INFORMATION GOVERNANCE

FOR BUSINESS DOCUMENTS AND RECORDS

ROBERT F. SMALLWOOD

INFORMATION GOVERNANCE

Founded in 1807, John Wiley & Sons is the oldest independent publishing company in the United States. With offices in North America, Europe, Asia, and Australia, Wiley is globally committed to developing and marketing print and electronic products and services for our customers' professional and personal knowledge and understanding.

The Wiley CIO series provides information, tools, and insights to IT executives and managers. The products in this series cover a wide range of topics that supply strategic and implementation guidance on the latest technology trends, leadership, and emerging best practices.

Titles in the Wiley CIO series include:

The Agile Architecture Revolution: How Cloud Computing, REST-Based SOA, and Mobile Computing Are Changing Enterprise IT by Jason Bloomberg

Big Data, Big Analytics: Emerging Business Intelligence and Analytic Trends for Today's Businesses by Michael Minelli, Michele Chambers, and Ambiga Dhiraj

The Chief Information Officer's Body of Knowledge: People, Process, and Technology by Dean Lane

CIO Best Practices: Enabling Strategic Value with Information Technology (Second Edition) by Joe Stenzel, Randy Betancourt, Gary Cokins, Alyssa Farrell, Bill Flemming, Michael H. Hugos, Jonathan Hujsak, and Karl Schubert

The CIO Playbook: Strategies and Best Practices for IT Leaders to Deliver Value by Nicholas R. Colisto

Enterprise Performance Management Done Right: An Operating System for Your Organization by Ron Dimon

Executive's Guide to Virtual Worlds: How Avatars Are Transforming Your Business and Your Brand by Lonnie Benson

IT Leadership Manual: Roadmap to Becoming a Trusted Business Partner by Alan R. Guibord

Managing Electronic Records: Methods, Best Practices, and Technologies by Robert F. Smallwood

On Top of the Cloud: How CIOs Leverage New Technologies to Drive Change and Build Value Across the Enterprise by Hunter Muller

Straight to the Top: CIO Leadership in a Mobile, Social, and Cloud-based World (Second Edition) by Gregory S. Smith

Strategic IT: Best Practices for Managers and Executives by Arthur M. Langer and Lyle Yorks

Transforming IT Culture: How to Use Social Intelligence, Human Factors, and Collaboration to Create an IT Department That Outperforms by Frank Wander

Unleashing the Power of IT: Bringing People, Business, and Technology Together by Dan Roberts

The U.S. Technology Skills Gap: What Every Technology Executive Must Know to Save America's Future by Gary J. Beach

Information Governance: Concepts, Strategies and Best Practices by Robert F. Smallwood

INFORMATION GOVERNANCE

CONCEPTS, STRATEGIES AND BEST PRACTICES

Robert F. Smallwood

WILEY

Cover image: © iStockphoto / IgorZh
Cover design: Wiley

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at http://booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

Library of Congress Cataloging-in-Publication Data:

Smallwood, Robert F., 1959-
Information governance : concepts, strategies, and best practices / Robert F. Smallwood.
pages cm. — (Wiley CIO series)
ISBN 978-1-118-21830-3 (cloth); ISBN 978-1-118-41949-6 (ebk); ISBN 978-1-118-42101-7 (ebk)
1. Information technology—Management. 2. Management information systems. 3. Electronic records—Management. I. Title.
HD30.2.S617 2014
658.4'038—dc23

2013045072

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

For my sons

and the next generation of tech-savvy managers

CONTENTS

PREFACE

Information governance (IG) has emerged as a key concern for business executives and managers in today's environment of Big Data, increasing information risks, colossal leaks, and greater compliance and legal demands. But few seem to have a clear understanding of what IG is; that is, how you define what it is and is not, and how to implement it. This book clarifies and codifies these definitions and provides key insights as to how to implement and gain value from IG programs. Based on exhaustive research, and with the contributions of a number of industry pioneers and experts, this book lays out IG as a complete discipline in and of itself for the first time.

IG is a super-discipline that includes components of several key fields: law, records management, information technology (IT), risk management, privacy and security, and business operations. This unique blend calls for a new breed of information professional who is competent across these established and quite complex fields. Training and education are key to IG success, and this book provides the essential underpinning for organizations to train a new generation of IG professionals.

Those who are practicing professionals in the component fields of IG will find the book useful in expanding their knowledge from traditional fields to the emerging tenets of IG. Attorneys, records and compliance managers, risk managers, IT managers, and security and privacy professionals will find this book a particularly valuable resource.

