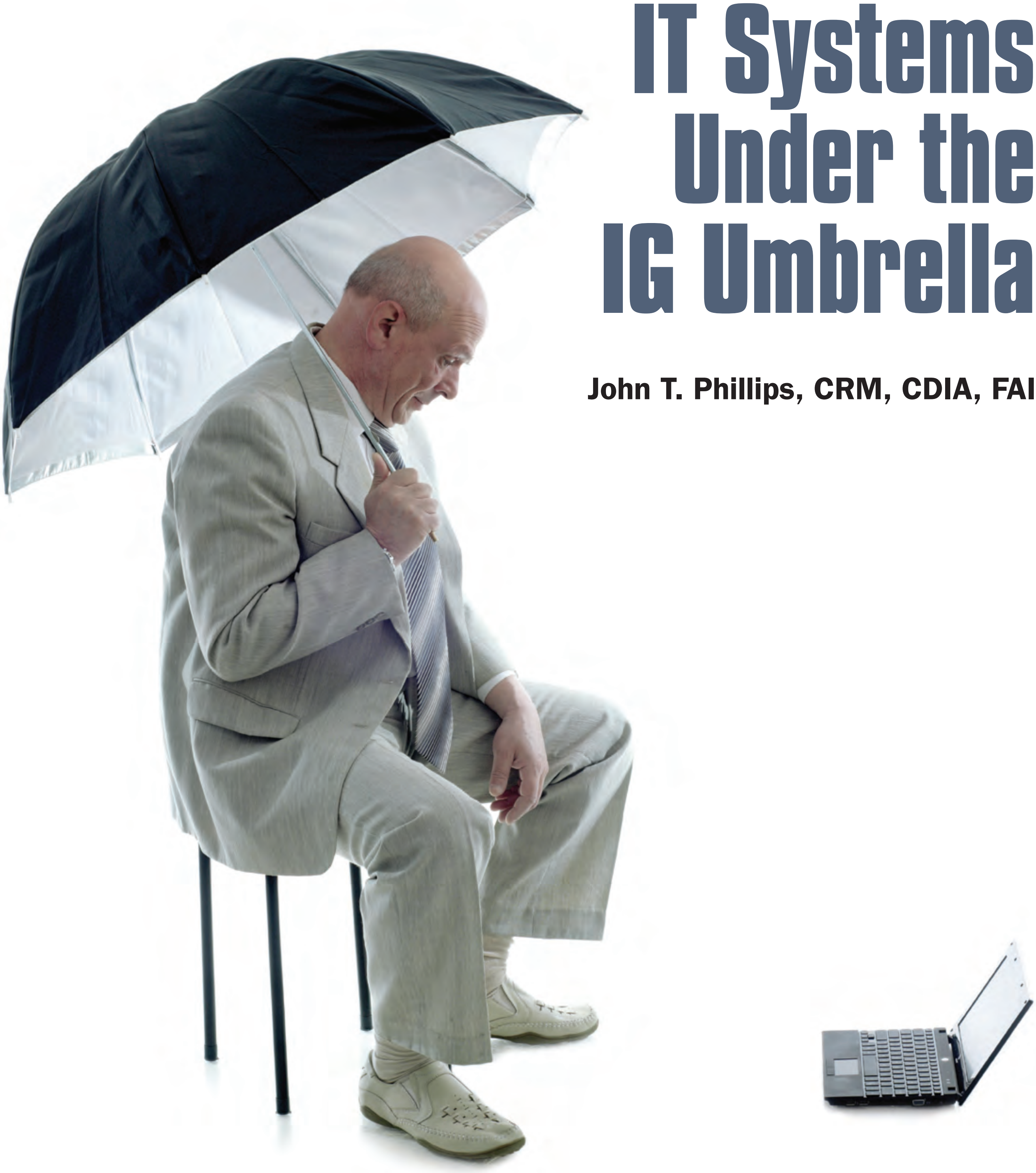
©2013 ARMA International • www.arma.org

Retiring Legacy IT Systems Under the IG Umbrella

John T. Phillips, CRM, CDIA, FAI



©2013 ARMA International • www.arma.org

When an information system is decommissioned, its data must remain usable – either in that system or in a new one to which the data is migrated – to meet retention requirements, as well as potential litigation or regulatory demands. This requires extensive, collaborative planning to ensure backwards compatibility of systems, software, and data formats.

