC) among its [Top Technology Initiatives](#) in recognition of the significant influence that MRC is likely to have on the accounting profession in the coming years. MRC has already had a significant impact in the way in which work gets done, and increased adoption will only compound its effects. The 2007 Top Technology Initiatives list defines MRC as “technologies that enable users to securely connect to key resources anywhere, anytime regardless of physical location.” The specific technologies that enable and support mobile & remote computing are varied, but include mobile end-user devices such as laptops, tablet PCs, PDAs and Smartphones; wireless technologies such as Bluetooth, Wi-Fi and WiMax; and remote access technologies such as Windows Terminal Services and Citrix Presentation Server.

# Leveraging Mobile & Remote Computing

## A Decision-Maker's Guide

---

Despite the hype, MRC is not new. Many large organizations have had mobile and remote capabilities in place for years, but these were most often early adopters; organizations with sufficient resources to absorb the significant infrastructure and support costs, as well as the risk associated with the adoption of emerging technologies. MRC was not a viable option for smaller organizations that had neither the appetite for IT risk nor the resources and personnel necessary to deploy new technology effectively.

Times have changed. There has been an explosion in the adoption of mobile & remote computing technologies as a result of the ubiquity of low-cost, high speed connectivity and the widespread availability of inexpensive MRC devices and technologies. Because of these advances, the costs associated with MRC have decreased to the point that nearly any organization, regardless of size or available resources, can implement a basic level of mobile and remote capability and begin taking advantage of the compelling benefits that properly implemented MRC initiatives can offer.

The emergence of mobile & remote computing is having profound effects on the way in which organizations operate. Consider the impact that remote access technologies have had on business systems, extending them into the homes of employees and allowing them to take critical business resources with them on business trips or long commutes. What was once a traditional five-day, 40-hour workweek where local systems and cables tethered employees to their desks, has now become a flexible work environment in which employees can leverage persistent network connectivity to do work wherever and whenever they need. As a result, work-related problems developing overnight may be confronted during off hours, so that a plan of action can be formulated and in some cases implemented before the employee arrives at the office the next day.

Mobile & remote computing also allows organizations to accommodate homebound workers, mobile workers and others working in non-traditional environments. Geographically dispersed employees are able to be every bit as productive as those in the office, allowing organizations to benefit from high performing workers even when business or personal matters keep them from the office.

Technological advances, reduced costs and a salient business case have made mobile & remote computing standard for businesses of all sizes. Many forward-thinking, technology-smart organizations have been able to leverage MRC technologies to achieve strategic competitive advantages in areas such as recruitment, retention, customer service and return on investment. The list of benefits that can be achieved through mobile & remote computing is impressive, and includes:

- Elimination of geographic restrictions
- Improved customer service
- Enhanced and more timely communication
- Flexible schedules and higher level of employee work-life balance
- Productivity gains
- Increased ability to attract and retain quality employees
- On-demand access to information and systems
- Reduced commuting costs and costs related to nonessential trips
- Reduced "brick and mortar" dependency and/or cost
- Facilitated succession, through the extension of flexible work arrangements to critical personnel, who due to life transition are not able to work a traditional 40 hour, in-office work week

# Leveraging Mobile & Remote Computing

## A Decision-Maker's Guide

---

### 3 Mobile & Remote Computing Decisions

The benefits of implementing a mobile & remote computing initiative are compelling and clear. What is not quite so clear is how to get started. There is no one size fits all MRC solution. One organization may be looking to increase productivity through the extension of the traditional workday, while another may be looking to build a virtual organization.

The question “What mobile & remote computing is right for my organization?” has many answers and depends on several factors. Organizations need to think about what they want to accomplish and the level of internal IT expertise and support available to them, and then determine the most appropriate solution. Budgets are also a major consideration, as is the overall culture of the organization and how it impacts risk.

Once an organization has determined their objectives and rationale for pursuing an expansion of mobile & remote computing capabilities, and evaluated their existing environment and available resources, the considerations become decidedly more tactical. To select and implement an effective MRC solution, management must make a number of tactical decisions related to two general categories:

- Network infrastructure, including software, hardware and end-user devices
- IT policy and security.

While decisions related to the selection of the remote access solution, supporting devices and software are important, the development, implementation and enforcement of comprehensive IT policies to support these technologies are equally important. Technology, in and of itself, is of little value without an overarching operating model that defines how the system will be monitored and used so as to minimize risk, maximize productivity gains, and prevent misuse or abuse.

#### 3.1 Network Infrastructure

Network infrastructure is key to implementing an effective mobile & remote computing environment. There are many technologies that make mobile & remote computing happen, including software, hardware and end user devices. The precise configuration you choose ultimately depends on the remote desktop solution chosen. Available options fall into one of three general categories: internally hosted server-based solutions, remote control solutions and web-based applications or Software as a Service (SaaS).

##### 3.1.1 Internally Hosted Server-Client Solutions

Server-based solutions involve server-client relationships and software configurations that support the deployment of critical business applications remotely over the Internet and/or an internal network. In the server-client model, applications reside on and are run off a server as opposed to the user's personal computer or computer device. In this arrangement, the server provides all the computing power necessary to run the application, while the client or local computer device provides an interface for interacting with the network-hosted application. A user only needs client software installed on their local desk- or laptop computer. The internally hosted server-client solution is the most popular enterprise-level solution, and [Citrix Presentation Server](#) or [Windows Terminal Services](#) are the two most notable products.

The advantage of internally hosted server-client solutions is that they allow users to run applications without having them installed on their desk- or laptop. Clients can be configured to run all applications, or just a few. It is common practice for businesses to deploy Microsoft Office applications and other productivity software to run locally, so that end users remain productive even in instances where connectivity is limited or unavailable. Adoption of an internally hosted server-client solution can also

# Leveraging Mobile & Remote Computing

## A Decision-Maker's Guide

---

lead to a reduction in IT support cost associated with the deployment of software updates, upgrades and patches, because deployment is centralized and automatically pushed to users, eliminating the need for IT to manually update each user's computer.

On the downside, the software licensing, server hardware, maintenance and support can be very expensive for internally hosted server-client solutions. While centralization should help offset some of these costs over time through reduced user support costs (less support needed for staff in the field) and lower end-user computing costs (user don't require the most powerful computers), the internally hosted server-client model is the most expensive, and does require substantial investment on the front end. Another disadvantage of this approach is that network-enabled computers and devices become gateways to the organization's network resources that if lost or stolen could be used by unauthorized parties to gain access. Also, as with any remote desktop solution, internally hosted server-client configurations require the user to have an Internet connection in order to run applications remotely.

### 3.1.2 Remote Control Solutions

GoToMyPC and LogMeIn are examples of remote control solutions in which a direct connection is established between a locally networked PC and a remote device allowing users remote access to the applications, files and network connections available on the locally networked computer. In the most common environment, a user will have GoToMyPC, LogMeIn or another remote control solution installed on their primary work computer providing them access to that computer from another remote computer via the remote computer's web browser. The remote user will see their primary desk- or laptop computer screen as if they were physically sitting in front of it and are able to access and use any of the primary computer's applications, data and connections. In remote control situations, users gain access to internal network resources through the existing connections on their primary desktop, which serves as an intermediary between the network and the remote device. They may also access applications and files stored locally on the primary device, because the remote computer or device provides an interface for interacting with the primary computer device.

