Although there are many benefits to using the new RFID technology, careful thought must be given to the possible risks that come with it.

RFID Risk Management

JOHN KOPALCHICK III, CPA, CIA, CPIM, CPM, CMBA
DIRECTOR, RISK CONSULTING
PROTIVITI

CHRISTOPHER MONK, CIA, CPIM, CPM
MANAGER, RISK CONSULTING
PROTIVITI

ILLUSTRATION BY
ED FOTHERINGHAM

PICTURE YOUR GROCERY STORE. Think of the cookie aisle and remember the last time you took a package off the shelf. Now, imagine that at the moment you put that package into your cart, the stockroom receives a real-time message from the inventory system that an item has been removed from the

COOKIES
Mr. Fotheringham

shelf and needs to be replenished. At the same time, a middleware application, using predefined business rules, automatically generates a replenishment ticket for the stocker and sends an order to the distribution center, adding the item to the store's next order. The manufacturer of the product receives notice that the distribution center inventory has been reduced and is able to monitor and replenish inventory based on defined business rules. Although this scenario may seem like something out of a "Star Trek" episode, it is not that far away. Called radio frequency identification or RFID, rudimentary versions of this hot, new technology are being used today, probably more often than most of us are aware.

RFID is transforming the way business is conducted. Some pundits think RFID could surpass the billions of dollars spent on bar-code technology in the 1980s, when it made its debut. Business consulting firm Frost and Sullivan predict spending on RFID technology and related process and systems integration will top US $7 billion by the year 2008. Already, several large manufacturers, distributors, and retailers have made RFID a top priority. Retail giants such as Wal-Mart, Target, and Albertsons grocery have mandated RFID capabilities at the case-and-pallet level to their top suppliers this year and will introduce further requirements by 2006. These mandates are affecting major consumer product manufacturers, including Gillette Co. and Procter & Gamble.

Even the U.S. government has made RFID a major initiative: The Department of Defense is requiring that all of its suppliers be RFID compliant. To alleviate the issue of counterfeit drugs flooding the United States, the Food and Drug Administration has issued a mandate for all pharmaceutical companies to begin tagging products with RFID chips at the bottle level. When used for asset tracking and supply-chain security purposes, industries such as media and communications, telecommunications, manufacturing and distribution, airline, and energy will be affected as well.

As chip prices drop and the size of integrated circuits continues to decrease, new applications for improving supply-chain visibility, inventory management, asset tracking, and supply chain security will begin to emerge. Although the journey to tagging at the item level will take five to 10 years, companies are moving toward implementing RFID capabilities, which will increase the risk and control implications as a result of this transforming technology. Because RFID will increasingly impact supply chain and operations executives, as well as others, the internal audit and risk management communities will need to focus on this technology.

Benefits of RFID

BENEFIT	DESCRIPTION
Enhanced Control (Financial and Operational)	■ Reduction in theft. ■ Reduction in counterfeiting. ■ Real-time inventoryintegration with financial reporting systems. ■ Verification of shipments and receipts for billing purposes.
Process Improvements	■ Automated inventory cycle counts. ■ Picking, packing, and shipping accuracy (order fulfillment). ■ Improved inventory planning and replenishment processes. ■ Improved supply chain integration.
Cost Reduction	■ Reduction in inventory. ■ Reduction in labor requirements for inventory management (operating costs).
Data Collection, Accuracy, and Integrity	■ Increased receiving accuracy. ■ Improved inventory visibility.

HOW THE TECHNOLOGY WORKS

The modern application of RFID is often referred to as a class of smart technologies that enables object-to-object communication. A small transponder, or "tag," containing a microchip attached to an antenna is inserted into an object's or product's packaging or label. As the item moves past a reader — for example, a pallet moving into a warehouse from a supplier — the reader, which is embedded in the ceiling at the dock's doors, converts the radio waves from the tag into information that can then be used by computers.