The information technologies that enhance our daily lives – from those that drive the business processes we count on for our livelihoods to those we use for personal enjoyment – depend on hardware and software that have a life cycle.

In business, that life cycle often is extended through upgrades and enhancements, and when there is no funding for new application development, these systems often continue in use beyond what should be the ideal end of their life cycle. Because they represent "the way we've always done the work," they are referred to as *legacy* systems. They can still get the job done, but they are like dinosaurs approaching extinction.

Eventually, though, organizations realize that their legacy systems need to be superseded by more advanced and cost-effective technologies. This signals the end of their life cycle, and they are decommissioned, or retired.

It's likely that a system's legacy data will still be subject to records retention or other requirements. That is why effective information governance (IG) demands continuity of electronic records not only throughout the life cycle of the systems that contain them, but also after those systems are decommissioned.

Collaborating on System Changes

Information technology (IT) personnel have considerable incentive to support business processes with the latest computer technologies. Technical updates enhance user contentment, systems performance, and ease of maintenance over the long run.

This perspective also has special implications for decommissioning systems. When electronic records are archived, they must remain usable, and successful data migration and use of archived records depend on extensive planning to ensure backwards compatibility of systems, software, and data formats.

For that reason, when IT and users both participate in strategic planning for IT infrastructure standards, an important topic should be the long-term viability of electronic records and data. Collaboration is imperative to determining what data formats are the best choices for current and future use.

Leveraging Users' Expertise

A distinction must be made between decommissioning a system because it is no longer viable and decommissioning one because new technology can better handle that system's mission-related activities.

One of the ironies in today's business setting is that even though management typically delegates oversight of IT functions and operations to IT personnel, system users are the real experts in how well a system is working. This is because the heart of an IT system comprises the raw data and electronic records it produces and manages rather than the operational speed of its processors, disk drives, and networks.

If the electronic records and system reports are not working correctly, the users will know first. For this reason, IT system users should participate in system planning sessions and must pay close attention to a system's changes to ensure that it continues to meet workflow and data quality expectations.

Generally, as long as system users can get their daily work done, they are not concerned about infrastructure improvements, and they won't likely ask for more sophisticated solutions or for a system to be decommissioned. The quality of technology system operations is of more interest to IT personnel, as they must perform daily maintenance, upgrade software, patch "bugs," monitor security, and intervene in cases of hardware failure.

IT is far more likely than users to know ahead of time about technology advancements that will call for the organization to consider decommissioning a particular system. Once they know, though, users should also participate in planning for decommissioning a system.

Preserving Data

Decommissioning or just shutting down most computer systems usually involves some form of preservation or data migration, making the data's format and the media upon which it is recorded critical for its viability and utility.

Archiving Data, Technology

Decommissioning a legacy system could entail archiving the system's technology assets and data to ensure its complete protection. Or, it could mean just shutting down the system without taking any precautions under the assumption that the replacement system will assume all previous workflow and data management functions.

Although the complete shutdown – rather than the replacement – of a computer system is rare, it may occur when an organization or one of its functions ceases. For

©2013 ARMA International • www.arma.org

example, if a research project ends, a government agency closes, or a business declares bankruptcy and ceases to exist, there may no longer be a need for a technology system or the electronic records it contains.

However, if the research information could be used for other projects, or the government records are subject to retention rules, or the business is involved in litigation that requires the resolution of debts, the information in a decommissioned system should be preserved.

Migrating Data

In most cases the legacy system's data must be migrated into the new system to ensure new software application viability or to meet regulatory, legal, archival, or other records preservation requirements.