The advantage of a remote control solution is that it is relatively inexpensive to setup up and maintain. In many cases, it can be configured in less than an hour. It also does not require any additional investment in server hardware. Because remote control solutions require less upfront investment, and are easy to deploy and configure, they are a great mobile & remote computing option for smaller organizations with limited IT budgets and existing network infrastructure.

One disadvantage is that remote control remote desktop solutions require users to have two separate computer devices, a primary device which is directly connected to the network, and a remote device configured to control the primary one. In this scenario, organizations may be responsible for purchasing and supporting both the primary and remote computers, paying more for end-user devices – laptops, and desktops – than they would in an internally hosted server-client solution. One way around this is to make a remote control solution available to users, but make the user responsible for purchasing the remote device. This makes it difficult, however, to enforce IT policies and ensure that the employee-owned remote devices conform to established security configurations that prevent unauthorized access to the remote computer. Accordingly, organizations opting for this arrangement may decide in favor of a more restrictive remote control configuration that prevents users from saving or printing network files or data locally on the remote device.

Organizations should also ensure that their remote control solution is configured so that the primary computer's keyboard is locked and that its monitor is blacked out when it is being accessed remotely. This will prevent unauthorized access and disclosure of sensitive information within the office while the user is accessing the device remotely.

# Leveraging Mobile & Remote Computing

## A Decision-Maker's Guide

---

### 3.1.3 Web-Based Applications or Software as a Service (SaaS)

Another mobile & remote computing option involves the use of web-based software services where applications are hosted by a service provider on their server, deployed over the Internet and accessed through the user's web browser. This arrangement is commonly referred to as software as a service (SaaS). In the SaaS model, applications are supported by third party vendors who lease their applications to end users, and run remotely over the Internet through secure connections. This kind of third party hosting generally involves specific business applications which are generally server-deployed; applications such as audit, tax, and general ledger software that are not typically installed and run on the end user's device. As the world heads toward a more centralized, web-based computer environment, however, businesses are also starting to move away from local deployments of common desktop software like Microsoft Office in favor of web-based deployments of these applications as well. In a sign of the times, Google recently implemented free web-based word-processor and spreadsheet applications complete with online document storage.

The advantage of utilizing third-party, SaaS applications as opposed to internally-hosted applications or software configured to run locally on the end-user device, is that SaaS products are extremely easy to deploy and usually require no hardware or support. As a result, they can be significantly less expensive. SaaS can also be implemented more quickly than internally hosted software, and organizations benefit from only having to purchase as much software as they need. They can always purchase additional licenses on an as needed basis as the organization grows, without the worry that subsequent releases will necessitate expensive hardware upgrades. Cost advantages are deepened by the fact that end user computer costs can be kept low, because the third party's server performs the bulk of the heavy-duty processing and user devices needn't be as powerful as when applications are hosted and run locally. Another significant advantage of SaaS is that it allows for much more accurate forecasting of IT overhead, because the software service is run on the provider's network for a set fee, and they are responsible for its support, maintenance and optimization.

A disadvantage of SaaS is that the applications tend to be less customizable due to the fact that generic configurations make it easier for providers to push updates to their clients more efficiently and helps keep the cost their low. Control over security and data back-up is also a concern. Accordingly, organizations should perform due diligence before purchasing a service contract to ensure that the provider's security and back-up practices meet or exceed internal standards.

## 3.2 Mobile & Remote Devices

In today's business environment it seems that being connected to the office at all times is the norm. Compact end-user devices are a substantial part of the driving force behind the mobile & remote computing trend. Laptops, Blackberries and Smartphones enabled with wireless technologies such as [Wi-Fi](#), [EVDO](#) and [EDGE](#) are having a major impact on how and when business is conducted. They allow users to squeeze productive work into even the smallest amount of downtime. As a result, users can be plugged into their organization's resources, applications and data as if they were in the office, regardless of where they are physically located.

### 3.2.1 Laptop Computers

Laptop computers fueled the initial push towards MRC. Their widespread availability has made it possible for users to bring critical applications and data with them anywhere, either literally in the case of productivity software which is installed and run locally, or by facilitating remote interaction with SaaS or applications hosted internally. Laptop computers make MRC practical, because they can be used as a mobile or remote worker's primary device regardless of whether or not they are in the office.

Laptops should be selected based on the needs of the end user. Users whose job functions require them to do a lot of typing may benefit from a model with a full-sized keyboard, while light weight models may be

# Leveraging Mobile & Remote Computing

## A Decision-Maker's Guide

---

a better choice for highly mobile workers. Organizations may choose laptop models with drive encryption, or biometric capabilities such as built-in fingerprint scanners to provide additional layers of security. Many companies issue standard laptop models – a handful of models from one or two manufacturers - based on the user's job description and the unique requirements of their position. Adopting standard device models allows internal IT support to familiarize themselves with the devices, enabling them to quickly setup, fix or replace devices when a problem occurs, reducing support costs as well as user down time. Standardized laptop options allow organizations to order in bulk and realize substantial cost savings. As the price of laptops has come down, many companies are choosing to deploy laptops over desktops to allow users additional flexibility, and to support continuity planning in the event of a service outage or other disruption of business at the office.

### 3.2.2 Blackberries, Smartphones and PDAs

The development, availability and affordability of ultra-mobile, hand-held computer devices such as Blackberries, Treos, and Smartphones have intensified the push towards mobile & remote computing, enabling users to truly stay connected anytime, anywhere. These devices feature persistent connectivity via cellular broadband services such as EDGE or EVDO, and offer remote users real time access to e-mail, calendars, address books, tasks, notes and the Internet. They also multi-task as cell phones and can be used to view and edit Microsoft Office documents as well as PDFs and other files. These devices can also run a number of useful applications, including the free [Voice over IP \(VoIP\)](#), and navigation software, which can be used to find directions and view maps. Handheld devices are also easy to use and intuitively designed for viewing and typing text, and may be the only device necessary for users whose primary concern is being able to send and receive e-mail. For those who do need the more robust computing that a laptop provides, some handheld devices, depending on the wireless carrier, can double as broadband modems providing persistent Internet connectivity through EVDO and EDGE networks.

### 3.3 Mobile & Remote Computing Peripherals

When it comes time to outfit the mobile and remote work-force with additional devices, tools and add-ons to help make them more productive in the field, there are many options for decision-makers to consider. Three categories of peripherals that warrant consideration are portable USB storage devices, printers and scanners.

#### 3.3.1 Portable USB Storage Devices

Portable storage devices such as USB thumb or stick drives, external hard drives, and even portable media players like the iPod provide a convenient and easy way for mobile and remote workers to store their data and conveniently transfer digital documents from one device to another. USB drives are highly portable with hefty storage capacities. Their compact nature coupled with the fact that they can be used with any computer that possesses a USB port, makes them an essential accessory for the mobile and remote worker.

