ARMA

VOLUME 2
APR-JUN 2019

MAGAZINE.ARMA.ORG

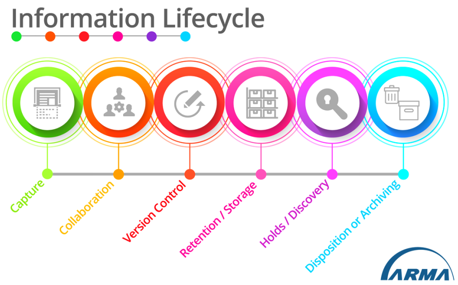
ARMA

CONTENTS

ALL ARTICLES

SPOTLIGHT

ARMA



Q&A

KM

MAGAZINE.ARMA.ORG

PUBLISHER & EDITOR IN CHIEF: NICK INGLIS, CIP, IGP, INFO | MANAGING EDITOR: JEFF WHITED | ADVERTISING ACCT MANAGER: JENNIFER MILLETT | EDITORIAL INQUIRIES: EDITOR@ARMAINTL.ORG | ADVERTISING INQUIRIES: JENNIFER.MILLETT@ARMAINTL.ORG | EDITORIAL BOARD: ALEXANDRA BRADLEY, CRM, FAI, HARWOOD INFORMATION ASSOCIATES LTD.; MARTI FISCHER, CRM, FAI, WELLS FARGO BANK; UTA FOX, CRM, FAI, CALGARY POLICE SERVICE; SOO KANG, IGP, CIPP/US, ZASIO ENTERPRISES, INC.; MADELEINE LA COUR, IGP, BAKER BOTTS LLP; PAUL LANOIS, CIPP/A, CIPP/C, CIPP/E, CIPP/US, CIPM, CIPT, FIP, CCSK, CIP, PCIP, CREDIT SUISSE; WILLIAM W. LEFEVRE, CRM, CA, FCA US LLC; BOB PRIDE, FERGUSON ENTERPRISES, INC.; STUART RENNIE, STUART RENNIE CONSULTING; JUDY VASEK SITTON, CRM, FAI, KINDER MORGAN; SHEILA TAYLOR, IGP, CRM, ERGO INFORMATION MANAGEMENT CONSULTING; MEHRAN VAHEDI, THE COCA-COLA COMPANY.

INFORMATION MANAGEMENT (ISSN 1535-2897) IS PUBLISHED QUARTERLY BY ARMA INTERNATIONAL. EXECUTIVE, EDITORIAL, AND ADVERTISING OFFICES ARE LOCATED AT 11880 COLLEGE BLVD., SUITE 450,
OVERLAND PARK, KS 66210. ARMA INTERNATIONAL (WWW.ARMA.ORG) IS A NOT-FOR-PROFIT PROFESSIONAL ASSOCIATION AND THE AUTHORITY ON GOVERNING INFORMATION AS A STRATEGIC ASSET.

MAGAZINE.ARMA.ORG WELCOMES EDITORIAL SUBMISSIONS. WE RESERVE THE RIGHT TO EDIT SUBMISSIONS FOR GRAMMAR, LENGTH, AND CLARITY. FOR SUBMISSION PROCEDURES, PLEASE SEE THE "AUTHOR GUIDELINES" AT HTTP://MAGAZINE.ARMA.ORG/BECOME-AN-AUTHOR.

OPINIONS AND SUGGESTIONS OF THE WRITERS AND AUTHORS OF ARTICLES IN MAGAZINE.ARMA.ORG DO NOT NECESSARILY REFLECT THE OPINION OR POLICY OF ARMA INTERNATIONAL.
ACCEPTANCE OF ADVERTISING IS FOR THE BENEFIT AND INFORMATION OF THE MEMBERSHIP AND READERS, BUT IT DOES NOT CONSTITUTE OFFICIAL ENDORSEMENT BY ARMA INTERNATIONAL OF THE PRODUCT OR SERVICE ADVERTISED.

HOW TO BREAK THE MOLD OF NEGATIVITY AROUND IM POLICIES

LEWIS EISEN

Most people associate IM policies with notions like requirements and restrictions. Those connotations are unfortunate because that's not what writing rules is about.

Written properly, rules are primarily about getting clarity and about target setting. No matter what the field — IM, IT, Security — rules are about helping people do the right thing.

The negative connotations are understandable, though, given the tone of voice of many policy documents.

Often organizations claim to hold “respect for others” as a core value, but when you look at their rules documents, the story is different. Whether they’re called “policies,” “standards,” or simply “guidelines,” many of these rules sound as if they were written by angry parents scolding naughty children. Getting buy-in under those conditions is an uphill battle.

Compare the following policy statements:

A) ”Corporate documents must be stored in the official repositories and MUST NEVER be stored on personal storage devices.”

B) ”Corporate documents are stored exclusively in official repositories.”

These statements clearly convey the same message: we want people to store their documents in one place and not another. So why is Statement A so much longer?