Government agencies may need to maintain public records for many years, or even permanently. Many of those agencies have issued extensive references to how agency systems are to be decommissioned.

For example, the Department of the Interior, Bureau of Land Management published *Information System Decommissioning Guide*, available at *http://tinyurl.com/kdd7x87*. The National Archives and Records Administration's (NARA) "Systems Development Life Cycle Checklists" provides a standardized process for all phases of system development, including decommissioning. See the checklist for that phase in Figure 1 on page 24. The full document is available at *www.archives.gov/records-mgmt/initiatives/sdlc-checklist.pdf*.

It is difficult to predict when records may be needed to support information-gathering activities. Audits can be originated by external organizations. Lawsuits can be filed by unforeseen plaintiffs with surprising claims. Disasters may demand that old data be used to reconstruct computer systems when no instances of an application survived a hurricane or tornado.

For these reasons, after migrating legacy data, an organization also might choose to preserve the original records in the decommissioned system, as it can be useful for demonstrating adherence to archival preservation mandates, achieving disaster recovery goals, or protecting the organization in e-discovery or regulatory investigations.

Choosing Storage Media

Media selected for storing decommissioned system data must be readable by computers from encoded solid state chips, tape, or disk drives. Compact disk – read only memory (CD-ROM), once the standard for long-term personal computer data storage, has given way to digital video disk (DVD), digital tape, optical tape, universal serial bus (USB) drives, and solid state multimedia cards (MMC) or secure digital (SD) devices that use "flash memory" to record data for offline use.

There is valuable debate and guidance from many informed professionals about the best method for long-term storage of data, especially from government sources, that should be considered when planning for a system shut down. For instance, NARA offers brochures providing "Tips for Scheduling Potentially Permanent Electronic Records," including e-mail, scanned images, and PDFs. Visit *www.archives.gov/publications/records-mgmt.html* to find direct links to PDF formats of these brochures.

… after migrating legacy data, an organization also might choose to preserve the original records in the decommissioned system …

Choosing the System Environment

In general, when creating a strategy for long-term data storage, consider the:

- Potential use environment for the data and electronic records
- Technology infrastructure of the environment where raw data might need to be loaded
- Operating system and application software environment:
  - A proprietary system (e.g. from Microsoft, Apple, IBM, Oracle, and others)
  - An open system (e.g., Linux operating system, C++, hypertext markup language (HTML), eXtensible markup language (XML), and other less vendor-dominated tools)

The potential use environment is the most important factor, and each decommissioning case will be different. For example, if the potential users of the electronic records are U.S.-based attorneys in e-discovery meetings, using Microsoft Windows operating system and application software and storing files in native formats with some rendered to Adobe Acrobat PDF, would probably work well, as this is the predominant document management environment for that group.

Planning for Software Obsolescence

Because software changes more often than hardware or data formats, it requires the most advanced planning. Organizations generally upgrade software on most machines every year, while their operating systems might receive just a few bug patches during that period.

Some software upgrades don't cause compatibility problems. Different versions of Microsoft Word, for instance, may be upgraded on the same computer with little or no

©2013 ARMA International • www.arma.org

changes in data formats. This kind of technology transitioning on existing computers increases functionality to manage more complex records, but it does not create backwards compatibility problems that would occur if the new software recognized only its new data format.

Choosing Data Formats

Changing business models create a need for innovative records and associated workflow processes. Fortunately, data formats like HTML, XML, and PDF are all used widely in many software application environments (and are not exclusively software vendor-driven), thus creating an inherent content longevity for any information stored in these formats.

A complicating factor for many organizations is their reliance on vendor software that creates proprietary data formats. There are few data file formats independent in design, though, as many vendors participate in setting standards for software and then try to make their own file formats compatible.