In addition to their common usage as portable repositories of digital data, portable USB drives may also be used to store and deploy portable applications so that users can utilize their own applications on any computer with a USB port. So far, the most common type of applications deployed in this manner are e-mail clients and web browsers, but portable versions of office productivity software and other productivity applications also exist. The major advantage of USB drives and USB-deployed applications is that they enable users to access to their applications without having to carry their laptops around. Also, because applications are run from the removable USB drive, it is less likely that users will leave sensitive information on the hard drive of any foreign devices they might use, as they might with remote access solutions.

Convenience notwithstanding, there are a number of poignant security concerns associated with portable USB devices. Because they are so compact and so portable, they tend to be easily misplaced, stolen or left

# Leveraging Mobile & Remote Computing

## A Decision-Maker's Guide

---

behind. This makes encryption of USB storage devices absolutely essential, especially when such devices contain sensitive information. There are a number of quality encryption products on the market that can be used to create encrypted directories on digital storage media, including USB drives, optical hard drives and CD- or DVD-ROMs.

Another security issue related to portable USB storage devices has to do with the fact that they are frequently used on computers which do not fall under the organization's security perimeter. When a USB storage device is plugged into a computer it becomes vulnerable to any viruses, Trojans and any other malicious software or code that might be lurking on that device. For this reason, users should be selective about the computers with which they use their USB devices. At a minimum, users should check to make sure that the computers with which they use their portable storage devices have active and up-to-date anti-virus software, and it is best to avoid public computer kiosks altogether.

### 3.3.2 Printers

Printers are another class of devices that should be considered when outfitting mobile and remote users. MRC users who frequently have a need to print documents out on paper should consider a light-weight, portable printer that can easily be carried with them when traveling on business. There are numerous portable models available, many of which measure only about 1/3 of the size of laptop computer. Another option is for users to carry a USB printer cable with them, allowing them the option to print on any available printer including those belonging to a client or hotel. Alternatively, in instances where a fax machine is available, remote users may send documents to a local fax machine via fax client software installed on their laptop. This is a perfectly adequate workaround in situations when there is either no printer available or when a technical problem impedes the use of an available printer.

It is important to note that remote printing can pose serious risks to confidentiality and the privacy of client, customer and employee information. Because remote users run the risk of remotely printing to a device to which they do not have access, remote printing of sensitive documents (i.e., client files, legal contracts, etc.) be avoided unless absolutely necessary, especially when it is perfectly acceptable to store and distribute files electronically.

### 3.3.3 Scanners

Scanners allow MRC users to digitally capture, file and store paper-based information digitally. For this reason, organizations may decide to equip their mobile and remote workers with portable scanners, especially if they have a frequent business need, as is the case with auditors, to convert paper documents into electronic files. There are a number of portable scanners on the market, many only a third of a laptop in size. One clever work-around for remote users who need to digitally capture paper documents, but lack access to scanner is to fax documents to their fax client software and file the resulting image file on their laptop as appropriate. Using this method effectively turns the available fax machine into a scanner.

## 3.4 Software

In addition to the remote desktop solutions noted above, there are additional software technologies that facilitate the creation of an effective and secure MRC environment. These include secured access solutions, communication applications and collaboration tools that allow users to share information and communicate both efficiently and securely.

### 3.4.1 Secured Access Solutions

There is no refuting that MRC involves increased security risks. The extension of security end points beyond the protection of an organization's internal security perimeter makes it easier for security gaps to occur. Fortunately, there are a number of software solutions that can be implemented to shore up mobile security end points, enabling organizations to boost employee productivity while reducing the

# Leveraging Mobile & Remote Computing

## A Decision-Maker's Guide

---

organization's risk exposure to an acceptable level. [Virtual Private Network \(VPN\)](#) and [Secure Socket Layer \(SSL\)](#) or [Transport Layer Security \(TLS\)](#) technologies represent popular and effective tools in the effort to keep remote connections and communication secure.

The term VPN refers to a class of software technologies that creates an encrypted Internet connection between a remote device and an organization's private network, enabling remote users to securely access internal network resources residing within an organization's firewall. In effect, VPN establishes a closed communications network tunneled through a larger network such as the Internet. This ensures that remote workers have access to everything that would be available to them within the company's walls, including internally hosted applications and data, intranets, e-mail and printers, while preventing unauthorized users from tapping into the connection to intercept transmitted information or gain access to the network. All organizations enabling remote connection to internally-hosted network resources via the Internet should employ VPN technology.

Transport Layer Security (TLS) and its predecessor Secure Sockets Layer (SSL) are web security protocols that employ encryption to provide for secure client-server communication over the Internet for things such as web browsing, e-mail, Internet faxing and instant messaging, while significantly reducing the likelihood of eavesdropping, tampering, and message forgery. Organizations establish SSL or TLS encryption on websites where secure data is transmitted. Websites employing the SSL or TLS protocols are noticeable different from other websites in that their web addresses begin with "https" rather than "http." Most Internet users will recognize SSL or TLS on websites that handle credit card transactions, but the technology can be extended to accommodate the communication of any sensitive data over the web. The cost of deploying VPN and SSL or TLS technologies vary depending on the size of the organization, the number of remote users, and the number of applications the organization wishes to secure.

[File Transfer Protocol \(FTP\)](#) is another option for secure transmission of sensitive information by remote workers via the Internet. FTP is an open standard that allows documents to be securely transferred between two computers, an FTP server and an FTP client, via a network such as the Internet. Remote users use the FTP client (included within most web browsers) to download and upload files to the FTP server. FTP implementations should employ SSL or TLS technology, but are otherwise relatively easy and inexpensive to implement. They may be supported internally, or purchased and hosted as a subscription from a third party provider.

### 3.4.2 Collaboration Tools

While FTP sites store files and support secure transfer of relatively large files over the Internet, collaboration tools such as intranets, [wikis](#) and [portals](#), including [Microsoft Sharepoint](#), make it easier to structure and share information, substantially reducing the amount of time that users spend searching for files, documents or other information. Intranets employ basic website technology and enhanced security to create online environments within which internal users can share sensitive information (e.g. IT, HR and accounting policies, phone directories, customer lists) across the organization. An intranet is essentially a miniature version of the Internet, which is closed to facilitate the exchange of information among a community of internal users. Information, documents and files are posted to sites within the intranet to be accessed by other intranet users via their web browsers.

Portals such as Microsoft's SharePoint technologies offer out-of-the-box intranet frameworks that can be implemented quickly to deliver additional functionality, such as wikis, discussion boards, and blogs to enhance collaboration among intranet users. Portal users are not only able to access or retrieve information, but can also add, remove and edit content on pages.

# Leveraging Mobile & Remote Computing

## A Decision-Maker's Guide

---

### 3.4.3 Communication Applications

Communication is key in any work environment, but especially in mobile and remote environments where team members are often in disparate locations, and unable to engage in face-to-face interaction. In order for a mobile or remote environment to be effective, workers need to have the ability to interact with their co-workers with the same ease and frequency as if they were physically together in the office. Fortunately there are a number of technology solutions available that can help facilitate this level of communication between remote workers and others within the organization.