The book strives to offer clear IG concepts, actionable strategies, and proven best practices in an understandable and digestible way; a concerted effort was made to simplify language and to offer examples. There are summaries of key points throughout and at the end of each chapter to help the reader retain major points. The text is organized into five parts: (1) Information Governance Concepts, Definitions, and Principles; (2) IG Risk Assessment and Strategic Planning; (3) IG Key Impact Areas; (4) IG for Delivery Platforms; and (5) Long-Term Program Issues. Also included are appendices with detailed information on taxonomy and metadata design and on records management and privacy legislation.

One thing that is sure is that the complex field of IG is evolving. It will continue to change and solidify. But help is here: No other book offers the kind of comprehensive coverage of IG contained within these pages. Leveraging the critical advice provided here will smooth your path to understanding and implementing successful IG programs.

Robert F. Smallwood

ACKNOWLEDGMENTS

I would like to sincerely thank my colleagues for their support and generous contribution of their expertise and time, which made this pioneering text possible.

Many thanks to Lori Ashley, Barb Blackburn, Barclay Blair, Charmaine Brooks, Ken Chasse, Monica Crocker, Charles M. Dollar, Seth Earley, Dr. Patricia Franks, Randy Kahn, Paula Lederman, and Barry Murphy.

I am truly honored to include their work and owe them a great debt of gratitude.

PART ONE

Information Governance Concepts, Definitions, and Principles

CHAPTER 1

The Onslaught of Big Data and the Information Governance Imperative

The value of information in business is rising, and business leaders are more and more viewing the ability to govern, manage, and harvest information as critical to success. Raw data is now being increasingly viewed as an asset that can be leveraged, just like financial or human capital.[1] Some have called this new age of "Big Data" the "industrial revolution of data."

According to the research group Gartner, Inc., Big Data is defined as "high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making."[2] A practical definition should also include the idea that the amount of data—both structured (in databases) and unstructured (e.g., e-mail, scanned documents) is so massive that it cannot be processed using today's database tools and analytic software techniques.[3]

In today's information overload era of Big Data—characterized by massive growth in business data volumes and velocity—the ability to distill key insights from enormous amounts of data is a major business differentiator and source of sustainable competitive advantage. In fact, a recent report by the World Economic Forum stated that data is a new asset class and personal data is "the new oil."[4] And we are generating more than we can manage effectively with current methods and tools.

The Big Data numbers are overwhelming: Estimates and projections vary, but it has been stated that 90 percent of the data existing worldwide today was created in the last two years[5] and that every two days more information is generated than was from the dawn of civilization until 2003.[6] This trend will continue: The global market for Big Data technology and services is projected to grow at a compound annual rate of 27 percent through 2017, about six times faster than the general information and communications technology (ICT) market.[7]

Many more comparisons and statistics are available, and all demonstrate the incredible and continued growth of data.

Certainly, there are new and emerging opportunities arising from the accumulation and analysis of all that data we are busy generating and collecting. New enterprises are springing up to capitalize on data mining and business intelligence opportunities. The U.S. federal government joined in, announcing $200 million in Big Data research programs in 2012.[8]

The onslaught of Big Data necessitates that information governance (IG) be implemented to discard unneeded data in a legally defensible way.

But established organizations, especially larger ones, are being crushed by this onslaught of Big Data: It is just too expensive to keep all the information that is being generated, and unneeded information is a sort of irrelevant sludge for decision makers to wade through. They have difficulty knowing which information is an accurate and meaningful "wheat" and which is simply irrelevant "chaff." This means they do not have the precise information they need to base good business decisions upon.

And all that Big Data piling up has real costs: The burden of massive stores of information has increased storage management costs dramatically, caused overloaded systems to fail, and increased legal discovery costs.[9] Further, the longer that data is kept, the more likely that it will need to be migrated to newer computing platforms, driving up conversion costs; and legally, there is the risk that somewhere in that mountain of data an organization stores is a piece of information that represents a significant legal liability.[10]

This is where the worlds of Big Data and business collide. For Big Data proponents, more data is always better, and there is no perceived downside to accumulation of massive amounts of data. In the business world, though, the realities of legal **e-discovery** mean the opposite is true.[11] To reduce risk, liability, and costs, it is critical for unneeded information to be disposed of in a systematic, methodical, and "legally defensible" (justifiable in legal proceedings) way, when it no longer has legal, regulatory, or business value. And there also is the high-value benefit of basing decisions on better, cleaner data, which can come about only through rigid, enforced **information governance** (IG) policies that reduce information glut.