Reading between the lines of Statement A, we can detect some subtle but clearly perceptible undertones. The business evidently suffers from a problem: people have not been respecting the rule until now. Moreover, it seems that the IM specialists are frustrated with that situation.

Statement B is gentler. The requirement is still strict, yet it’s expressed in a helpful rather than reproachful manner.

The person who wrote Statement A wanted to address the issue directly, but that wasn’t considered sufficient. Clearly, someone at this organization believes that employees need to be shouted at before things will improve.

In fact, compliance is more likely in an organization when the rules sound positive and helpful. After all, your policies are a reflection of your corporate culture. A policy suite full of “must,” “should,” and “no exceptions” statements is a clear indication that the organization lives under a command-and-control management style rather than a collaborative, teamwork approach.

Moreover, negatively worded statements unintentionally reveal your weaknesses to your employees and customers—both current and prospective. Seriously, does everybody really have to know that some employees have not been complying? The admonishment in the second part of Statement A is a gratuitous appendage to what can be a simply worded rule.

Most policy writers tell me that Statement A does not reflect their own communication style. They don't talk to people in that tone of voice. It's not who they are, and it's not how they want to come across. They're using harsh wording in written policies for historical reasons.

But it's not justifiable. The strictest rules in any country, in fact, are the criminal laws — the rules against murder, assault, kidnapping... you know, the really rotten stuff. The precise wording of those rules varies from jurisdiction to jurisdiction, but the tone of voice is always the same: it's a simple declarative sentence. Something along the lines of this: "A person who commits murder is guilty of a felony."

There is no shouting, no finger wagging, no "we know best" parent-child dynamic. It's a simple, respectful statement.

So the reality is that we have a situation where the strictest laws for the most heinous crimes in the country are worded more respectfully than the policies that come out of most organizations.

Ponder that for a moment. Do the people who promote Statement A really believe that murdering your boss is less serious an offense than storing corporate documents on personal devices?

It is possible to break the mold. Think of the policy statements you write not as limitations or threats, but as targets and recipes for success. Most people in an organization truly want to do things right. The job of the policy writer is to specify what that means in a manner that's clear, succinct, and respectful.

Well-written policies are positive and helpful.

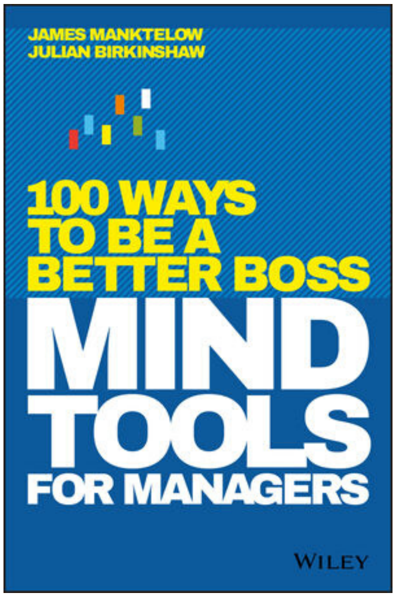
about the author

Lewis Eisen

Lewis S Eisen, B.A., J.D., C.I.P. combines several years practicing law with 15 years of business consulting and 16 years experience in Information Management in the Government of Canada. He speaks at venues across the United States and Canada and is the author of the book 'How to Write Rules that People Want to Follow: A Guide to Respectful Policies and Directives'.

Mind Tools for Managers: A Crash Course in Effective Management Skills

Charity Whan



JAMES MANKTELOW
JULIAN BIRKINSHAW

100 WAYS TO BE A BETTER BOSS

MIND TOOLS FOR MANAGERS

WILEY

TITLE: MIND TOOLS FOR MANAGERS – 100 WAYS TO BE A BETTER BOSS
AUTHOR: JAMES MANKTELOW & JULIAN BIRKINSHAW
PUBLISHER: HOBOKEN – WILEY, 2018
ISBN 9781119374404 (PDF)
ISBN 9781119374374 (EPUB)
ISBN 9781119374473 (HARDBACK)
PRICE: $28.00
SOURCE: HTTPS://WWW.WILEY.COM/EN-US/MIND+TOOLS+FOR+MANAGERS%3A+100+WAYS+TO+BE+A+BETTER+BOSS-P-9781119374374

Mind Tools for Managers: 100 Ways to Be a Better Boss focuses on identifying the complete list of skills that managers can master to be better leaders in their organizations. The authors provide working professionals with practical advice for these competencies – such as the ability to adequately cope with change and stress – and they direct their readers to an accompanying website where they can access such external resources as videos, skill-building articles, and worksheets.

Key topics from this skill overview include:

- Understanding personalities and managing them accordingly
- Prioritizing tasks and finding more time in the day by eliminating low-yield activities
- Finding a work-life balance that works best for both the manager and employees
- Translating the organization's mission into goals that people will easily understand
- Systematically getting to the root of a problem through Root Cause Analysis
- Understanding how to motivate people, including motivating those from different generations
- Resolving conflict, as well as dealing with office politics and protecting teams from it
- Working effectively with customers and external stakeholders

The authors of Mind Tools for Managers bring together a lengthy background in career research and development, with a sustained history of solid research methodology. Utilizing a survey of more than 15,000 managers and professionals worldwide, the authors actually identify a grand total of 100 skills they deem necessary to be successful in today's average organization.

