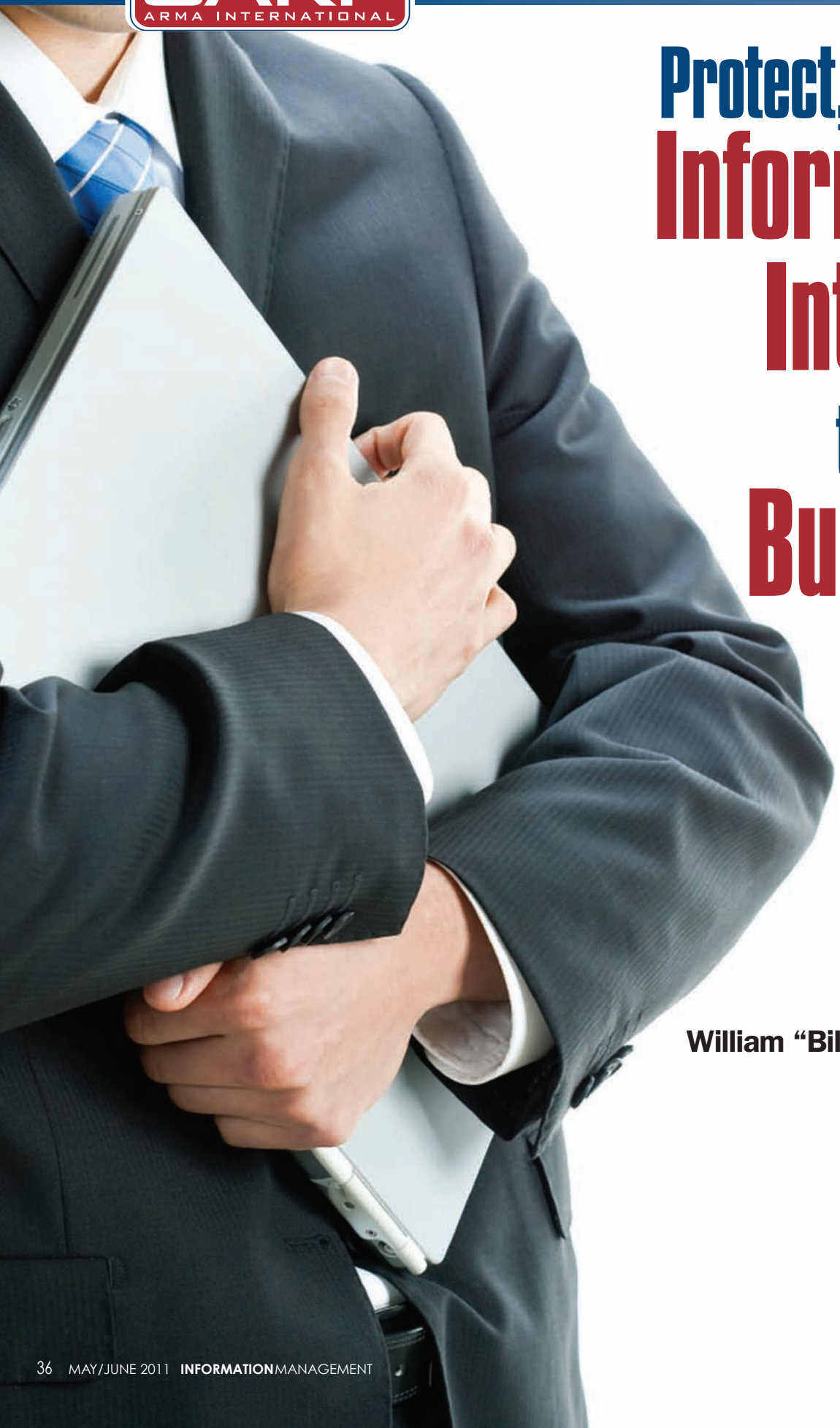

Protect, Maintain Information Integrity to Reduce Business Risk

William "Bill" Manago, CRM

In today's business world, information is the life blood of the organization. Information assets provide the data that describes the activities of the organization: what it has done and what it plans to do in the future. Some information is in the form of official business records, but the majority is in the form of electronically stored information that is unstructured, unmanaged, and stored on any number of data repositories and file shares.