The information read from the tag is analogous to a license plate for each item. One proposed universal standard for the license-plate information on the tag is the electronic product code (EPC), which, similar to bar codes, is divided into segments that have identifiers for the manufacturer, product, and version. However, unlike bar codes, the tag also contains a specific serial number for that distinct product. The information about that product is housed on a server and an object name service (ONS) points the computer to another server where information about the product is stored. The physical tag serves as the product's physical DNA while the EPC serves as the product's genetic code housing detailed information about the product's physical description, location history, and manufacturing location and date. The ONS can reference servers on-site or at the supplier or independent providers that house the information.

There are two basic forms of RFID tags: active and passive. Both forms contain a microprocessor attached to an antenna, but active tags also contain a battery, which allows them to send their information over longer ranges. The battery also can power the chip's circuitry to perform other functions such as monitoring the environment. For example, active tags can communicate end-of-shelf-life status, changes in pressure and temperature, traces of radiation or chemicals, or evidence of tampering. Passive tags simply use the electromagnetic waves sent out by the reader as the power source to transmit their information.

Tags can also be read-write or read-only, depending on the application. The cost of tags — one of the primary factors affecting the rate of adoption — is currently anywhere from US $10 to $100 for active and 30 to 50 cents for passive. When the costs decrease to 5 cents per tag, which is the general industry standard for positive return on investment on tagging each item, more and more companies will adopt the technology.

RISK ASSESSMENT PROCESS

Like any major system implementation or process-reengineering project, there are numerous risks surrounding RFID. Protiviti, an international provider of independent internal audit and business and technology risk consulting services, groups them across four domains:

- Engineering/technical risks.
- Business environment risks.
- Process risks.
- Technology risks.

These risk domains are inherent in three major phases of RFID transformation:

- Pre-implementation or planning.
- Pilot.
- Post-implementation or rollout.

Through a companywide project risk assessment, before and throughout the RFID implementation stages, key risks and audit issues can be identified and prioritized, and recommendations for control and process improvements can be defined and agreed upon. Internal auditing can play a key role in both facilitation discussions around the risk framework and in identifying control and process improvement needs and opportunities on both a pre- and post-implementation basis.

ENGINEERING/TECHNICAL RISKS

There are several important risks pertaining to the engineering or technical aspects of RFID that are known throughout the industry. Although these risks are primarily external to organizations and, therefore, out of the organization's control, the risks must still be considered and monitored. Among them are physical "read" limitations impacting reliability and repeatability of high-volume RFID applications, as well as the cost of RFID tags and the multiple standards that currently exist, all of which impact the rate of adoption and interoperability.

The physical read limitations are being addressed on a widespread application basis by EPC Global, a consortium of founders of modern RFID applications, and the research and development functions of the organizations involved. These read limitations and read performances also need to be a focus within each organization considering RFID adoption as they pertain to their specific products. In addition, EPC Global is leading the drive to develop a single set of standards that can be adopted across all industries on a global level. The RFID chip manufacturing processes and chip-to-tag application processes continue to evolve, which will bring costs down.

Internal auditors should monitor these technical issues on an ongoing basis as part of the risk assessment process as their organizations plan for RFID deployment. However, as issues are resolved and companies move forward into a pilot program or full implementation, key risks and controls will need to be identified as part of developing a responsive audit plan.

BUSINESS ENVIRONMENT RISKS

Issues pertinent to the current business environment include the development

RFID vs. Bar Code Technology

FEATURE	BAR CODING	RFID TAGGING
Proximity and Orientation	Requires line of sight to be read (i.e., the bar code must face the reader at close range to be read).	A sensor can read the tag without having line of sight or orientation requirements, as long as the tag is within range of the reader.
Environmental Conditions	Bar code technology is sensitive to environmental issues such as dirt, label abrasion, or temperature.	Tag packages can be designed to withstand harsh environments and manufacturing processes.
Read Quantity	Only one bar code can be read at a time.	Many tags can be read simultaneously. Read rates are much higher than with bar codes.
Data Granularity	Bar codes use Universal Product Code (UPC) data at the product level (only identifies manufacturer and product, not unique items). Information is static and cannot be changed.	RFID tagging uses electronic product codes (EPC), where each item contains a unique identification serial number. Historical information, such as date/time/place of manufacture and movement history, can be captured for each item. Some tags have read/write capability.