Crash Course in Management Skills

Mind Tools for Managers can certainly be a resource to leaders as they work on developing the kinds of abilities they may need to be a better boss on the job. As a single volume resource, it is an easy-to-use toolkit for managers looking to improve their skill set. Each chapter contains a similar grouping of skills, such as those related to fostering creativity and innovation, and the external references as mentioned above are listed throughout the chapters where appropriate.

However, it's probably telling of our current work culture that it's even necessary to suggest that it requires 100 different skills for any manager to be successful. Obviously, it's likely not possible that any one manager could ever use all 100 skills at the same time. It would take years for one person to even encounter all the various scenarios listed in this book. Considering this, readers can look at Mind Tools as a sort of crash course – a range of thoughts, ideas, and inspirations – that would be helpful at various points in a career.

The Challenge of 'Mind Tools'

Group President Mads Nipper of Grundfos A/S provides praise on the book's cover, stating that "many books on management suffer from the 'Silver bullet' syndrome, focusing on one important technique as the solution to all our management problems." She says that Mind Tools stands in stark contrast as a book that dares to approach mastering the "many, many disciplines" it takes to be a good boss. While I do not technically disagree with that statement, I do believe authors can go too far in their attempts at comprehensiveness.

At several times, the reader is left wanting a little more detail and specific examples about how these skills might be applied. But it's really no wonder, what with 100 individual ideas to cover,that the authors may have felt the need to keep their overview as brief as possible. This book has just over 240 pages, so it could be argued that a second volume might have been prudent, allowing the authors to flesh out the more important topics.

Further, it would have been particularly helpful if the authors had provided actual case studies or examples of how these skills were successfully implemented in real-life scenarios. Overall, however, Mind Tools for Managers is a useful book with its multitude of tips, best practices, and links to practical resources. It would certainly be considered a worthwhile read for all managers across a variety of industries, new and experienced alike.

about the author

Charity Whan

Charity Whan is a case administrator for the U.S. District Court, Southern District of California. She can be reached at Charity_Whan@casd.uscourts.gov.

ESTABLISHING A COLLABORATION PROCESS TO BOLSTER KNOWLEDGE MANAGEMENT

STAN GARFIELD

Collaboration: interacting with peers and colleagues to exchange ideas, share experiences, work together on projects, and solve problems.

Work teams, project teams, and communities need a consistent way to share their knowledge, coordinate their activities, and communicate with one another. Providing a process for collaboration enables basic functions such as document and photo libraries, file sharing, membership rosters, lists, discussions, polls and surveys, calendars, meeting sites, and links. Making this process a standard ensures that there is a consistent way to collaborate so that once a user has learned how to do so, it will always be the same.

A standard collaboration process ensures a predictable, reliable, backed-up, and supported environment, which is preferable to ad hoc methods such as email, shared drives, personal hard drives, or unsupported tools. The process should allow a team to continue collaborating without losing information even if one or more of the members departs, a computer is lost or stolen, or a hard drive fails.

Without a standard process, collaboration will be done in a variety of sub-optimal ways, or not at all. Thus, it is desirable to define a policy which requires the collaboration process to be followed by all teams. Supporting the policy should be a standard tool for collaboration with a self-service creation process which is very easy to use. Until collaboration becomes ingrained, make it one of the three goals for knowledge management for all employees for whom it is relevant. For example, “For every customer project, a team space using the standard collaboration tool should be created for project team collaboration.” Then report each month on progress to achieving the goal.

The combination of a quick self-service creation process for team spaces, the ease of use of the chosen collaboration tool, and an employee goal should lead to rapid and widespread adoption. As a result, you should be able to declare success and replace the collaboration goal with a different goal for the subsequent year.

A collaboration process should include policy, procedure, a standard tool, and standard templates for different types of teams, training, and support. These should be supplemented with a capture process that allows reusable content to be selected from team spaces and submitted to appropriate repositories for later reuse. It’s also helpful to provide guidelines for how to collaborate, including effective ways to ask others for help.

Providing a standard, supported way for teams to collaborate is an essential enabler of knowledge management. It allows knowledge to flow between people, creates an environment where documents and ideas can be shared, and provides supporting tools such as polls that make it easy to find out what team members are thinking.

Suggested Steps

1. Implement a collaboration process for project teams.
2. Define and enforce a collaboration policy for how teams are to collaborate.
3. Discourage team collaboration from taking place outside the team space. For example, project team members should not maintain any files on other sites or rely on email or non-standard collaboration tools.

An Example

At HP, we wanted to establish that collaboration was expected to occur, and in a standard way. Before there was such a standard, people were collaborating informally, sending email to one other, or storing documents on someone's hard drive. The problem was that if someone left the project team, others wanting to find out what had been shared might not be able to access it. Without a standard way to collaborate, you won't get the kind of collaboration you want—or it will happen inconsistently.