Today's information landscape includes a wide range of content formats (e.g., audio, video, web, and social media). This data is created, received, and collected to:

- Facilitate and sustain day-to-day operations
- Support predictive activities, such as budgeting and planning
- Assist in answering questions about past decisions and activities
- Demonstrate and document compliance with applicable laws, regulations, and standards

This environment creates a tremendous challenge for effectively managing business records and information.

Using GARP® to Meet the Challenge

ARMA International's Generally Accepted Recordkeeping Principles® (GARP®) define the discipline of *records and information management,* which refers to the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with records creation, maintenance, use, and disposition to achieve adequate and proper documentation of the policies and transactions of an organization and the effective and economical management of the organization's operations.

GARP® codifies thousands of years of evolving records practices into eight principles for ensuring information's: accountability, integrity, protection, compliance, availability, retention, disposition, and transparency. This article focuses on the principles of integrity and protection; see *www.arma.org/garp* to view all eight annotated principles.

The complementary GARP® Information Governance Maturity Model is a blueprint for measuring risks that come from shortcomings in records programs. (See the model, too, at *www.arma.org/garp*.) *Information governance* (IG) refers to the multidisciplinary structures, policies, procedures, processes, and controls implemented to manage information on all media in such a way that it supports an organization's immediate and future regulatory, legal, risk, environmental, and operational requirements. Effective IG can enhance the quality, availability, and integrity of an organization's information.

IG is a holistic approach to maintaining an organization's information in accordance with an expanding set of legal, regulatory, and privacy requirements. Once these requirements have been identified, the organization should implement a series of governance standards and internal controls so its information is effectively and efficiently managed. IG includes the processes, roles, standards, and metrics to guarantee the effective and efficient use of information throughout the organization.

GARP® can be applied holistically using policy-driven methods to create, manage, control, secure, discover, and dispose of all information – not just records. With the integration of GARP® and IG, companies are better able to mitigate risk, increase customer service, and decrease the cost of maintaining data, information, and records needed to support business operations.

Examining the Principle of Integrity

GARP®s Principle of Integrity states that recordkeeping programs should be constructed to ensure a reasonable and suitable guarantee of authenticity and reliability of records and information generated or managed by or for the organization. The Principle of Integrity assumes that records have not been changed or altered since they were declared and managed as records.

Organizations increasingly rely upon their information as a valuable asset to develop significant competitive advantage, make sound business decisions, and support business operations. Organizations are constantly challenged to proactively manage information and to verify the quality, security, and trustworthiness of their information assets.

A holistic approach to the Principle of Integrity examines more than the authenticity of a record, once captured. It takes into account the technology tools used to capture and manage information, the quality of the processes used to create or receive information, and the people involved in the process. It also takes into account how information is processed and what information is needed to document the activities of the organization.

In a study "How Much Information? 2003" (supplemented by insights from the U.S. National Science Foundation), researchers from the University of California-Berkeley's School of Information Management calculated that for every piece of information available in front of a reader, an estimated 10 pieces of related information (e.g., rough drafts, notes, raw data, copies, and various versions) are stored elsewhere in the organization.

Therefore, for every document or dataset included in a presentation to senior management, there are 10 related documents or datasets not included. This begs the question, "How will they know if the information presented is of the highest quality, accurate, and complete?" All information used to make business decisions and/or to document regulatory com-

pliance must be accurate, complete, and attributable.

The study is often cited as the source of the notion that only 5% to 6% of information within an organization meets the definition of and are managed as records, while the remaining 94% to 95% of information holdings are largely unmanaged, discoverable, and, therefore, pose significant risk to the organization's success.

Apply Rules Across the Information Supply Chain

To accomplish the goal of information integrity, organizations must examine the flow of information across their information supply chain within and between enterprises. Quality rules and processes must be implemented at each information entry point.

These rules and policies need to:

- Be adhered to as the information flows across the organization
- Ensure that processes are measurable, repeatable, and automated. If the information at its source is of the highest quality, then any dependent systems can trust that data received is of high quality and reliable.

The information supply chain describes how information is shared by activities that distribute useful information among multiple entities (e.g., people, systems, or business units) in an open environment. Sharing information should address four questions:

1) *What* should be shared?
2) With *whom* should it be shared?
3) *How* should it be shared?
4) *When* should it be shared?