A Study of RFID Risk: Gillette Co.

At the request of Gillette Co.'s vice president of internal audit and its Value Chain Organization, Protiviti conducted an RFID risk assessment survey during the first quarter of 2004, with a focus on RFID operations from the point of manufacture to the distribution center. Preliminary information including risk types, type of pilot, and business model were gathered to create the survey through both facilitated sessions and interviews with key Gillette stakeholders involved in the auto-ID initiative. The result was a survey that would guide Gillette's pilot team through a comprehensive risk assessment and prioritization, which helped the team understand and manage the universe of risks associated with RFID.

The purpose of the survey was to identify and prioritize the specific risks associated with RFID technology for Gillette by assessing the likelihood or probability of the risk occurring given the current state of its processes and the marketplace, and by assessing the impact of the risk on management's ability to achieve its business objectives. A domain of 46 key risks related to process and technology for pre-implementation, implementation, and post-implementation phases were identified (see "Gillette Co Risk Map" on the facing page). Each respondent also was asked to provide comments on Gillette's current level of preparedness in addressing each risk, thus providing information for internal auditing to identify key risks and controls in place and develop audit plans for areas needing further development.

SURVEY

The respondents represented various functions within the organization, including information technology (IT), finance, value chain, marketing, and customer support. Respondents were asked to rank all 46 risks identified on a scale of one to five for each category, with one being the lowest level of likelihood/impact and five being the highest or most significant. Risks were classified and presented in order of phase — pre-implementation, implementation, post-implementation — and grouped by environment-, process-, or technology-related risks (technical risks were not addressed).

The survey results were averaged for each risk score, and the results were plotted on a 2 x 2 risk matrix, with the upper-right quadrant representing the critical risks (high likelihood and high impact). Thirty-three of the 46 risks were scored as critical, or fourth quadrant, risks. As a result, the top 10 — most critical — risks within the fourth quadrant were defined, and further analysis was provided based upon the individual comments from the survey respondents.

ENGINEERING RISKS

Several broad themes emerged from the survey. Results indicated that many of the primary risks associated with RFID for Gillette are known risks throughout the industry, such as physical limitations, unknown and changing costs (and the resulting inability to calculate a return on investment), and the lack of industrywide standards and its resulting impact on adoption and interoperability.

There are additional personnel risks with change management. These risks must be addressed through formal and proactive communication strategies and plans ensuring all stakeholders understand how they are impacted by RFID. Gillette and/or EPC Global initiatives are currently addressing many of these risks.

IT RISKS

Other key IT risks surfaced that have not been widely discussed in trade journals and among RFID participants. These include:

- Tasks associated with application control and IT change management may not be adequate, such as analyzing and addressing pilot results, system cutover, requirements management, program change control, configuration change control, process change control, and quality assurance processes.
- Facilities used as backups may not have adequate RFID capabilities to serve customers (applies to a phased rollout by geography).
- Long-term disruptions in data processing or availability may occur. Support processes, including job scheduling, backup and recovery, continuity planning, and help desk services may not be adequate.
- The large volume of data collected may not be effectively used to create "information" relevant to manage and control the business or shared in an effective manner.

Data and comments received from the survey respondents, as well as the average risk scores, will provide key input for the generation of Gillette's audit plan in 2005 and beyond. In particular, internal auditing must monitor internal based risks (versus external- or environmental-based risks) over data integrity, business interruption, and physical process changes to ensure the success of the auto-ID implementation, both initially and on an ongoing basis.