Just requiring team collaboration is not enough. You have to make it easy for people to create a collaboration space. At HP, we used Microsoft SharePoint team sites, which allowed us to emphasize self-service—anyone could create and begin using their team site in just a few minutes. What helped things take off was that we provided a template and allowed users to populate it with standard information and links that a project typically needed. One of HP's three original KM goals was that every project should establish a project space. But we no longer needed that as an explicit goal because everybody had started doing it routinely.

It is important to identify the business requirements that collaboration addresses. At HP, it was the need for project teams to work together, to communicate effectively, and to have shared access to documents. We created a standard environment that didn't require people to learn multiple tools or prevent them from reusing materials across projects. The self-service element was important—people didn't have to wait for the IT department to create sites for them.

The collaboration process spanned four stages in the project life cycle:

1. In the initial phase, someone began pursuing an opportunity. They started a collaborative team space for the team going after the deal.
2. They began including people from the sales force and from services, or anyone within the company working on that deal who needed to collaborate.
3. As the project moved along, new project team members might be added, and the project manager might get assigned to work on another deal. Teams needed a way for things to be handed off from the sales part of the opportunity to the delivery part of it. The team space offered a way for handoffs to happen—to prevent information from being lost, and to ensure critical materials (e.g., proposals and project plans) were widely reusable.
4. Finally, these documents could be shared from the team space into the project document library, where others could access and reuse them. A standard workflow process moved documents from the team space into the project document library.

about the author

Stan Garfield

Experienced knowledge management practitioner, communities of practice evangelist, and social business leader. Garfield's resume includes some of the top names in the information space including HP, Deloitte, and PricewaterhouseCoopers. Learn more and connect with Stan at https://sites.google.com/site/stangarfield/.

Attorneys Respond to Delaware Court’s Affirmation That Emails and Texts May Constitute Corporate Books and Records

In reporting on recent actions in the Delaware courts, WilmerHale attorneys Stephanie C. Evans and Alan J. Wilson remind organizations to carefully manage all evidence of communications among boards and directors, whether it comes in traditional formats or through less formal media.

Writing for Mondaq, the attorneys note that several court actions this year in Delaware have clarified the scope of the Delaware General Corporation Law, Section 220, which gives stockholders and directors the right to demand access to an organization's books and records "where a proper purpose can be demonstrated." Importantly, the courts have affirmed that emails, text messages, and other less formal communications may constitute books and records of a corporation.

Attorneys Evans and Wilson write that these opinions "illustrate how Delaware courts interpret 'books and records' flexibly under Section 220 to keep pace with evolving record-keeping and communication practices."

The court has noted that a company that documents its actions through more traditional means, such as minutes, resolutions, and official letters, will likely have no problem satisfying an appropriate Section 220 request, and warned that companies cannot choose an electronic communication medium with the idea of keeping "shareholders in the dark about substantive information to which [Section] 220 entitles them."

Additionally, the Delaware courts have signaled they may in certain instances – on a case-by-case basis – request to review the devices that hold such "personal" communications.

Evans and Wilson of WilmerHale advise directors, corporate secretaries, and company counsel to "be mindful of good corporate housekeeping practices involving the maintenance of corporate books and records." Further, they advise such entities to always keep documentation of board actions in formal meeting minutes and written consents; to make sure these formal records are "sufficiently robust" so that directors or stockholders don't feel the need to seek less formal communications; and to educate everyone about the risks of using less-formal communications and personal accounts or devices when discussing business.

MAPPING DOCUMENT MANAGEMENT PROCESSES

(LEVERAGING AN INFORMATION LIFECYCLE)

The following is an excerpt from an ARMA White Paper "Reviving Document Management: How the Knowledge and Experience of Document Management Can be Leveraged for Organizational Improvement", sponsored by Access.