Webmail secured with SSL or TLS technology ensures that all remote users have reliable, secure access to e-mail, even if their device lacks a formally configured connection. Because webmail is hosted on the Web, users are able to access their e-mail from any computer with an Internet connection and a web browser. Larger organizations still tend to utilize VPN to facilitate access to an internally hosted e-mail server, so for them, webmail is a secondary access option for e-mail. However, there are a number of organizations – usually smaller in scale – who rely on webmail as their only option for remote e-mail access. The advantage of webmail is that it can help reduce technology overhead, by outsourcing end-user support and e-mail server maintenance.

[Instant messaging \(IM\)](#) is another valuable communication software tool. Once thought of as a fluff technology for tech-savvy Gen-Xers and Millennials, IM has matured into a viable business application, enjoying widespread adoption across organizations of all sizes. The beauty of IM is that it lets employees communicate back and forth as quickly as if they were having a real-time conversation, providing an easy way to ask a quick question and get a quick response without the need to pick up the phone or type an e-mail. IM also allows individuals to communicate when a vocal conversation may not be appropriate, during teleconferences or virtual presentations for instance.

As with e-mail, IM should be hosted internally inside an organization's firewall, or purchased as a subscription from a secure third-party vendor who utilizes SSL or TLS encryption. IM is also similarly bound by rules and regulations governing document retention such as the Federal Rules of Civil Procedure, so organizations will need to establish and enforce formal IM retention policies, and clearly understand those of their 3<sup>rd</sup> party provider.

Voice over Internet Protocol or VoIP represents another critical software service that organizations implementing mobile & remote computing initiatives might want to consider. VoIP allows users located anywhere in the world to send and receive phone calls from their mobile workstation or hand held device as if they were in the office. VoIP is significantly cheaper than traditional telephone service, since equipment and cost-per-call is lower. There are still some noticeable differences in quality between traditional phone service and VoIP, which may be exacerbated by bandwidth problems, reduced transmission speed and heavy traffic. As time passes and technology progresses, however, this quality difference should become less and less of an issue.

One exciting development in the area of communication software is the emergence of [unified communication solutions](#) that enable users to send and receive voice, fax, e-mail, instant messages, images, video, and VoIP, and launch Web conferencing from a single interface by phone, PC, or Internet-enabled device. Unified communication solutions consolidate all of a user's digital communications on one convenient dashboard.

### 3.5 Policies and Security Considerations

With all of the compelling benefits associated with mobile & remote computing, it is easy to view it purely as a win-win situation. In reality, however, the deployment of mobile devices and the facilitation of remote access exposes an organization to a much greater degree of risk than a traditional non-MRC IT

# Leveraging Mobile & Remote Computing

## A Decision-Maker's Guide

---

environment. Because security endpoints in the MRC environment extend beyond the safety of the hardwired network and its firewall, there is greater opportunity for security breaches to occur, making a comprehensive security policy incorporating policy, training and enforcement absolutely essential. For one thing, handheld mobile devices are much more likely to be stolen, lost or misplaced by virtue of their compact size and portability. Mobile and remote devices also come in contact with viruses, Trojans, bots and other malware more frequently due to increased reliance on public networks and unfamiliar computer devices (printers, kiosks, etc.). In order to successfully manage the increased risk, formal policies outlining the proper use of organization resources need to be outlined and drawn up. These policies should address the three general areas of risk associated with mobile & remote computing: physical loss, unauthorized access and unsafe user behavior.

### 3.5.1 Physical Loss

The same qualities, size and portability that make these devices so convenient also make them much more likely to be lost, stolen or misplaced. Physical loss is inevitable. Given enough time, it is going to happen, and since these devices are network-enabled, a lost device exposes the organization to significant risk. Mobile devices serve as gateways to the organization's network and any information residing there. It is extremely important that organizations plan for the likelihood of loss or theft and consider policies that minimize the potential for damage by addressing security at the device level, application level and data level.

Organizations can provide device-level protections against physical loss by ensuring the mobile computing devices such as laptops are physically secured via cable locks or similar measures when used remotely or in the office. Users should also employ the "Lock Computer" functionality built into Windows by typing `ctrl + alt + del` and then "Lock Computer" when leaving their devices unattended, even for a minute. All computer devices including laptops and handheld devices should be password protected via "strong" passwords that are at least seven characters in length. Strong passwords involve some combination of capital, lowercase, numeric and special characters, to make them more difficult to crack. Organizations may also consider utilizing multi-factor authentication schemes at log-in requiring users to provide: 1) Something the user knows (Passphrases or answers to questions); 2) Something the user has (Tokens, i.e. Magnetic badges), and 3) A personal feature of the user (i.e. biometrics, including fingerprint or retinal scans). Many laptops ship with optional fingerprint scanners, making implementation of multi-factor authentication as simple as purchasing a specific laptop model.

To provide protection at the application level, organizations need to make sure that application access is also password protected via strong passwords. In the case of a VPN application, it is advisable that a separate and distinct strong password be required to grant access. This makes it that much more difficult for unauthorized users to gain access to critical network resources.

Data level protection involves the use of [encryption](#) to "scramble" data so that it is unreadable to unauthorized users who lack a decryption key or password. There are a number of encryption software products on the market that allow encrypted directories to be created on hard drives, USB drives, CD- or DVD-ROMs, and other media, as well as encryption products for e-mail and e-mail attachments. Encryption ensures that sensitive data stored on a lost or stolen device will not be disclosed to unauthorized users. Organizations should look for products that employ 128 bit encryption or higher.

# Leveraging Mobile & Remote Computing

## A Decision-Maker's Guide

---

### 3.5.2 Unsecured Access

To help guard against unsecured access, organizations should abide by the following rules of thumb:

- Always use Ethernet over wireless when available – it is inherently more secure
- Install and use acceptable firewall software
- Deploy Anti virus & Anti spyware software on all organization computers and computer devices
- Always use VPN when connecting to network resources remotely
- Be sure to deploy the latest security patches simultaneously to all computers and devices as they become available
- Use digital signatures and certificates when transmitting data via e-mail
- Encrypt documents that contain sensitive data before e-mailing them
- Ensure that Web-based applications are hosted using TLS or SSL secured websites (HTTPS)

In addition to these general guidelines, the following Wi-Fi best practices should also be communicated and enforced:

- Use [broadband wireless](#) over Wi-Fi, reserving Wi-Fi for Internet browsing only
- Turn-off all wireless capabilities (Wi-Fi 802.11a/b/g/n, Bluetooth, Infrared, and wireless broadband) when not in use
- Disable all ad hoc/peer-to-peer connections when in the field
- Avoid large hotspots (i.e. hotels and airports) where it is unclear who is online

### 3.5.3 Unsafe User Behavior

The final area that an effective mobile & remote computing security strategy needs to address is unsafe user behavior. This category of risk represents the great unknown, because there is no guarantee that users will observe the organization's formal policies when out of the office. Education and training is key. Established policies must be formally communicated to end-users and reiterated in frequent training sessions and documented and disseminated in writing so that they become habit and part of the organization's culture and expectations for performance. The need for management to achieve user buy-in cannot be over-emphasized. An organization may have a brilliant and exhaustively comprehensive policy document in place, but if nobody reads and/or follows the policies it contains, it won't serve its purpose.