PROCESS RISKS

Few critical process risks surfaced from the survey. The primary concerns identified were the existence of adequate RFID-enabled backup facilities, business continuity planning, and the impact and integration of RFID-enabled processes with existing business processes. Generally speaking, Gillette, as a whole, focused on the broader post-implementation process risks. This is primarily attributed to the proactive nature with which Gillette is pursuing its RFID initiative. Gillette appears confident that it has the immediate risks contained, and is further along in its efforts on the broader, more long-term risks.

of a standard and open architecture or standard protocols, unknown costs, and return on the technology. Organizations such as the International Organization for Standardization and EPC Global are working on developing standards. Standardization is key to interoperability, or the ability of tags and readers from different vendors to communicate, which is critical for a high rate of adoption. As the adoption rate increases, more will be spent on research and development related to ultra-high-volume manufacturing processes, which will drive the costs of chips down even further.

The absence of common standards and interoperability poses a critical risk to organizations investing in RFID. Internal auditors can play a key role in assessment and identification of these key risks and monitor the business environment for changes that will impact their organization.

PROCESS RISKS

Once RFID becomes more mainstream, its vast capabilities will impact many processes that are currently handled manually, such as inventory replenishment and control, distribution, shipping, planning, and retail category management activities, to name a few. Transaction processing and validation will become more automated and need little-to-no human intervention. Real-time changes in production and distribution cycles will be possible.

At the same time, the technology's impact on current processes may not be understood, clearly defined, documented, or communicated throughout the organization, resulting in inconsistent execution and data integrity issues. All processes and exception processing affected by RFID must be considered, including handling receiving issues and returns — such as quantity, quality, and part discrepancies — and overages and shortages. Ultimately, these changes will have a significant impact on processes integrated with financial reporting systems, which will — at least in the United States — have to be addressed in the context of compliance and control efforts related to the U.S. Sarbanes-Oxley Act of 2002.

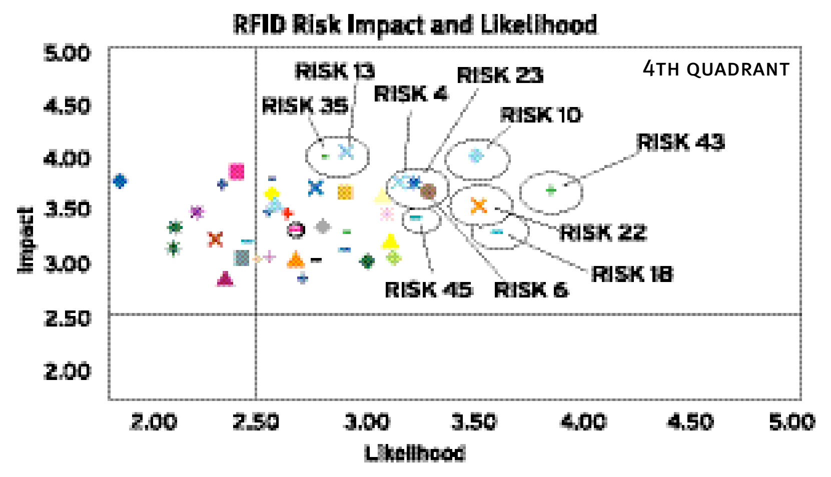
Business and information technology (IT) strategy around RFID technology, selection of RFID hardware and software, and process reengineering associated with RFID implementation may not be clearly