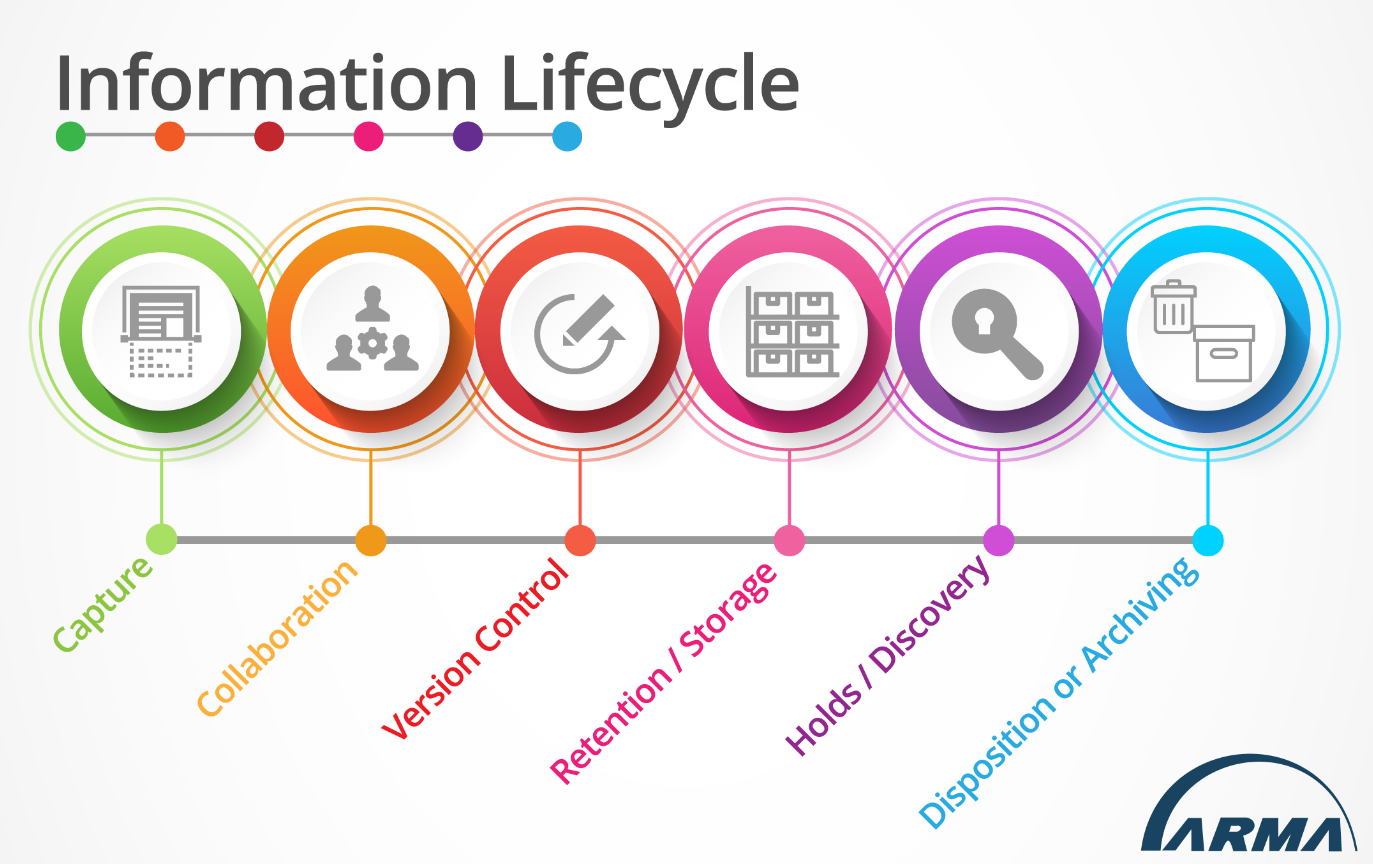
Processes around documents must mirror the processes around all organizational information. A consistent lifecycle for all information in an organization must be applied, with room for the unique nuances of document management to assert themselves. For this consistency across systems and classes of information (including documents), one should leverage an information lifecycle model.

All organizational information has both a point of creation and an end-point of disposal (or that information is moved into archives – think of founding documents and historical artifacts of an organization).

While the point of creation may be different in document management (a scanning process or integration with another information system through integration), it's essential to align the lifecycle mapping with other organizational information systems.

ARMA defines an information lifecycle graphically with the image on the following page.

All organizational information, documents or otherwise, must have a creation point (we'll discuss this in a moment). The information is then usable by the organization through its collaboration phase. When a piece of information is changed or edited, we should be employing version control to ensure the potential restoration of any accidental changes, and we maintain any prior versions required for records purposes. Information, or in this

