# Mitigating Risk In Wireless Technology Migration

## Introduction:

Today's agile business demands anytime/anywhere connectivity. That's why so many inventory management solutions include wireless technology for AIDC. With the rapid evolution of wireless products, however, along with compliance issues and ever-changing logistics, migration to advanced wireless systems is inevitable. It's also necessary: failure to adapt has negative implications with both suppliers and customers and technology mis-steps could potentially lead to significant downtime. This paper helps identify businesses that should migrate to newer wireless technologies and offers a road map that will help you to discover the best possible supply chain automation and inventory management migration partner.

## What is driving wireless migration?

Since the late 1980's, Automatic Identification Data Capture (AIDC) technology has been experiencing a **product lifecycle** decline. Through a series of standardizations and technology updates, the lifetime for AIDC devices has gone from an 8 to 10-year cycle to a 24 to 36-month cycle. Legacy infrastructure components adopted in the past 4-5 years, such as switches, access points, ports, and components as well as end devices such as hand scanners and vehicle map devices, will soon be at the end of their life.

Service offered for these products is also shrinking as the window of availability for replacement parts availability is closing. Customers are saying: "I can't get the product" and "I can't get it serviced."

Another driving force for wireless migration is the increased need for **wireless infrastructure security**, which has come into the limelight in the past 24 months. It is affected by two issues- **compliance** and **general best practices**. The major federal regulatory compliance framework around wireless includes *HIPPA*, which provides security and privacy of consumer healthcare information and the *Sarbanes-Oxley Act, (SOX)*, which was enacted to combat corporate accounting scandals. *SOX* helps detect errors, monitors transactional integrity, and prevents fraudulent or unauthorized activities. And if a company takes credit card information anywhere across its wireless network, *Payment Card Industry Data Security Standard (PCI-DSS)* compliance is also required to monitor security risks across the consortium of credit card information.

**Best practices** surrounding security, particularly with all of the knowledge and hype around new wireless features and capabilities, is also driving migration. Companies are increasingly vulnerable to being hacked and need to take increased precautions. For example, the original wireless security, known as *WEP*, *(Wireless Equivalency Protocol)* was intended, as the name suggests, to be the equivalent of wired security. However, *WEP* quickly proved to have a large number of points of attack. Now any equipment manufactured after November 2003 that bears the Wi-Fi compatible logo must implement WPA or WPA 2 security. Other things to consider--are there legal ramifications for non-compliance? If your information is compromised, how long would it take and what would it cost to get your system back up and running? What about public relation issues--should events spin out of control?

Other **new application** requirements are also forcing migration. Old text-based, green screen interfaces are being replaced by GUI (point and click) and HTML web based interfaces. So the software manufacturer upgrade path is also forcing the move to new interfaces.

**Features and functions:** While the general features such as higher speed, and brighter displays may be subjective points that don't require wireless technology migration, there are plenty of new feature functions that do. For example, features that have the ability to support voice recognition, RFID technology, and some of the wireless accessories being utilized to automate functionalities such as scales and form factor devices for hands-free wearable units to increase productivity.

**Platform standardization:** Over time some of the largest Tier One companies that have been using wireless, and have grown through acquisition, now operate with a hybrid of technologies. There are interface channel issues, terminal end user and encryption code concerns, as well as vender management and infrastructure support problems. In short, the cost of ownership increases, because they can't support the same technology and they can't share technical resources (such as a common parts pool), which complicates maintenance and management. In addition, emerging RFID and voice recognition devices are not supported in the legacy equipment Tier One companies are now using. Even though they were early adopters of wireless technology, many Tier One companies are at the declining stage of the lifecycle of those wireless products they bought in the 1980's.

## What are the first steps for technology migration?

Okay, so you have decided that technology migration to wireless, or migration to a wireless upgrade is something you want to do. What are the first steps?

**Determine what you know about yourself and your integration partner.**

When looking for the right integration partner there are two philosophies to choose from: A partner who is product centric or one who offers a consultative perspective.

Choose a **product centric** fulfillment partner if you think know everything you need to know to complete the integration yourself. If all you want is one particular product, in a certain quantity, choose a product centric partner.

However, if you've reviewed proposals and recommendations from various suppliers, and you feel that your in-house expertise needs some buffeting, then work with a **consultative partner**--more specifically one that is not "married" to any particular products. They will weigh the advantages and disadvantages of a hybrid solution for your particular integration. They will offer multi-vendor product support from their portfolio and determine the best solution that will provide the greatest benefits.

## Do a background check on your partner.

Before choosing a partner, be sure to verify that they offer the kind of **product methodologies** that have been benchmarked, documented and proven with a quality metric, whether it's ISO, TQM, etc. Everybody talks about a process but do they really have one? Also ask about functional, industry and market **certifications**. Make sure your potential partner is certified in these three areas: products, processes and people.