Organizations are struggling to reduce and right-size their information footprint by discarding superfluous and redundant data, e-documents, and information. *But the critical issue is devising policies, methods, and processes and then deploying information technology (IT) to sort through which information is valuable and which no longer has business value and can be discarded.*

IT, IG, risk, compliance, and legal representatives in organizations have a clear sense that most of the information stored is unneeded, raises costs, and poses risks. According to a survey taken at a recent Compliance, Governance and Oversight Counsel summit, respondents estimated that approximately 25 percent of information stored in organizations has real business value, while 5 percent must be kept as business records and about 1 percent is retained due to a litigation hold. *"This means that*

Big Data values massive accumulation of data, whereas in business, e-discovery realities and potential legal liabilities dictate that data be culled to only that which has clear business value.

Only about one quarter of information organizations are managing has real business value.

With a smaller information footprint, it is easier for organizations to find the information they need and derive business value from it.

[about] 69 percent of information in most companies has no business, legal, or regulatory value. Companies that are able to dispose of this data debris return more profit to shareholders, can leverage more of their IT budgets for strategic investments, and can avoid excess expense in legal and regulatory response" (emphasis added).[12]

With a smaller ***information footprint****, organizations can more easily find what they need and derive business value from it.*[13] They must eliminate the data debris regularly and consistently, and to do this, processes and systems must be in place to cull valuable information and discard the data debris daily. An IG program sets the framework to accomplish this.

The business environment has also underscored the need for IG. According to Ted Friedman at Gartner, "The recent global financial crisis has put information governance in the spotlight. . . . [It] is a priority of IT and business leaders as a result of various pressures, including regulatory compliance mandates and the urgent need for improved decision-making."[14]

And IG mastery is critical for executives: Gartner predicts that by 2016, *one in five chief information officers in regulated industries will be fired from their jobs for failed IG initiatives.*[15]

Defining Information Governance

IG is a sort of super discipline that has emerged as a result of new and tightened legislation governing businesses, external threats such as hacking and data breaches, and the recognition that multiple overlapping disciplines were needed to address today's information management challenges in an increasingly regulated and litigated business environment.[16]

IG is a subset of corporate governance, and includes key concepts from records management, content management, IT and data governance, information security, data privacy, risk management, litigation readiness, regulatory compliance, **long-term digital preservation**, and even business intelligence. This also means that it includes related technology and discipline subcategories, such as document management, enterprise search, knowledge management, and business continuity/disaster recovery.

IG is a subset of corporate governance.

IG is a sort of superdiscipline that encompasses a variety of key concepts from a variety of related disciplines.

Practicing good IG is the essential foundation for building legally defensible disposition practices to discard unneeded information and to secure confidential information, which may include trade secrets, strategic plans, price lists, blueprints, or personally identifiable information (PII) subject to privacy laws; it provides the basis for consistent, reliable methods for managing data, e-documents, and records.

Having trusted and reliable records, reports, data, and databases enables managers to make key decisions with confidence.[17] And accessing that information and business intelligence in a timely fashion can yield a long-term sustainable competitive advantage, creating more agile enterprises.

To do this, organizations must standardize and systematize their handling of information. They must analyze and optimize how information is accessed, controlled, managed, shared, stored, preserved, and audited. They must have complete, current, and relevant policies, processes, and technologies to manage and control information, including *who* is able to access what information, and *when*, to meet external legal and regulatory demands and internal governance policy requirements. In short, IG is about information control and compliance.

IG is a subset of corporate governance, which has been around as long as corporations have existed. IG is a rather new multidisciplinary field that is still being defined, but has gained traction increasingly over the past decade. The focus on IG comes not only from compliance, legal, and records management functionaries but also from executives who understand they are accountable for the governance of information and that theft or erosion of information assets has real costs and consequences.

"Information governance" is an all-encompassing term for *how an organization manages the totality of its information.*

According to the **Association of Records Managers and Administrators** (ARMA), IG is "a strategic framework composed of standards, processes, roles, and metrics that hold organizations and individuals accountable to create, organize, secure, maintain, use, and dispose of information in ways that align with and contribute to the organization's goals."[18]

IG includes the set of policies, processes, and controls to manage information in compliance with external regulatory requirements and internal governance frameworks. Specific policies apply to specific data and document types, records series, and other business information, such as e-mail and reports.