In addition, compliance with internal policies needs to be monitored and enforced. There are a number of managed security and enforcement solutions available. While some employees may complain that usage monitoring is invasive and unwarranted, the threat posed by a security breach, network attack, and theft and/or disclosure of sensitive information is too great to take a hands-off approach to enforcement. The organization needs to be sure to communicate to employees that the ultimate objective of monitoring and enforcement is to keep the enterprise secure and minimize threats that negatively impact its viability. Before implementing monitoring and enforcement policies and procedures, an attorney should be consulted to ensure that the organization's strategy is in compliance with local, state and federal privacy laws.

# Leveraging Mobile & Remote Computing

## A Decision-Maker's Guide

---

Table II provides tactical advice for addressing the three key risk areas related to MRC:

**Table II**

Risk Area	Tactical Advice
<b>Physical Security</b>	<ul style="list-style-type: none"> <li>▪ Implement biometric verification to facilitate multi-layer authentication</li> <li>▪ Physically secure mobile devices with cable locks if possible</li> <li>▪ Monitor for unsafe user behavior</li> <li>▪ Mandate password authentication via strong passwords at both the device and application levels</li> </ul>
<b>Data Security</b>	<ul style="list-style-type: none"> <li>▪ Sensitive data should only be stored on encrypted devices</li> <li>▪ USB flash drives and other USB storage devices should provide encryption</li> <li>▪ Back-up data to a central, off-site server</li> </ul>
<b>Unsecured Access</b>	<ul style="list-style-type: none"> <li>▪ Use Ethernet or broadband wireless over Wi-Fi when available</li> <li>▪ Install and use a firewall</li> <li>▪ Require up-to-date Anti virus / Anti Spyware</li> <li>▪ Always use an IPSec, SSL or TLS VPN to attach to network or home office resources</li> <li>▪ Host Web-based company applications such as e-mail using SSL or TLS (HTTPS)</li> <li>▪ Require employees to turn off all unprotected shares</li> <li>▪ Use SSL or TLS websites when sending/entering sensitive data (i.e. credit cards numbers)</li> <li>▪ Digitally sign data to make it difficult for hackers to change data during transport</li> <li>▪ Encrypt documents that contain sensitive data that will be sent over the Internet</li> <li>▪ Disable or remove wireless capabilities if they are not being used</li> <li>▪ Avoid hotspots where it is difficult to tell who is connected</li> <li>▪ Ad-hoc/peer-to-peer settings should be disabled</li> </ul>

## 4 Mobile & Remote Computing Solutions

Every organization has unique needs, established operating models and its own personality. Accordingly, the use of MRC technologies and the precise configuration chosen will vary from organization to organization. There are, however, a number of common objectives which organizations hope to achieve through the expansion of mobile & remote computing capabilities, including:

- Flexible Work Arrangements & Home-Based Workers
- A Well-Connected Mobile Workforce
- Temporary Worker Accommodations
- Disaster Recovery and Business Continuity
- Client Self-Service

Now that we have established a better understanding of the MRC solutions available, and have explored some of the security issues and policy considerations related to mobile & remote computing, let's take a look at the common business objectives that might prompt an organization to pursue a mobile & remote computing initiative and viable solutions for achieving each.

# Leveraging Mobile & Remote Computing

## A Decision-Maker's Guide

---

### 4.1 Flexible Work Arrangements & Home-Based Workers

Employees are working from home more than ever. Originally, flexible work arrangements were reserved for disabled workers, part-timers or employees engaged in job-sharing arrangements. With commutes growing ever longer, however, and work activities consuming an ever increasing amount of our time, more and more employees are looking to spend at least some time working from home to achieve better work-life balance and greater productivity. As a result, more and more highly qualified job candidates are factoring the availability of flexible work arrangements into their employment decisions.

Flexible work arrangements may vary substantially within an organization. Depending on job category, and the work requirements of the position, they may range from one day a week to a semi-permanent work-from-home arrangement in which only occasional visits to the office are necessary. As home offices become more permanent, it may be necessary to support employees with more established infrastructures.

Current mobile & remote computing technologies make work-from-home arrangements quite easy for organizations to implement. For the home-based remote worker, the network connection is the key. In order for the home-based worker to be productive, they must have a reliable and secure connection between the home office and the organization. Organizations should opt for a broadband connection – cable, cellular, fiber optic or high speed DSL - with enough bandwidth to run applications from the organization's servers, download files stored on the network, and back-up home office data to prevent lost productivity in the event of a computer error, or damage to the remote device. The cost of high-speed connections in most urban and suburban areas has dropped significantly, thanks to incentive pricing from cable and phone companies. Beware of the lowest cost options. While bargains may deliver faster connections than dial-up, they may not be as reliable as business-oriented solutions, and will undoubtedly provide less in the way of support.

Establishing an Internet connection is only the first step, however. Once a connection has been established, and a service provider has been chosen, the remote connection to the organizations network must be established and secured. This is typically achieved through the deployment of a VPN, which enables remote users to connect to internal resources by tunneling through the Internet and the organization's firewall via an encrypted communication pathway.

The infrastructure needed to support remote employees once they are connected depends on the application they are using. SaaS and other web-deployed applications tend to require less in the way of infrastructure; only a web browser which serves as the client, while other internally-hosted applications may require a client component to be installed locally on the remote users PC. For example, local applications accessed via Citrix (or other infrastructure software) tend to lag; it may take a while for the results of a mouse click to be visible.

For the home-based employee, the organization should anticipate providing a desk- or laptop PC, reimbursing the employee for some portion of the Internet connection, and revisiting appropriate use/personal use policies. Supervision, accountability and availability of the employee are HR issues the employer will need to address. Some employees can perform in the detached environment of a home office much better than others.

### 4.2 A Well-Connected Mobile Workforce

A properly outfitted mobile workforce allows for greater face time with clients and potential clients, and expansion of the organization's market reach beyond geographically adjacent areas without the loss of communication and productivity typically associated with work outside of the office. In an effective MRC environment, mobile workers including salespeople, field staff (i.e. auditors) and on-site support

# Leveraging Mobile & Remote Computing

## A Decision-Maker's Guide

---

personnel who typically, spend more time on the road than they do in the office, are able to access organization resources, and are as accessible to clients and office personnel as if they were physically in the office. Mobile workers need to be able to adapt, even in circumstances where infrastructure may be limited or unreliable.

The mobile worker does not require the persistent connection to the organization that a homebound remote worker does, but periodic access is necessary. Because the majority of the mobile worker's time is spent with clients and at client sites, they need to be able to "check-in" with the home office when they have the time without having to worry about whether or not a connection will be available. Historically, mobile workers have been dependent on public infrastructure such as Wi-Fi networks at airports, hotels or coffee bars with all of their inherent security risks, for access to organization resources. Because unpredictable intermittent connectivity is not enough to support the mobile worker, organizations should consider equipping them with broadband cards employing EVDO, EDGE or 3G wireless technology. Cellular broadband is offered by all the major cell phone carriers, and affords mobile workers network access wherever there is cellular service. If a high-speed data network is not available, the cards are generally backwards compatible, enabling them to run on older cell systems at slower speeds. Furthermore, because they are private networks with fewer users and employ encryption to prevent unauthorized access, cellular broadband networks are inherently more secure than public Wi-Fi. Currently, broadband cards cost about \$60 per month.