For obvious reasons **geographic reach** is important too. Knowing you'll have immediate attention to a given problem with the capabilities of keeping track of all of your locations and distribution anywhere at anytime is going to give you peace-of-mind.

Ask about their **comprehensive offerings** and not just about product space but also support maintenance, consulting and all of the associated professional and lifecycle services.

**Accountability.** Make sure your integration partner provides a Service Level Agreement document that describes the minimum performance criteria. This contract language will

typically describe any remedial actions and penalties that will take effect if their product's performance falls below a promised standard. Check out their track record. Are their customers happy? Do they offer customer feed back in the form of SAP data? Be sure you can tangibly touch, feel and see their accountability programs (verses just seeing information on a PowerPoint slide). Make sure their programs fulfill your total expectations.

Research their **long-term market** presence. What's your future partner's reputation in the industry? Will they still be in business when it's time for upgrades or even routine maintenance and support?

## What are the issues when choosing the right hardware?

The first question to ask is a simple one: How far along a **given technological lifecycle** is the product you are considering? Is it emerging technology that might have some integration issues? Is it six months away from obsolescence? What are your current needs within that lifecycle? Can this product deliver on the promise on any short-term or even immediate sweet spot of opportunity?

What are your other **current needs?** Think big picture and minute-by-minute details. What are your ergonomic, feature-function, technological and environmental needs? Consider things like weight, size of units, mobile units, and what about peripherals? Are there temperature parameters? Are there condensation, precipitation and vibration specifications? What are the ergonomic issues for the entire solution? Should the unit be wearable? Are their mounts needed for vehicles? Can these products deliver to your unique and precise needs?

What are your **future needs**? Are you considering putting voice on your network down the road? What about RFID support? Will you want to add guest access? Or secure client devices?

Think about **vendor standardization**. Do you want to go with a single vendor solution, offered by companies such as Motorola or a mixed environment? This decision will affect your spare pools, system costs and support management.

## What are the installation issues?

For starters, if you're running a legacy operation, you don't want to give up all the efficiency gains you have achieved. If a new automated system breaks down, you will still need to ship products. Especially if you have penalty clauses with your customers, you really can't afford breakdowns. For new installations, the quicker you get up and running, the faster you can start seeing a return on your investment. Your integration partner will paint a rosy picture of the future, but you'll want a real road map to guide you every step of the way.

Look for **proven methodologies** for getting any installation done and a single point of contact. You'll want to know who is doing what, when and you'll want an outline of the effective project management. Ask for documents that define **clear requirements** and **acceptance criteria.** That means you'll want to define your partner's project management functions, integration and test functions, site and survey functions, all their offered services, and you'll want a **pre-installation** checklist per location.

You'll also want documentation for how critical issues are going to be addressed for the life of the system with regards to:

- **Knowledge transfer--** What training documentation are installers leaving behind for you after they're gone?

- **Support maintenance**--When exactly does a project manager step into the transition phase?

Remember too, every vendor does not adhere to best industry practices. When there are exceptions, and there always are, you'll want to know upfront how your partner will address **exception management** and who is the **single point of contact** to deal with these new variables.

How graceful the **transition** is from the day everything is up and running, to the support and maintenance phase depends upon how willingly your integration partner proactively moves you through it. Do they have a project manager who will stay with you for the first 30 days? Do they run test plans? Do they set up a telephone support calls? There is nothing worse than having a problem and not knowing whom to call.

## What support options are available between Implementation and Break/Fix Management?

Continuing on the transfer theme, you have a responsibility to understand the various **support needs** beyond depot maintenance and break/fix activities. There's device management and maintenance, product set and solution support, possibly setting up a help desk, and so on. Is your partner going to help you decide the best support system for you? Know what you are transitioning to--will your partner provide knowledge transfer?

You can choose to be **self-supported**. You will need to be trained and learn how to set-up infrastructures. You can choose a **shared support** program whereby you may decide to handle the tier one support and look for help with tiers two and three. Or you could **completely outsource** support. Not a bad idea with constantly evolving technologies,

and standardization such as Windows operating systems, wireless interfaces, logistical applications, and new end-user terminal technology constantly being introduced.

## Conclusion

Wireless migration for AIDC is in dynamic transition. The strategy to use your own resources to save money may actually over extend in-house capabilities, especially when new interfaces and configurations are encountered.

An outside solutions provider and systems integrator experienced with multiple vendors can provide invaluable expertise. Many Tier One companies find that it pays to choose a partner who understands the complexities of the ever-changing automation and inventory management environment, along with its standards, certification and integration issues. PEAK Technologies is a proven partner that offers differentiated knowledge of new technologies, industry best practices, and network and wireless interface protocol changes. These comprehensive capabilities can mitigate the risk of wireless technology migration and provide long-term value for your ADIC applications.