COSMOS
Navigate the Compliance Universe

CEP Magazine - April 2021
Record management 101, Part 1: Consider these principles

By Jacki Cheslow, CCEP, CCEP-I, CRM

Jacki Cheslow (j.cheslow@ieee.org) is Global Compliance Program Leader for New York City-based The Institute of Electrical and Electronics Engineers, Incorporated.

The relationship between compliance and record and information management (RIM) is growing, and in some instances, RIM is being merged into compliance programs. So it is important for compliance professionals, at a minimum, to have an understanding of the basic tenets of RIM and the risks of poor RIM practices versus the benefits of good RIM practices. In this first part of a two-part series, we'll be exploring the importance of a well-designed RIM program and how you can assess your own program (or create one) accordingly.

A great starting point for those interested in learning more is ARMA International's Generally Accepted Recordkeeping Principles®[1] (Principles). ARMA International is a global association of record, information management, and information governance professionals focused on creating standards and guidelines for managing information and records throughout their life cycle. The Principles are designed to provide organizations with a standard of conduct for governing information and give compliance professionals the guidelines by which to judge (or base) their record and information programs on. We will look at them in more detail, but let's first take a moment to consider the scope of the RIM challenge most organizations are facing today.

A sea of information

Very recently, I came across this quote from Microsoft CEO Satya Nadella, who predicts that "50 billion devices will be connected by 2030" and notes that "90% of the data that we have today was created in the last two years."[2] That's a pretty astounding statement until you look at what's happening every day. Consider that as of July 2020, there were more than 4.8 billion internet users in the world; 18.1 million text messages were sent every minute last year. In 2019, 188 million emails were sent in the world every minute. Every 24 hours, 500 million tweets are published on Twitter. Every day, 2.5 quintillion bytes of data are created.[3] Just think about it: 2.5 quintillion bytes of data would fill 10 million Blu-ray discs and, when stacked, would equal the height of four Eiffel Towers.

When you consider some of these statistics, it is easy to recognize that organizations need to get control of their information before it gets out of control.

Consequences of bad record-keeping

Among this sea of information, bad record-keeping practices can lead to serious problems with a rippling effect. Often these bad habits go unnoticed until they result in large consequences. One example is of TAXA 4x35, a Danish taxi company that was audited by the Danish Data Protection Agency (DPA) in 2018.[4] Auditors found the taxi company had implemented a data retention policy but had failed to follow it. Consequently, the auditors reported that personal data relating to around 9 million individual taxi rides were being held beyond the lawful retention policy. The DPA recommended a penalty fine of DKK 1.2 million (roughly €160,000), noting that TAXA

4x35 held the data and did not delete them after they were no longer necessary. It is important to note that while the national data protection and supervisory authorities in most jurisdictions can issue fines by their own administrative competences, the DPA in Denmark must issue a police report, after which the police will investigate the claims and determine whether the claims constitute sufficient basis for pressing charges against the company in question. The penalty fine of up to DKK 1.2 million is ultimately determined and sentenced by the court. In October 2019, the recommendation was approved.

Then we have the case of utility company PG&E, perhaps the most horrific example of consequences for poor record-keeping. In 2010, a natural gas pipeline explosion in San Bruno, California, destroyed 58 homes and killed eight people. A National Transportation Safety Board report noted that PG&E's record-keeping played a major role in the explosion.[5] A 2019 investigative report in *The Wall Street Journal* alleges that in 2017, PG&E was responsible for "at least 17 major wildfires…[which] together scorched 193,743 acres in eight counties, destroyed 3,256 structures and killed 22 people."[6] It seems that PG&E knew they had a record-keeping issue, as a follow-up article noted: "PG&E has told state regulators it has struggled to consolidate data on the condition of its equipment," and Kevin Dasso, PG&E's vice president of asset management, said "the lack of comprehensive information made it difficult to determine which transmission lines were approaching the point of failure."[7]

This is an extreme example, and poor record-keeping did not start the fires, but in most of these instances, PG&E's record-keeping practices were cited in the causal analysis.

ARMA's Principles

Accountability

"A senior executive (or a person of comparable authority) shall oversee the information management to appropriate individuals."

Having a senior executive champion for the program will help to drive and, if necessary, force the change necessary to implement or reinforce your program. They are often better situated to assign responsibilities and hold others accountable than those responsible for RIM.

Transparency

"An organization's business processes and activities, including its information governance program, shall be documented in an open and verifiable manner, and that documentation shall be available to all personnel and appropriate, interested parties."

Sounds familiar, doesn't it? You need a well-constructed program that is documented, auditable, and repeatable. Your program should include regular review with appropriate approvals as needed.