For example, although the PDF file format is often referred to as a *de facto industry standard*, the internal code for creating these files, which was licensed to Adobe until July 2008, was subsequently released as a royalty-free, open standard published by the International Organization for Standardization (ISO) as ISO 32000-1:2008 *Document management – Portable document format – Part 1: PDF 1.7.*

Integrating Records Management into the Systems Development Life Cycle

Phase 9. Retirement and Rollover

1. At the time of retirement or rollover of the system, are records preserved, retained, and fully accessible for the full retentions in accordance with appropriate dispositions?
2. At the time of retirement or rollover of the system, are temporary records destroyed in accordance with appropriate dispositions?
3. At the time of retirement or rollover of the system, are permanent records transferred to NARA in accordance with the appropriate dispositions?

Figure 1: "Integrating RM into the SDLC" **Source:** National Archives and Records Administration "Systems Development Life Cycle Checklists."

Organizations must ensure there will be no long-term issues with file formats used to store decommissioned electronic records. Although most vendors offer several file formats in which their applications can store data, some options may not be in compliance with regulatory guidelines or litigation readiness demands. In fact, deploying most open systems software solutions also promotes a dependence on open systems software maintenance services, which may have limited options. Planning ahead for future access requirements is the key.

Recreating Software Applications

Recreating actual software applications in order to view records is costly and time consuming. So, organizations might elect to preserve the original application software in case it is needed to generate accurate records.

Planning for E-Discovery Challenges

E-discovery presents special challenges related to decommissioning systems, preserving their legacy data over time, and producing it as authentic, credible evidence for litigation- or regulatory-related purposes.

Data maps, which describe the locations and nature of electronic records, are of considerable value when stored information must be located, held, and produced. To ensure their value, successive data maps should be linked in a manner that allows systems migrations or transformations to be understood.

Using these tools will enhance the organization's ability to implement credible legal holds, minimize the cost of its discovery, and improve the utility of the information. They will be especially useful if a large amount of information must be shared during "meet and confer" sessions, during which judges expect attorneys to resolve e-discovery issues before litigation in court begins.

Maintaining Credibility

Once a hold is issued, records subject to the hold must be preserved within their existing computer system or by migration into a records hold repository. Maintaining these records within an existing system can become a problem if that system needs software upgrades that save old records in newer data formats, as this potentially impacts their evidentiary credibility.

Older documents saved in new data formats may not exhibit the same look and feel of the original records. Newer software may not recognize certain fonts or graphics that were generated in older applications. Sometimes the only way to ensure that electronic documents can be properly displayed and printed is to test each document during a system migration, which is a costly and time-consuming process. This can be made less onerous by testing randomly chosen sets of data instead.

Complying with Retention

Outsourcing the retention of electronic records to e-discovery software vendors may present another danger; they may not know that those records are subject to retention rules that exceed immediate needs for records holds. One can only assume that e-discovery vendors are responsible for the retention periods spelled out in their contracts.

Decommissioning Under the IG Umbrella

When organizations design and implement IG programs, they must address the complete life cycle of in-

©2013 ARMA International • www.arma.org

formation – from creation to disposition. That includes information in operational systems, in system backups, and in specialized data archiving repositories.

Once an IT system has been identified as having reached the end of its lifecycle, appropriate staff and budget resources must be available to plan and perform decommissioning activities, beginning with data migration, if needed, and ending with the post-decommission review.

Organizations may find that planning for de-commissioning coincides well with implementing disaster protection programs or performing records cleanup and destruction activities; these actions typically direct the responsible destruction of electronic records and involve people who know how to address data security, privacy, and other information risks.

Because the goal of IG programs is to encompass all electronic records repositories and data archives, they must address the offline data and software archives that decommissioning of systems creates.

IG programs must inherently incorporate strategic planning for evolving technologies. Standardization of supported data formats, applications software, and operating systems is an important component of IG tactical initiatives. E-discovery issues, including authenticity of data and chain of custody documentation, that enhance the credibility of evidence can be addressed early in the life cycle of information by ensuring that any system proposed for decommissioning is managed thoroughly under the umbrella of a properly managed IG program. **END**

John T. Phillips, CRM, CDIA, FAI, can be contacted at john@infotechdecisions.com. *See his bio on page 47.*