Of course there are also a number of handheld devices that offer connectivity to internal networks for remote e-mail access and simple viewing of digital documents. PDAs, Smartphones and Blackberries run across the same EVDO and 3G enabled networks mentioned above, and some can even act as a broadband modem, extending mobile connectivity to laptops and other devices.

### **4.3 Temporary Worker Accommodations to Retain Talent and Minimize Lost Productivity**

Today's increasingly complex and competitive business environment places a premium on highly skilled, highly trained, high-impact workers. Companies invest tremendous resources in recruitment, training and retention, and can ill-afford to lose top performers. This is especially true in situations such as that faced by the CPA community, where the transition of the baby boomers out of the workforce is creating serious leadership challenges for many organizations, and causing the available workforce to shrink despite growing demand for the services they provide. In this lean recruiting atmosphere, organizations cannot afford to lose their top talent, yet all too often they allow high-impact personnel to slip away because of a lack of flexibility and an inability to think outside the box when it comes to alternative work arrangements.

Life transitions such as child birth, parenthood, divorce, ailing family members and pre-retirement often cause affected workers to leave their positions and temporarily pull out of the workforce. They recognize that the increased demands on their time and the additional responsibilities arising from the life event make it impossible to perform their job functions as they had previously. Many of the employees who detach themselves from their jobs in these situations do not return to that job when life returns to normal. This sudden and often permanent loss of critical employees and the accompanying loss of knowledge, experience and leadership can have a detrimental effect on organization performance, leading to substantial losses or declines in areas such as productivity and customer service.

Mobile & remote computing enables organizations to keep high performance personnel undergoing a life transition on the team, by supporting part time, work-from-home, and job sharing arrangements. These flexible work arrangements give personnel the flexibility they need to tend to life transitions, while remaining engaged with the organization at some level. Work arrangements created for staff in the midst of a life transition are meant to be permanent in nature, using remote control solutions such as Windows

# Leveraging Mobile & Remote Computing

## A Decision-Maker's Guide

---

Remote Desktop, LogMeIn or GoToMyPC to enable employees to access and control an office PC from home or some other remote location. As with other MRC solutions, it is best to use the encrypted communication pathway afforded by VPN to facilitate and secure the connection to the home office. When more limited access is sufficient, web-deployed applications or SaaS accessed through a SSL or TLS-secured website can be a good solution.

The scenario presented here is also appropriate for supporting flexible work arrangements to address the needs of other displaced workers, such as those unable to make it to the office due to inclement weather, natural disaster, or other extenuating circumstances.

### 4.4 Disaster Recovery & Business Continuity

Business disruptions can occur for a number of reasons, ranging from relatively benign-sounding occurrences like a burst pipe to catastrophic events like Hurricane Katrina or 9/11. There are also plenty of scenarios in between that can disrupt an organization, including office fires, derailed trains, downed power lines and server failures. These problems may not yield catchy headlines, but they can devastate an organization in a matter of hours.

Mobile & remote computing is an important component of many disaster recovery /business continuity plans. It enables workers to continue to perform their jobs even when access to the physical office is unavailable. The key is leverage. As organizations roll out mobile technologies, it is important to review how they integrate with existing plans, especially if disaster/recovery planning is compliance-mandated (e.g., Sarbanes-Oxley or HIPAA).

Data back-up and network redundancy are crucial if MRC is to be effective in facilitating business continuity. Simply providing a laptop to organization employees won't be sufficient if they cannot access the data and applications they need to do their job. Locally stored data should be backed up off-site regularly, preferably through automated processes that do not require conscious involvement on the part of end-users. Making the additional effort to *synchronize* data to servers in different locations means the remote worker may see little or no disruption.

As for access to critical business applications, either an internally hosted solution reproduced offsite, or third-party web-hosted SaaS products should be considered. In the case of SaaS, the level of backup and system redundancy offered by the major providers far exceeds that which even the largest and most sophisticated organizations can achieve economically. Because remote control-based solutions rely on office-bound computers to serve as intermediaries between the network and the remote devices, they are not the best option for organizations looking to achieve substantial business continuity and disaster recovery advantage from their MRC solutions. If an event causes a disruption at the home office, chances are that the primary device will be disrupted as well.

Technical and cost issues need to be considered when attempting to integrate MRC technologies into a disaster/business continuity plan. Organizations need to make sure when calculating the ROI for these options that they include the cost of not having access to their data for 1-2 days, one month or several months. Laptops may be more expensive than desktops, but if you can't access your desktops, they are of little use.

### 4.5 Client Self-Service

In the 24/7 information-now world in which we live and work, customers and clients expect quick and convenient access to the information they need, when they need it. They have become quite comfortable with electronic communication and often prefer e-mail and web interaction to face-to-face meetings. Efficient communication saves them valuable time and money, and having the ability to find and access the information they are looking for on demand rather than having to establish an appointment keeps

# Leveraging Mobile & Remote Computing

## A Decision-Maker's Guide

---

them focused on and engaged in the day-to-day operations of their business. Despite its convenience, e-mail is not always the best option for communicating and exchanging information with customers/clients. For instance, e-mail transmitted via the Internet is inherently less secure than messages sent over a private internal network, and may be vulnerable to interception and disclosure. E-mail communication is further limited by the fact that available bandwidth and e-mail server configurations impose limits on message size. This can make it difficult to send large client files via e-mail.

Portals (or extranets) offer an ideal solution for addressing the needs of clients and the limitations of e-mail. They utilize the same Internet technology employed by intranets and the web to create secured web pages that deliver self-service functionality to customers and clients, allowing them to download digital files and access the information they want when they want it, regardless of business hours. A properly configured client portal features password protection to help ensure that only authorized users can gain access, and can easily accommodate large client files. Portals can also be customized so that each authenticated user is only able to access the pages, documents and information they are intended to. They also support establishing profiles and other personalization techniques that modify portal content and presentation based on permissions and personal preferences. With a portal, all of a customer/client's information can be stored in one place, forming a central repository. On the client/customer side, a web browser is all that is required.

For larger organizations, in-house portal development is possible, but requires a robust IT department with deep programming skills. Smaller organizations may have to outsource portal development, or purchase packaged portal software or a subscription to SaaS portal solutions – may be able to engage development and customization consultants from the vendor, usually at a competitive rate.

Portals can be hosted internally or with a third-party Internet service provider (ISP). In general, outsourced hosting is preferable for organizations with little room for error. If even a brief outage is unacceptable, engaging an ISP that will agree to a rigid service level agreement is prudent. SaaS portal solutions tend to include hosting.

## 5 Conclusion

Determining your objectives and addressing risk are critical when defining your organization's MRC strategy. While there are many benefits of implementing MRC technologies, they can also pose new sets of challenges, not all of which are technical. They often have operational, personnel and procedural implications that can change the face of your business. To create an effective plan, begin by identifying the specific technologies that can help you reach your organization's goals and the amount of risk that the organization is willing to assume.

Risk in itself is not necessarily a problem, as long as you are ready to mitigate these risks throughout the implementation process. Careful planning helps organizations identify what could go wrong before they are faced with problems that could cost significant time or money. Planning starts with understanding how MRC technologies can deliver a competitive advantage, and continues with the selection and implementation of specific solutions, along with appropriately documented policies and procedures tailored to address the unique risks inherent in the solution and the organization's culture.