Gillette Co. Risk Map

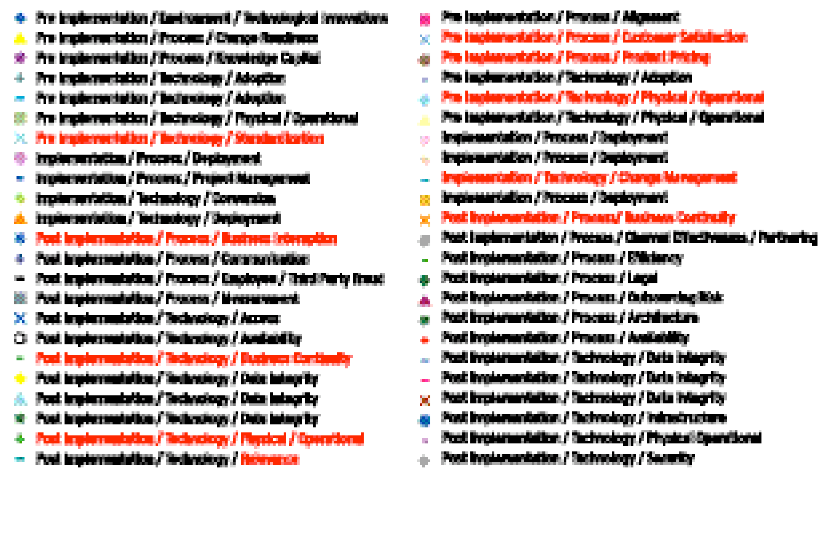
The average survey responses for likelihood and impact of each risk are plotted on a 2 x 2 risk matrix, with the upper right quadrant representing the most significant or most critical risks — high likelihood and high impact. In this example, the graphical representation shows that 33 of the 46 total risks were scored as critical, or fourth-quadrant risks. Among those, 12 risks are process-related and 21 are technology related. As a result, the top 10 risks — most critical — within the fourth quadrant were defined and further analysis was provided based upon the individual comments from the survey respondents. Identifying the most critical risks to the organization allows internal auditors to prioritize efforts related to further process assessment and testing to ensure appropriate plans are in place to effectively identify, manage, mitigate, and control each risk.

TOP 10 RISKS

Risk 4:	Pre-Implementation/Process/Customer Satisfaction
Risk 6:	Pre-Implementation/Process/Product Pricing
Risk 10:	Pre Implementation/Engineering/Physical/Operational
Risk 13:	Pre-Implementation/Engineering/Standardization
Risk 18:	Implementation/Technology/Change Management
Risk 22:	Post Implementation/Process/Business Continuity
Risk 23:	Post Implementation/Process/Business Interruption
Risk 35:	Post Implementation/Technology/Business Continuity
Risk 43:	Post Implementation/Technology/Physical/Operational
Risk 45:	Post Implementation/Technology/Relevance



Graph size increased to show detail of fourth quadrant.


Pre Implementation / Environment / Technological Innovations
Pre Implementation / Process / Change Readiness
Pre Implementation / Process / Knowledge Capital
Pre Implementation / Technology / Adoption
Pre Implementation / Technology / Adoption
Pre Implementation / Technology / Physical / Operational
Pre Implementation / Technology / Standardization
Implementation / Process / Deployment
Implementation / Process / Project Management
Implementation / Technology / Conversion
Implementation / Technology / Deployment
Post Implementation / Process / Business Interruption
Post Implementation / Process / Communication
Post Implementation / Process / Employee / Third Party Fraud
Post Implementation / Process / Measurement
Post Implementation / Technology / Access
Post Implementation / Technology / Availability
Post Implementation / Technology / Business Continuity
Post Implementation / Technology / Data Integrity
Post Implementation / Technology / Data Integrity
Post Implementation / Technology / Data Integrity
Post Implementation / Technology / Physical / Operational
Post Implementation / Technology / Relevance
Pre Implementation / Process / Alignment
Pre Implementation / Process / Customer Satisfaction
Pre Implementation / Process / Product Pricing
Pre Implementation / Technology / Adoption
Pre Implementation / Technology / Physical / Operational
Pre Implementation / Technology / Physical / Operational
Implementation / Process / Deployment
Implementation / Process / Deployment
Implementation / Technology / Change Management
Implementation / Process / Deployment
Post Implementation / Process/ Business Continuity
Post Implementation / Process / Channel Effectiveness / Partnering
Post Implementation / Process / Efficiency
Post Implementation / Process / Legal
Post Implementation / Process / Outsourcing Risk
Post Implementation / Process / Architecture
Post Implementation / Process / Availability
Post Implementation / Technology / Data Integrity
Post Implementation / Technology / Data Integrity
Post Implementation / Technology / Data Integrity
Post Implementation / Technology / Infrastructure
Post Implementation / Technology / Physical Operational
Post Implementation / Technology / Security