Organizations that can answer these questions can confirm they are using proper, accurate information and greatly improve information-sharing results, avoid overload or deficiency, reduce sharing costs, and be more responsive to requests for information and discovery.

Profile to Determine Quality, Integrity

Once information has been obtained and stored, it needs to be profiled to determine its quality and integrity. The profile of a piece of information should consist of key attributes that would allow an auditor to trace the step-by-step history of the information, beginning with its creation or receipt, to establish an effective chain of custody.

The audit trail should:

- Provide a history of changes made to a piece of information, either manually or within a system
- Enable the enforcement of accountability
- Enable an auditor to retrieve and vouch for data
- Assist the auditor in determining

Data Integrity in the News

There are numerous news reports about organizations that failed to produce and maintain quality and accurate records. Following are several notable examples of the importance of good IG practices:

- In the financial calamity that occurred in the U.S. housing market collapse and the Bernard Madoff investment swindle, voluminous, meticulous records existed. But in these two cases, processes were not in place to ensure the information's accuracy and integrity, and may have, in fact, served to obscure the true nature of the organizations' business transactions, making it difficult for regulators to detect impropriety.
- Puget Sound Energy faces a $2 million proposed fine for the actions of a contractor that allegedly falsified records of gas line leak inspections, according to *The Seattle Times*.
- The Nebraska State Auditor's Office released findings that suggested sloppy financial recordkeeping within the Omaha Fire Department. The Auditor's Office stopped short of calling the findings fraud, stating that, "We can't audit records that don't exist; we can't audit processes that are not in place."
- The mismanagement of gravesite information at Arlington National Cemetery, as excerpted from the March 31, 2011, issue of *Time* magazine, resulted in hundreds of unmarked and mismarked graves:

  Time Reveals New Details of Poor Record Keeping at Arlington National Cemetery

  There are disturbing new details emerging about past mismanagement and poor record keeping at Arlington National Cemetery. The situation is putting into question whether or not America's honored fallen have been buried in the correct graves.

  [Democratic Senator Mark] Warner [of Virginia] announced he is sponsoring a new law to stop another old Arlington practice – saving prime burial spots for VIPs. He says the cemetery's system of keeping records on index cards both contributed to the mix up and provided cover for it.

  The new head of the cemetery, Katherine Condon, has undertaken the job of computerizing the cemetery's old record keeping, and told *Time* she's confident they can be sorted out without resorting to digging the more than 300,000 graves at Arlington.

the source, integrity, and quality of the information and who originated the data

Characteristics of an effective audit trail include:

- Date and time of creation and/or receipt
- Person who created or processed the information transaction
- Where the information was processed
- Changes made to the information over time
- Organization's purpose for the information
- Organization's application(s) that use the information

The Securities and Exchange Commission has recently proposed a consolidated audit trail that system regulators can use to track information related to trading orders received and executed across the securities markets. The audit trail will include several information attributes. It will require:

- Every exchange and the Financial Industry Regulatory Authority (FINRA), as well as their respective members, to provide certain detailed information to a newly created central repository regarding each quote and order in a national market system security, and each reportable event with respect to each quote and order
- Self-regulatory organizations and its members to provide a majority of the required order and event information to the central repository in real time or close to real time
- Each member of an exchange or FINRA to "tag" each order received or originated by the member with a unique order identifier that would be reported to the central repository. The identifier would remain with that order throughout its life, including routing, modification, execution, and cancellation.
- Each customer to be assigned a unique customer identifier that would be the same for that customer, in a uniform format, across all broker dealers

Examining the Principle of Protection

GARP's Principle of Protection states, "A recordkeeping program shall provide a reasonable level of protection to records and information that are private, confidential, privileged, secret, or essential to business continuity." Information generated by an organization in the course of business requires various degrees of protection, which is mandated by laws, regulations, and/or corporate governance. This amount of protection is necessary to provide surety that information critical to an organization's continued operation during or after a crisis is available.

Lack of Data Protection in the News

Several headlines of significance demonstrate the need for the GARP's® Principle of Protection:

FEMA Loses Lessons Learned Data (*InformationWeek*, February 9, 2011) – The Federal Emergency Management Agency (FEMA) has been without access to years' worth of lessons-learned data for nine months, unable to recover access to it since a server failure in May 2010, according to a newly issued report by the Department of Homeland Security's inspector general.