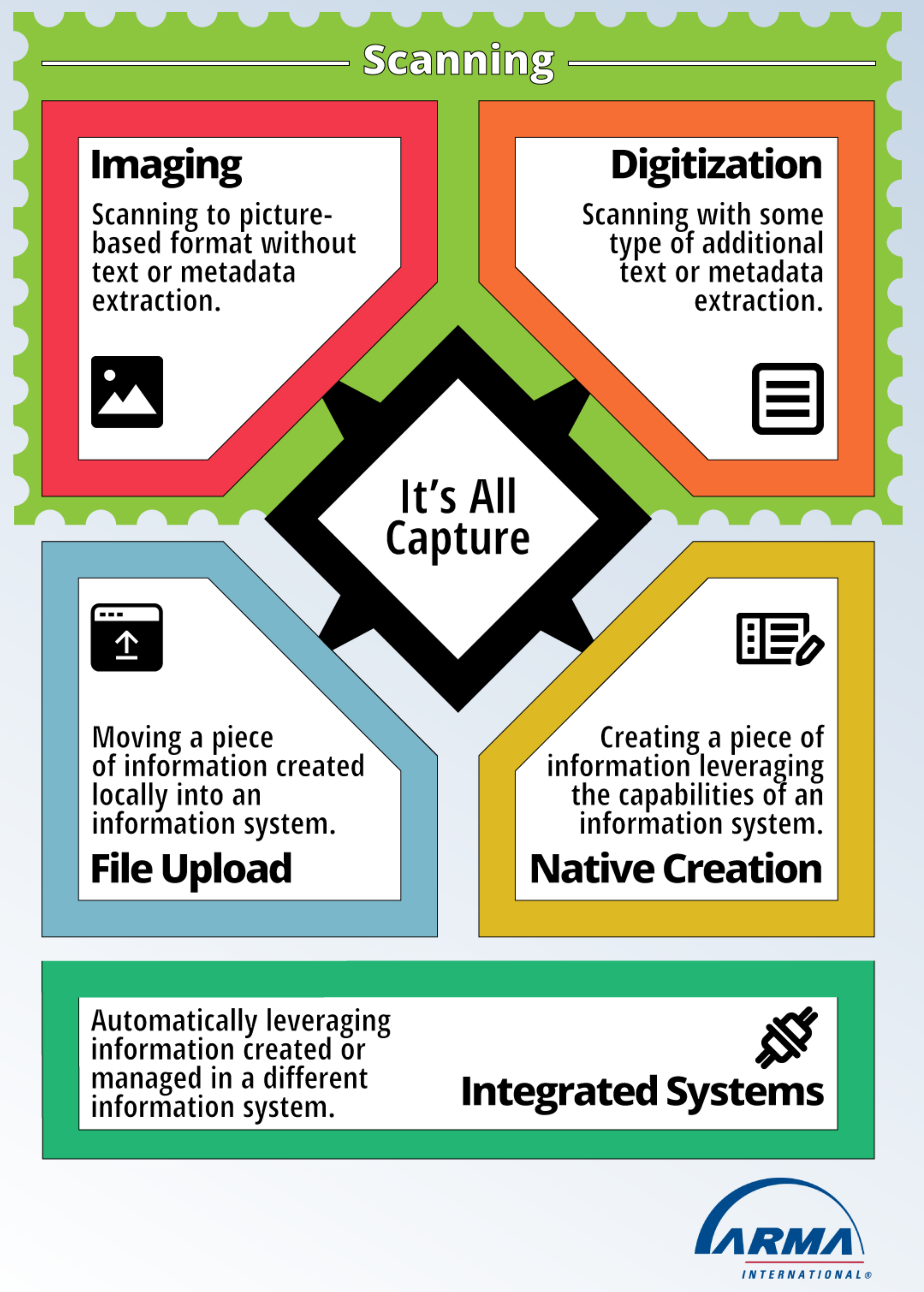


case documents, should be retained or stored for the required lengths of time for external regulations and compliance purposes, but also for the length of time that they remain useful for the organization (whichever is longer). We should, in most organizations, be able to apply holds or eDiscovery processes whenever there is related litigation – holds and processes that ensure that relevant information isn't deleted or disposed of during the course of any form of litigation. At the end of the lifecycle, the information should be disposed according to pre-defined disposition processes and/or sent to archives.

For document management, the information lifecycle generally starts with scanning or system integration (see image on the following page). System integration generally moves the intake of documents closer to their origination and may create documents out of other form-based processes. Scanning (either imaging or digitization) is a type of capture (a broader term that also includes file upload and native file creation).

Scanning processes in most organizations have matured from imaging (simple scanning of paper documents into picture-based formats like JPG, PNG, or TIFF) to digitization (scanning of paper documents that includes either metadata extraction or text recognition that converts the paper into a machine-readable format like DOC or PDF). If your organization is still employing basic scanning processes and hasn't yet matured to digitization processes, this is an area of potentially great benefits without a significant amount of effort.

Further, document management systems' metadata fields should align with organizational goals for metadata fields in other broader systems, such as ECM systems or IM systems. If an organization isn't undertaking an information governance-focused approach (more on that later), it is possible for the document management team to proactively leverage other systems' taxonomies and employ those within the document management system – leveraging a project management methodology for those changes.


Scanning
Imaging
Scanning to picture-based format without text or metadata extraction.
Digitization
Scanning with some type of additional text or metadata extraction.
It's All Capture
Moving a piece of information created locally into an information system.
File Upload
Creating a piece of information leveraging the capabilities of an information system.
Native Creation
Automatically leveraging information created or managed in a different information system.
Integrated Systems
ARMA INTERNATIONAL®

01 GDPR AFTER *ONE YEAR*

AS IT NEARS ITS FIRST ANNIVERSARY, THE GDPR GETS PREDICTABLY VARIED REVIEWS

LATER THIS MONTH, THE EU'S GENERAL DATA PROTECTION REGULATION (GDPR) WILL MARK ITS ONE-YEAR ANNIVERSARY, AND MULTIPLE NEWS OUTLETS ARE CHIMING IN WITH COMMENTARY ON THE IMPACT OF THE LANDMARK LAW.

Legaltechnews, for instance, reports on an IAPP Global Privacy Summit session in which a European data protection official and others reviewed the law's first year and forecasted what might come next.