Stated differently, IG is "a quality-control discipline for managing, using, improving, and protecting information."[19]

Practicing good IG is the essential foundation for building legally defensible disposition practices to discard unneeded information.

IG is "a strategic framework composed of standards, processes, roles, and metrics, that hold organizations and individuals accountable to create, organize, secure, maintain, use, and dispose of information in ways that align with and contribute to the organization's goals."[20]

IG is how an organization maintains security, complies with regulations, and meets ethical standards when managing information.

Fleshing out the definition further: "Information governance is policy-based management of information designed to lower costs, reduce risk, and ensure compliance with legal, regulatory standards, and/or corporate governance."[21] IG necessarily incorporates not just policies but information technologies to audit and enforce those policies. The IG team must be cognizant of information lifecycle issues and be able to apply the proper retention and disposition policies, including digital preservation where records need to be maintained for long periods.

IG Is Not a Project, But an Ongoing Program

IG is an ongoing program, not a one-time project. IG provides an umbrella to manage and control information output and communications. Since technologies change so quickly, it is necessary to have overarching policies that can manage the various IT platforms that an organization may use.

Compare it to a workplace safety program; every time a new location, team member, piece of equipment, or toxic substance is acquired by the organization, the workplace safety program should dictate how that is handled. If it does not, the workplace safety policies/procedures/training that are part of the workplace safety program need to be updated. Regular reviews are conducted to ensure the program is being followed and adjustments are made based on the findings. *The effort never ends*.[22] The same is true for IG.

IG is not only a tactical program to meet regulatory, compliance, and litigation demands. It can be *strategic*, in that it is the necessary underpinning for developing a management strategy that maximizes knowledge worker productivity while minimizing risk and costs.

Why IG Is Good Business

IG is a tough sell. It can be difficult to make the business case for IG, unless there has been some major compliance sanction, fine, legal loss, or colossal data breach. In fact, *the largest*

IG is a multidisciplinary program that requires an ongoing effort.

impediment to IG adoption is simply identifying its benefits and costs, according to the Economist Intelligence Unit. Sure, the enterprise needs better control over its information, but how much better? At what cost? What is the payback period and the return on investment?[23]

It is challenging to make the business case for IG, yet making that case is fundamental to getting IG efforts off the ground.

Here are eight reasons why IG makes good business sense, from IG thought leader Barclay Blair:

1. *We can't keep everything forever.* IG makes sense because it enables organizations to get rid of unnecessary information in a defensible manner. Organizations need a sensible way to dispose of information in order to reduce the cost and complexity of the IT environment. Having unnecessary information around only makes it more difficult and expensive to harness information that has value.
2. *We can't throw everything away.* IG makes sense because organizations can't keep everything forever, nor can they throw everything away. We need information—the right information, in the right place, at the right time. Only IG provides the framework to make good decisions about what information to keep.
3. *E-discovery.* IG makes sense because it reduces the cost and pain of discovery. Proactively managing information reduces the volume of information exposed to e-discovery and simplifies the task of finding and producing responsive information.
4. *Your employees are screaming for it—just listen.* IG makes sense because it helps knowledge workers separate "signal" from "noise" in their information flows. By helping organizations focus on the most valuable information, IG improves information delivery and improves productivity.
5. *It ain't gonna get any easier.* IG makes sense because it is a proven way for organizations to respond to new laws and technologies that create new requirements and challenges. The problem of IG will not get easier over time, so organizations should get started now.
6. *The courts will come looking for IG.* IG makes sense because courts and regulators will closely examine your IG program. Falling short can lead to fines, sanctions, loss of cases, and other outcomes that have negative business and financial consequences.
7. *Manage risk: IG is a big one.* Organizations need to do a better job of identifying and managing risk. The risk of information management failures is a critical risk that IG helps to mitigate.
8. *E-mail: Reason enough.* IG makes sense because it helps organizations take control of e-mail. Solving e-mail should be a top priority for every organization.[24]

Failures in Information Governance

The failure to implement and enforce IG can lead to vulnerabilities that can have dire consequences. The theft of confidential U.S. National Security Agency documents by Edward Snowden in 2013 could have been prevented by properly enforced IG. Also, Ford Motor Company is reported to have suffered a loss estimated at $50 to $100 million as a result of the theft of confidential documents by one of its own employees. A former product engineer who had access to thousands of trade secret documents and designs sold them to a competing Chinese car manufacturer. A strong IG program would have controlled and tracked access and prevented the theft while protecting valuable intellectual property.[25]

Law enforcement agencies have also suffered from poor IG. In a rather frivolous case in 2013 that highlighted the lack of policy enforcement for the mobile environment, it was reported that U.S. agents from the Federal Bureau of Investigation used government-issued mobile phones to send explicit text messages and nude photographs to coworkers. The incidents did not have a serious impact but did compromise the agency and its integrity, and "adversely affected the daily activities of several squads."[26] Proper mobile communications policies were obviously not developed and enforced.