While the data was recovered by November 2010, the software needed to read it hasn't been restored, meaning that FEMA personnel aren't able to access certain historical data stretching back to 2004, before Hurricane Katrina, California wildfires, and other major recent disasters.

Former State Senator Accused of Destroying Documents (*wgrz.com*, January 4, 2011) – Sen. Mark Grisanti's (R-Buffalo) staff [on their first day on the job] found their Buffalo office empty of important files. In response to Grisanti's letter to outgoing New York State Senator Antoine Thompson (D-Buffalo) asking that all relevant documents be secured during the transition, "[Thompson] said he would keep all relevant documents secured during the transition, but that was not the case," television station WGRZ quoted Grisanti's chief of staff, Doug Curella, as saying.

The television station reported it found many of the missing documents filed into several garbage cans in the basement of the Mahoney State Office Building. Some were shredded.

Ex-Citadel Exec Pays $1.1 Million for Destroying Evidence (*FINalternatives.com,* October 2010) – Mikhail Malyshev, the former Citadel Investment Group executive whose launch of a high-frequency trading firm led to a lawsuit from his former employers, has paid $1.1 million in sanctions for destroying evidence in the case.

Zurich Insurance Fined £2.3m over Customers' Data Loss (BBC, August 2010) – The UK operation of Zurich Insurance has been fined £2.27 million (more than $3.25 million U.S.) by the Financial Services Authority for losing personal details of 46,000 customers. It is the highest fine levied on a single firm for data security failings.

A recordkeeping program must include appropriate protection controls that:

- Are applied to information from the moment it is created to the moment it undergoes final disposition
- Should protect against unauthorized alteration, destruction, loss, or disclosure of information
- Encompass the steps needed to keep the information in a computer and human-readable format
- Are accessed by authorized personnel only

Therefore, every system that generates, stores, and uses information should be examined with the Principle of Protection in mind to guarantee appropriate controls are applied to them.

As the foundation of data governance, the Principle of Protection can be applied holistically to all of the information held by an organization. *Data governance* (DG) is an industry term that defines the framework of people, processes, and permissions, or access rights, employed to verify proper data use. All enterprises need a strategy and process that governs appropriate and authorized use of business data.

DG includes all aspects of information (e.g, spoken, written, printed, electronic, or other medium) and information handling (e.g., created, viewed, transported, stored, or destroyed). This holistic approach to information protection should significantly reduce the risk of data misuse. A comprehensive, policy-driven DG program should deliver:

- Effective and scalable data access control
- Better and consistent data protection
- Decrease in cost and complexity of data control
- Comprehensive and granular audit of data use

The practices and techniques to consider when developing a data protection strategy are:

- *Backup and recovery* – The safeguarding of data by making offline copies of the data to be restored in the event of a disaster or data corruption
- *Remote data movement* – The real-time or near-real-time moving of data to a location outside the primary storage system or to another facility to protect against physical damage to systems and buildings. The two most common forms of this technique are remote copy and replication. These techniques duplicate data from one system to another system in a different location.
- *Storage system security* – Applying best practices and security technology to the storage system to augment server and network security measures
- *Data lifecycle management (DLM)* – The automated movement of critical data to online and offline storage. Important aspects of DLM are placing data considered to be in a final state into read-only storage where it cannot be changed and moving data to different types of storage, depending on its age.
- *Information lifecycle management (ILM)* – A comprehensive strategy for valuing, cataloging, and protecting information assets that is also tied to regulatory compliance. ILM, while similar to DLM, oper-

ates on information, not raw data. Decisions are driven by the content of the information, requiring policies to take into account its context.

All these methods should be deployed together to form a proper data protection strategy.

This holistic approach using the GARP® Principles of Integrity and Protection will significantly reduce an organization's risk of data misuse. The complex and critical nature of information security and its governance demand that it be elevated to the highest organizational levels. As a critical resource, information must be treated like any other asset essential to the survival and success of the organization.

William "Bill" Manago, CRM, can be contacted at william.manago@autonomy.com. *See his bio on page 51.*