Integrity

"An information governance program shall be constructed so the information assets generated by or managed for the organization have a reasonable guarantee of authenticity and reliability."

Integrity here refers to the integrity of your data and the internal controls surrounding it. This includes protecting your business records from inappropriate alteration or loss. The program should take into account the mechanisms and controls that surround data maintenance, migration and disposition, software maintenance and upgrades, etc.

Protection

"An information governance program shall be constructed to ensure an appropriate level of protection to information assets that are private, confidential, privileged, secret, classified, essential to business continuity, or that otherwise require protection."

Do you know what is collected, why, how it is used, where it is stored, and what happens when it is no longer needed? Do you understand the laws governing these data? Are the appropriate information security protocols in place? How confident are you in your business continuity and disaster recovery processes? Answering each of these questions puts you on the path to protecting your data.

Compliance

"An information governance program shall be constructed to comply with applicable laws, other binding authorities, and the organization's policies."

Does your program appropriately identify both internal and external requirements that affect your RIM program, and do your employees understand those responsibilities? Does everyone involved understand the implications of noncompliance?

Availability

"An organization shall maintain its information assets in a manner that ensures their timely, efficient, and accurate retrieval."

There's an expression common among RIM professionals: If you have a record and can't find it, then you don't actually have a record. Are your employees knowledgeable about the records and information they create and maintain? Do they understand the company's recordkeeping systems and how they work? Is there sufficient documentation surrounding those systems? Do you test your expectations versus reality?

Retention

"An organization shall maintain its information assets for an appropriate time, taking into account its legal, regulatory, fiscal, operational, and historical requirements."

Have you done the work to ensure that you have established appropriate retention periods? Do you have documentation to support the decisions that were made? How have the retention periods been implemented—for hard copy records or electronically stored data?

Disposition

"An organization shall provide secure and appropriate disposition for information assets no longer required to be maintained, in compliance with applicable laws and the organization's policies."

Disposition is not just about deleting data. Disposition refers to end-of-life decisions being made about records and information and may include long-term storage, archiving, or secure disposal. Long-term storage will include data that have a long but defined retention period. Archival data refer to historical or research data that an organization wants or needs to maintain. For both of these, the program should consider format and software. Is the media you're choosing appropriate for long-term or archival storage?

When it comes to disposal, it is important to keep in mind that simply deleting or overwriting data is never a

secure way of removing data. With simple recovery software, those files can be retrieved with little difficulty. Your procedures should include the appropriate methods of disposal for paper (transport, storage, and destruction); electronically stored information; and electronic equipment.

The tools available to you

There's a lot of similarity within the Principles to what we are already doing in compliance, so the synergies are there to bring RIM under the compliance umbrella. ARMA summarizes the Principles in an easy-to-remember acronym: A-T-I-P-C-A-R-D.

No organization does it all or does it perfect, but if you have an existing program and want to know where you stand, the Principles, as well as other industry standards, practices, and legal/regulatory requirements that surround records management, can help you get started.

Takeaways

- Compliance and record management go hand in hand.
- Once thought of as two separate and distinct disciplines, compliance and records management are coming together.
- Poor record-keeping practices can result in real-life consequences.
- As compliance professionals, at a minimum, we should understand the principles of record-keeping.
- ARMA International's Generally Accepted Recordkeeping Principles® provide a global standard and a high-level framework of good practices for records and information management programs.

1 Generally Accepted Recordkeeping Principles. © 2017 ARMA International, https://www.arma.org/page/principles.
2 Satya Nadella, "Microsoft Inspire 2019 Corenote with Satya Nadella," Microsoft Inspire, Las Vegas, July 22, 2019, https://bit.ly/395FJnA.
3 Branka Vuleta, "How Much Data Is Created Every Day? [27 Staggering Stats]," SeedScientific, January 30, 2020, http://bit.ly/2Y4sQ6N.
4 European Data Protection Board, "The Danish Data Protection Agency proposes a DKK 1,2 million fine for Danish taxi company," news release, March 25, 2019, http://bit.ly/39WSkZu.
5 California Public Utilities Commission, "CPUC Begins Penalty Consideration Regarding PG&E Gas Pipeline Recordkeeping," news release, February 24, 2011, https://bit.ly/2NsxYjc.
6 Russell Gold, Katherine Blunt, and Rebecca Smith, "PG&E Sparked at Least 1,500 California Fires. Now the Utility Faces Collapse." *The Wall Street Journal*, January 13, 2019, http://on.wsj.com/2McYMDl.
7 Katherine Blunt and Russell Gold, "PG&E Knew for Years Its Lines Could Spark Wildfires, and Didn't Fix Them," *The Wall Street Journal*, July 10, 2019, http://on.wsj.com/3sKQUtA.