Among her comments, Andrea Jelinek, the European Data Protection Board chair and Austrian Data Protection Authority director, noted how the law's implementation didn't halt the international interest in data privacy but seemed to heighten it, especially in the United States.

Jelinek voiced hope for a strong U.S. data protection law because of the breadth of impact that privacy scandals have had on American citizens. She suggested the United States establish an "enforcer to be taken seriously" by those who might infringe on any privacy rules. (The article goes on to say the U.S. Federal Trade Commission has only 40 staffers.)

Forbes.com this week published an article by Julian Vigo on how the tech culture and internet use have been affected by the GDPR. She writes that in addition to codifying data privacy laws across the EU, “a secondary ethos of the GDPR was to redress the imbalance of power between big tech and consumers, forcing big tech companies to be accountable for how they use data.”

The article stresses that many people and organizations “are still not clear about what the limits of GDPR compliance [are], what this means for their businesses and even how this has affected the larger tech culture where keywords like ‘consent’ and ‘transparency’ and ‘accountability’ are still largely just vague terms without a solid reference for most.”

Writer Vigo concludes her piece with what she sees as a bit of comical irony: “Almost a year into GDPR and the UK’s own Information Commissioner’s Office (ICO) staff haven't been handed a GDPR privacy notice which is both comic and indicative of the very complexities that the GDPR has impacted upon European tech culture.”

An Allen Bernard piece on SCMagazine.com goes deeply and quite thoughtfully into an evaluation of the GDPR “experiment.” Bernard speaks with several expert sources who give analysis on just about every angle of the law.

“The way companies are reacting varies depending on their exposure,” Bernard writes. He stresses that many are waiting to see how the GDPR fares in the courts; legal decisions could help them determine if the cost of complying is greater than the potential cost of sanctions.

Among its many key points, the article emphasizes that more laws are coming, citing the California privacy act and the possibility of a national U.S. law.

Bernard and a data privacy executive with Deloitte also discuss the four GDPR provisions that are problematic for many companies: right to erasure, right of access, right to data portability, and 72-hour notification.

Bernard takes his readers through the numerous challenges and uncertainties that are inherent in such uniform data privacy laws, but the readers are left with an optimistic note – that by complying with such laws, organizations are getting their information houses in order, which is a benefit across the board. Bernard writes: “The upsides to these efforts are many: a clear understanding where data resides, standardized privacy practices and awareness training across the company, and an enhanced reputation for integrity in the market.”

A PAIR OF FOUNDATIONAL CONCEPTS

Nick Inglis, CIP, IGP, INFO

(The following is an excerpt from the ARMA Guide to the Information Profession)

Words matter and word choices matter. In any profession that is looking to move forward in maturity, there are often vernacular issues that make gaining a comprehensive understanding of the profession a challenge. This is one of the reasons bodies of knowledge are so incredibly helpful: they help to clarify the vocabulary of a profession.

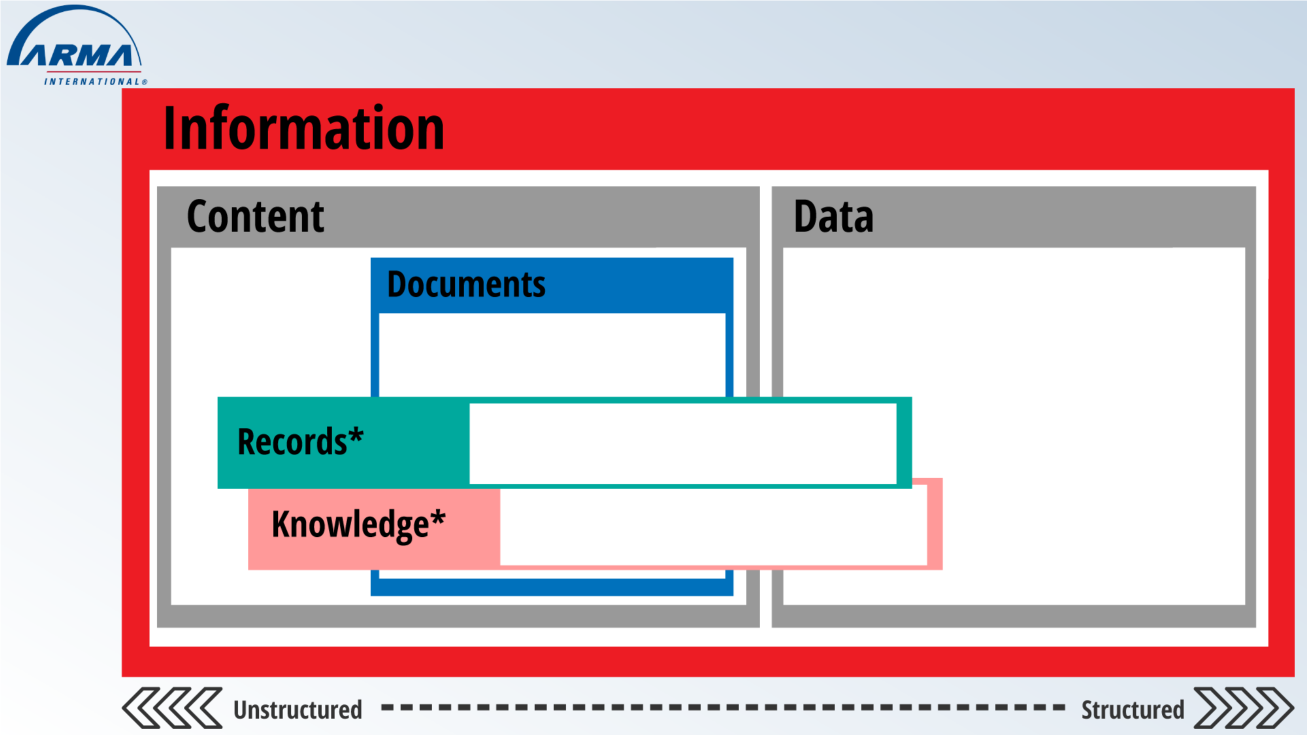
The information profession is filled with confusing terms, misused terms, and confusing acronyms. We revel in using words like "content" and "document" interchangeably (they're not interchangeable) and misunderstand the differences between "governance" and "management," all the while tossing around acronyms like ECM, BPM, ERM, IG, and EPR. Ok, I made up that last acronym, but if I didn't tell you that, you might not have been sure. So, you can see that the issues are numerous.