Permission to publish charts granted by Gillette Co. internal audit organization.

defined or aligned with overall supply-chain and business strategies. The alignment of strategies, policies, processes, organizational skills, and related capabilities is a critical success factor when reengineering processes and implementing any major new system or technology. Information requirements for decision-making, measurement, and control, as well as supporting systems, tools, and data are also important. As in all major changes, the level of knowledge, buy-in, and commitment of the human participants determines most successes or failures. Therefore, training and staff acceptance are integral to the change-management effort.

Internal auditors can play a vital role in the identification of RFID issues, risks, and process changes, ultimately impacting the technology's success in an organization.

In addition, strategy regarding controlled usage (all products/distribution channels versus limited scope) may not be effectively employed to balance infrastructure costs with associated revenue and benefits. The value proposition and scope of rollout or process automation may not be appropriately balanced and understood.

TECHNOLOGY RISKS

Arguably, implications of RFID on the IT world are among the most critical because of the amount of data moving between systems and partners. Long-term disruptions in information processing or data availability may occur. Companies may be subject to unauthorized data access by third parties and data protection issues. Support processes, including job scheduling, backup and recovery, continuity planning, and help desk services, may not be adequate.

Also, the large volumes of data collected may not be effectively used to create information relevant to manage the business or be effectively shared. For example, consider the number of discrete items in a single Wal-Mart distribution center and the points through which each item is tracked throughout the supply chain. Multiply that number by the number of Wal-Mart distribution centers in the United States and the figure is in the hundreds of millions of transactions. That's just one retailer.

The current 96-bit product codes, which are stored on Class 1 EPC tags, can uniquely identify more than 250 million manufacturers, each with more than 1 million products and unique identifiers for every product. Multiplying that out would result in transmissions of terabytes of data every day. Without relevant data mining, processing, and analytics, the collected information remains data, rather than information an organization can leverage. Forrester Research Inc., a technology research and consulting firm, predicts 5 billion consumer-packaged goods will have RFID tags by 2006.

Management of data capacity (data warehousing), scalability of systems, integration, and compatibility with existing systems may be inadequate. Excessive customization may be required of legacy systems, which could affect their performance along with increasing their support costs, and resulting in an inability to follow vendor upgrade schedules. System bandwidth may not be sufficient to fully capture, process, and validate high volumes of data.

Several of these risks are common to any application implementation and may be addressed by existing IT processes and controls. However, with the magnitude of change being brought about by RFID, additional attention and controls may be required. An organization's internal audit function can play a key role in this process by developing internal audit plans, capability assessments, project risk assessments and systems, and process reviews to ensure all identified risks are evaluated, understood, and have adequate mitigating controls in place.

PUTTING IT TOGETHER

Internal auditors need to combine an understanding of the latest technologies with the latest audit, risk, and capabilities assessment techniques to continue to provide and improve risk evaluation and control assessment, as well as process improvement services.

Key questions the internal auditor should consider in any RFID project include:

- Have key business environment risks been identified in the organization's decision to implement RFID, including payback, supply chain capability, and customer capability?
- Have key risks regarding network security been identified?
- Have risks regarding data management and integrity been identified?
- Are organizational culture and change management risks understood and addressed effectively?
- Have business processes been identified and positioned for backup or exception process purposes?
- Will additional financial controls need to be in place for processing transactions directly to ledgers from networks or tags?
- Are current business processes mapped and understood prior to implementing any changes made possible by RFID?

RFID is a promising technology that provides many potential benefits for companies across different industries. There are a variety of significant risks associated with RFID that need to be considered in any RFID endeavor. Internal auditors can play a vital role in the identification of RFID issues, risks, and process changes, ultimately impacting the technology's success in an organization.

To comment on this article, e-mail the authors at jkopalchick@theiia.org.