IG is also about information security and privacy, and serious thought must be given when creating policies to safeguard personal, classified or confidential information. Schemes to compromise or steal information can be quite deceptive and devious, masked by standard operating procedures—if proper IG controls and monitoring are not in place. To wit: Granting remote access to confidential information assets for key personnel is common. Granting medical leave is also common. But a deceptive and dishonest employee could feign a medical leave while downloading volumes of confidential information assets for a competitor—and that is exactly what happened at Accenture, a global consulting firm. During a fraudulent medical leave, an employee was allowed access to Accenture's Knowledge Exchange (KX), a detailed knowledge base containing previous proposals, expert reports, cost-estimating guidelines, and case studies. This activity could have been prevented by monitoring and analytics that would have shown an inordinate amount of downloads—especially for an "ailing" employee. The employee then went to work for a direct competitor and continued to download the confidential information from Accenture, estimated to be as many as 1,000 critical documents. While the online access to KX was secure, the use of the electronic documents could have been restricted even *after* the documents were downloaded, if IG measures were in place and newer technologies (such as information rights management [IRM] software) were deployed to secure them directly and maintain that security remotely. With IRM, software security protections can be employed to seal the e-documents and control their use—even after they leave the organization. More details on IRM technology and its capabilities is presented later in this book.

Other recent high-profile data and document leakage cases revealing information security weaknesses that could have been prevented by a robust IG program include:

- Huawei Technologies, the largest networking and mobile communications company in China, was sued by U.S.-based Motorola for allegedly conspiring to steal trade secrets through former Motorola employees.

> Ford's loss from stolen documents in a single case of intellectual property (IP) theft was estimated at $50 to $100 million.

- MI6, the U.K. equivalent of the U.S. Central Intelligence Agency, learned that one of its agents in military intelligence attempted to sell confidential documents to the intelligence services of the Netherlands for £2 million GBP ($3 million USD).

And breaches of personal information revealing failures in privacy protection abound; here are just a few:

- Health information of 1,600 cardiology patients at Texas Children's Hospital was compromised when a doctor's laptop was stolen. The information included personal and demographic information about the patients, including their names, dates of birth, diagnoses, and treatment histories.[27]
- U.K. medics lost the personal records of nearly 12,000 National Health Service patients in just eight months. Also, a hospital worker was suspended after it was discovered he had sent a file containing pay-slip details for every member of staff to his home e-mail account.[28]
- Personal information about more than 600 patients of the Fraser Health Authority in British Columbia, Canada, was stored on a laptop stolen from Burnaby General Hospital.
- In December 2013, Target stores in the U.S. reported that as many as 110 million customer records had been breached in a massive attack that lasted weeks.

The list of breaches and IG failures could go on and on, more than filling the pages of this book. It is clear that it is occurring and that it will continue. *IG controls to safeguard confidential information assets and protect privacy cannot rely solely on the trustworthiness of employees and basic security measures.* Up-to-date IG policies and enforcement efforts and newer technology sets are needed, with active, consistent monitoring and program adjustments to continue to improve.

Executives and senior managers can no longer avoid the issue, as it is abundantly clear that the threat is real and the costs of taking such avoidable risks can be high. A single security breach is an IG failure and can cost the entire business. According to Debra Logan of Gartner, "When organizations suffer high-profile data losses, especially involving violations of the privacy of citizens or consumers, they suffer serious reputational damage and often incur fines or other sanctions. IT leaders will have to take at least part of the blame for these incidents."[29]

Form IG Policies, Then Apply Technology for Enforcement

Typically, some policies governing the use and control of information and records may have been established for financial and compliance reports, and perhaps e-mail, but they are often incomplete and out-of-date and have not been adjusted for changes in the business environment, such as new technology platforms (e.g., Web 2.0, social

IG controls to safeguard confidential information assets and protect privacy cannot rely solely on the trustworthiness of employees and basic security measures.