Begin by reading additional resources about the specific MRC solutions from which you think your organization can benefit. Then, work with your IT provider or consider engaging the services of a qualified technology consultant, like a Certified Information Technology Professional (CITP), who can guide you through the issues. Together, you can develop a budget and scalable plan that delivers the Return on Investment (ROI) you need.

# Leveraging Mobile & Remote Computing

## A Decision-Maker's Guide

---

### 6 Acknowledgements

The AICPA would like to thank the following individuals for their involvement and participation as a member of the AICPA's IT Executive Committee Mobile and Remote Computing Working Group. These individuals invested considerable time and effort to develop this paper and other elements of the IT Membership Section's Mobile and Remote Computing content suite. We are grateful for their tireless efforts.

**John Seale, CPA.CITP**

Partner  
RBSK Partners PC

**Thomas J. Metzler, CPA.CITP**

Consultant  
Resources Global Professionals

**David Ryan, CPA.CITP**

Chief Information Officer  
Artromick International, Inc.

Staff:

**Nancy A. Cohen, CPA.CITP**

Senior Technical Manager - IT  
Specialized Communities & Practice Management

**Matthew Murtaugh**

Project Manager - IT  
Specialized Communities & Practice Management

**Scott H. Cytron**

Senior Vice-President  
Piermont Communications, Inc.

**Tamera Loerzel**

Sr. Consultant  
Convergence Coaching, LLC

# Leveraging Mobile & Remote Computing

## A Decision-Maker's Guide

---

### 7 Glossary of Terms

**Active Server Pages (ASP)** – Microsoft's server-side script engine that web developers use to create dynamic web pages. It is marketed as an add-on to Microsoft Internet Information Services (IIS), formerly Microsoft Server. Programming ASP websites is made easier by various built-in objects. Each object corresponds to a group of frequently-used functionality useful for creating dynamic web pages.

Adapted from: Wikipedia; [http://en.wikipedia.org/wiki/Active\\_Server\\_Pages](http://en.wikipedia.org/wiki/Active_Server_Pages)

**Bandwidth** – A measure of frequency range typically measured in hertz. Bandwidth commonly refers to data (information) transmission rates when communicating over certain media or devices.

Adapted from: Wikipedia; <http://en.wikipedia.org/wiki/Bandwidth>

**Broadband** – In telecommunications, broadband refers to a signaling method that includes or handles a relatively wide range of frequencies, and may be divided into channels or frequency bins. Broadband is always a relative term, understood according to its context. The wider the bandwidth, the greater the information carrying capacity. In data communications, a modem will transmit a bandwidth of 64 kilobits per seconds (kbit/s) over a telephone line; over the same telephone line, a broadband ADSL line provides a bandwidth of several megabits per second. Cable broadband increases the chance of maintaining a constant broadband speed compared to ADSL services.

Adapted from: Wikipedia; <http://en.wikipedia.org/wiki/Broadband>

**Citrix Presentation Server (formerly Citrix MetaFrame)** – A remote access application publishing product that allows people to connect to applications available from central servers. One advantage of publishing applications using Presentation Server is that it lets people access these applications remotely from their homes, airport Internet kiosks, Smartphones and other devices outside of their corporate networks. For example, users can log in to their corporate network from an airport kiosk, see all of the applications they would see everyday at work, including Outlook e-mail and any internal applications, and access them from the kiosk in a secure environment. Centralizing applications for publication also makes it easier for administrators to manage them.

Adapted from: Wikipedia; <http://en.wikipedia.org/wiki/Citrix>

**EDGE (Enhanced Data rates for GSM Evolution)** – An evolution of the GSM mobile communication standard feature that supports increased data transmission rates and improved data transmission reliability. It is a type of wireless broadband deployed in Smartphones, some PDAs, laptops and PCMCIA cards. High-speed data applications, such as video services and other multimedia benefit from EDGE's increased data capacity. EDGE is global and works over long distances provided there is a signal. AT&T (formally Cingular) is the most common carrier utilizing the EDGE standard.

Adapted from: Wikipedia; [http://en.wikipedia.org/wiki/Enhanced\\_Data\\_Rates\\_for\\_GSM\\_Evolution](http://en.wikipedia.org/wiki/Enhanced_Data_Rates_for_GSM_Evolution)

**Encryption** – Often referred to as scrambling, encryption is the process of converting information via algorithm into a form that is unreadable without special knowledge. Long used by governments and militaries to keep sensitive information secretive during transmission, encryption is now employed by the public to protect information transmitted or stored via systems, such as the Internet, mobile telephone networks and bank automatic teller machines (ATMs).

Adapted from: [Wikipedia; http://en.wikipedia.org/wiki/Encryption](http://en.wikipedia.org/wiki/Encryption)

# Leveraging Mobile & Remote Computing

## A Decision-Maker's Guide

---

**Evolution Data Optimized (EV-DO, EVDO, EV)** – A wireless broadband data transmission standard adopted by many mobile phone service providers in the United States, Canada, Mexico, Europe, Asia, Russia, Brazil and Australia, and deployed in Smartphones, PDAs, laptops and PCMCIA cards. Similar to EDGE, EVDO transmits data at a significantly faster rate and works over even longer distances provided there is a signal. At this time, EVDO is only offered by Sprint and Verizon.

Adapted from: Wikipedia; <http://en.wikipedia.org/wiki/Evdo>

**Firewall** – An information technology security device configured to permit, deny or proxy data connections set and configured according to an organization's security policy. Firewalls can either be hardware or software-based.

Adapted from: Wikipedia; [http://en.wikipedia.org/wiki/Firewall\\_\(networking\)](http://en.wikipedia.org/wiki/Firewall_(networking))

**FTP or File Transfer Protocol** – An internet protocol used for exchanging files over any network that supports the TCP/IP protocol, including intranets and the Web.

Adapted from: Wikipedia; <http://en.wikipedia.org/wiki/FTP>

**Instant messaging (IM)** – A form of real-time, text-based communication between two or more computer users connected over a network such as the Internet. Instant messaging requires the use of a client program. It differs from e-mail in that conversations are then able to happen in real time. Popular IM services on the public Internet include .NET Messenger Service (MSN Messenger and Windows Live Messenger), AOL Instant Messenger, Excite/Pal, Gadu-Gadu, Google Talk, iChat, ICQ, Jabber, Qnext, QQ, Meetro, Skype, Trillian, Yahoo! Messenger and Rediff Bol Instant Messenger.

Adapted from: Wikipedia; [http://en.wikipedia.org/wiki/Instant\\_Messaging](http://en.wikipedia.org/wiki/Instant_Messaging)

**Intranet** – A private computer network that uses Internet protocols, network connectivity and public telecommunication infrastructure to facilitate the secure sharing of information within an organization. Because an intranet employs Internet concepts, such as clients and servers, and utilize Internet protocol, intranets may be thought of as private versions of the Internet, or as versions of the Internet confined to a single organization. Although an organization's internal website is often referred to as an intranet, internal websites are but one intranet service. Organizations also use Internet technologies to provide new interfaces with legacy systems and data.

Adapted from: Wikipedia; <http://en.wikipedia.org/wiki/Intranet>

**Mobile & Remote Computing (MRC)** – Technologies and policies that enable users to securely connect to key resources anywhere, anytime, regardless of physical location.

**Personal Digital Assistants (PDAs)** – Handheld computers originally designed as personal organizers, but became much more versatile as technology progressed. PDAs are often referred to as pocket or palmtop computers, and can run many standard computer applications, including calculators, clocks, calendars, Internet browsers, e-mail applications, word processors, address books and spreadsheets, and can even be used as radios, Global Positioning Systems (GPS), cameras and video recorders. Newer PDAs also have both color screens and audio capabilities, enabling them to be used as mobile phones (Smartphones), web browsers, or portable media players. Many PDAs can access the Internet, intranets or extranets via Wi-Fi, or Wireless Wide-Area Networks (WWANs). Many PDAs employ touch screens as the primary interface. Blackberries, Palm Devices, Treos and Smartphones are all common PDAs.

Adapted from: Wikipedia; [http://en.wikipedia.org/wiki/Personal\\_digital\\_assistant](http://en.wikipedia.org/wiki/Personal_digital_assistant)

**Portable Desktop** – Solutions that enable users to define and carry their own unique desktop

# Leveraging Mobile & Remote Computing

## A Decision-Maker's Guide

---

environment with them on flash media and work from remote locations, and unrelated computer devices. Once you are done working on that device and remove the flash media, all typical "fingerprints," such as temp file browser links, are no longer present on that device, but remain on the media with the configured desktop.

**Remote Desktop** – A software solution for accessing a PC and its resources from remote locations as if you were sitting at the desktop. Examples include Microsoft Remote Desktop, PC Anywhere, Remote PC and GoToMyPC.

**Sharepoint, Windows SharePoint Services (WSS) or Windows SharePoint** – A free add-on to Windows Server 2003 made available by Microsoft, which offers basic web portal and intranet functionality. It includes an integrated set of controls that allows users to create intranet pages and modify the content, appearance, and behavior of Web pages directly from their browser. These portal pages may include project sub-sites, version-controlled document storage, and basic search functionality. SharePoint sites are ASP.NET web sites hosted on Internet Information Services 6.0, using a SQL Server database on the back-end to store data.

Adapted from: Wikipedia; [http://en.wikipedia.org/wiki/Windows\\_SharePoint\\_Services](http://en.wikipedia.org/wiki/Windows_SharePoint_Services)

**Secure Sockets Layer (SSL)** – A cryptographic protocol for securing communications conducted over the internet. See Transport Layer Security (TLS).

**Terminal Server** – A solution for deploying software applications to remote computers. It is used for easier management of applications across an internal network as well as remote sites.

**Transport Layer Security (TLS)** – An internet protocol that employs encryption to provides endpoint authentication and communications privacy to help secure communications over the Internet related to activities such as web browsing, e-mail, Internet faxing, instant messaging and other transfers of data. TLS is the successor to SSL. While there are slight differences between SSL and TLS, the protocol remains substantially the same.

The TLS (and SSL) protocol provides server authentication so that the user – either an individual or an application - can be sure of the device with which they are communicating.

Adapted from: Wikipedia; [http://en.wikipedia.org/wiki/Transport\\_Layer\\_Security](http://en.wikipedia.org/wiki/Transport_Layer_Security)

**Unified Communications (UC)** - refers to the integration of disparate communications systems, media, devices and applications, including fixed and mobile voice, e-mail, instant messaging, voice over IP (VoIP), voice-mail, fax, and audio, video and web conferencing into a single environment providing the user the ability to redirect and deliver, in real-time, communications sent from a variety of systems to the device nearest the intended recipient.

Adapted from: Wikipedia; [http://en.wikipedia.org/wiki/Unified\\_communications](http://en.wikipedia.org/wiki/Unified_communications)

**Voice-over Internet Protocol (VoIP)** – The routing of voice conversations over the Internet or through any other IP-based network. VoIP-to-VoIP phone calls are sometimes free, while VoIP to public switched telephone networks (PSTN) may have a cost that's borne by the VoIP user. VoIP is also referred to as IP Telephony, Internet telephony, Broadband telephony, Broadband Phone and Voice over Broadband.

Adapted from: Wikipedia; <http://en.wikipedia.org/wiki/VoIP>

**Virtual Private Network (VPN)** – A private communications network used by organizations to communicate confidentially over a public network. VPN traffic can be carried over a public networking infrastructure (i.e., the Internet) on top of standard protocols, or over a service provider's private network

# Leveraging Mobile & Remote Computing

## A Decision-Maker's Guide

---

with a defined Service Level Agreement (SLA) between the VPN customer and the VPN service provider. A VPN solution creates encrypted private channels through which data can be transferred securely between two points.

Adapted from: Wikipedia; <http://en.wikipedia.org/wiki/Vpn>

**Web Portal** – A network site that serves as a single point of access to information on the web. Portals present information from diverse sources in a unified way, and provide an excellent way for organizations to bring together access control and procedures from multiple disparate applications, while maintaining a consistent look and feel. A Personal Portal is a site on the web that typically provides personalized capabilities to its visitors, providing a pathway to other content. It is designed to use distributed applications, different numbers and types of middleware and hardware to provide services from a number of different sources. Business portals are designed spaces for sharing and collaboration in the workplace. Portals designed so that the content works on multiple platforms, such as personal computers, personal digital assistants (PDAs) and cell phones.

**Wi-Fi (Wireless Fidelity)** – A type of wireless broadband originally developed to connect mobile computing devices, such as laptops to Local Area Networks (LANs). Wi-Fi is now increasingly used for more services, including Internet and VoIP phone access, gaming, and basic connectivity of consumer electronics such as televisions, DVD players, and digital cameras. A person with a Wi-Fi enabled device, such as a PC, cell phone or PDA, can connect to the Internet when in proximity of a Wi-Fi access point. The region covered by one or several access points is called a hotspot. Hotspots can range from a single room to many square miles of overlapping hotspots.

Adapted from: Wikipedia; <http://en.wikipedia.org/wiki/Wifi>

**Wiki** – A website that allows visitors to add, remove, edit and change content, typically without the need for registration. It also allows for linking among any number of pages. The ease of interaction and operation makes wikis effective tools for mass collaborative authoring. The term wiki can also refer to the collaborative software itself, such as a wiki engine that facilitates the operation of such a site, or to specific wiki sites, including the computer science site WikiWikiWeb (the original wiki) and online encyclopedia Wikipedia.

Adapted from: Wikipedia; <http://en.wikipedia.org/wiki/Wiki>

**Wireless Broadband** – A fairly new technology that provides high-speed wireless Internet and data network access over a wide area. Wireless Broadband features speeds roughly equivalent to wired broadband access. Mobile Wireless Broadband technologies include new services from companies such as Verizon, Sprint, and Cingular, which allow a more mobile version of this broadband access. Consumers can purchase a PC-card, laptop-card, or USB equipment to connect their PC or laptop to the Internet via cell-phone towers using either EVDO or EDGE.

Adapted from: Wikipedia; [http://en.wikipedia.org/wiki/Wireless\\_broadband](http://en.wikipedia.org/wiki/Wireless_broadband)