Content or Data or Document or Information or Knowledge or Record?

One of the biggest issues with the information profession is the misunderstanding and misuse of our information types: content, data, documents, knowledge, and records.

Each information type has a separate and distinct definition, and the terms are not interchangeable. Each type of information is, however, information. For example, all content is information but not all information is content. Confused yet? That's why these issues exist.

Without a proper understanding of these terms, we cannot have a shared vocabulary across the information profession - this is the most important barrier that we remove in this effort. We believe that the easiest way to understand the differences between these terms is visually:



Everything, whether unstructured or structured (or even semi-structured), is information. Content is unstructured information while data is structured (this is easiest to understand through the structure of a database). Data tends to be relational while content tends not to be.Documents are a type of content, semi-structured, through the use of a container (either paper or Word or PDF most commonly). Knowledge is a repurposable type of information that tends to include content more often than data. The goal of knowledge is for it to be shared between individuals within an organization (think of best practices resources). Records, like knowledge, can also be content or data and serve as evidence of a transaction or information that rises to the importance of being preserved.

Through this visual understanding, we know several things:

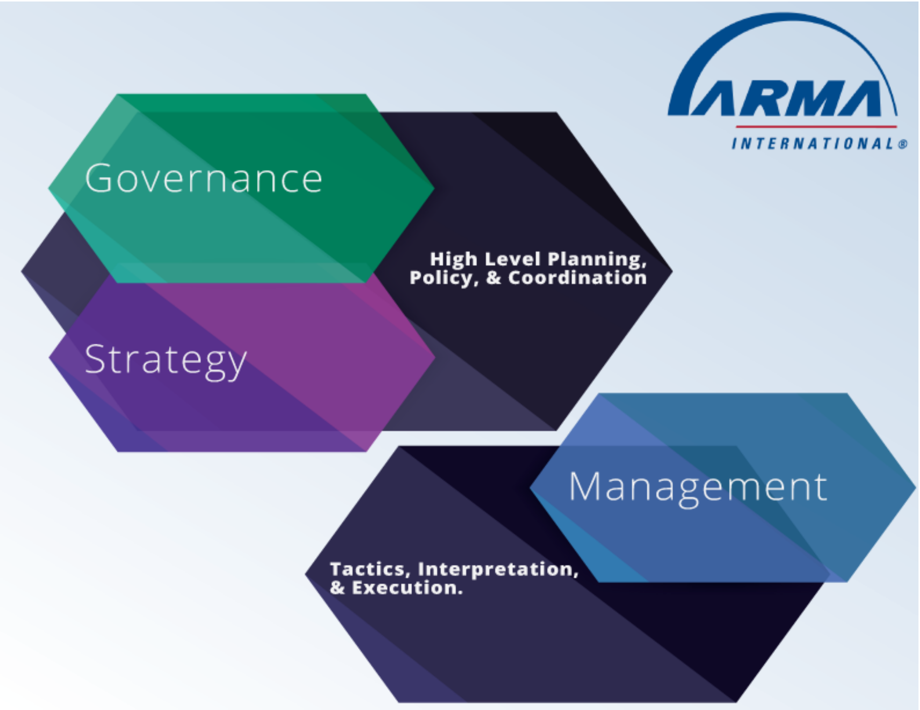
- Content is unstructured
- Documents are semi-structured
- Data is structured
- Knowledge can be found in any form
- Records can be found in any form
- All documents are content
- Not all content can be considered documents
- All documents are information
- Not all information is documents
- Content is not data
- Data is not content
- Everything is information

Governance, Strategy & Management

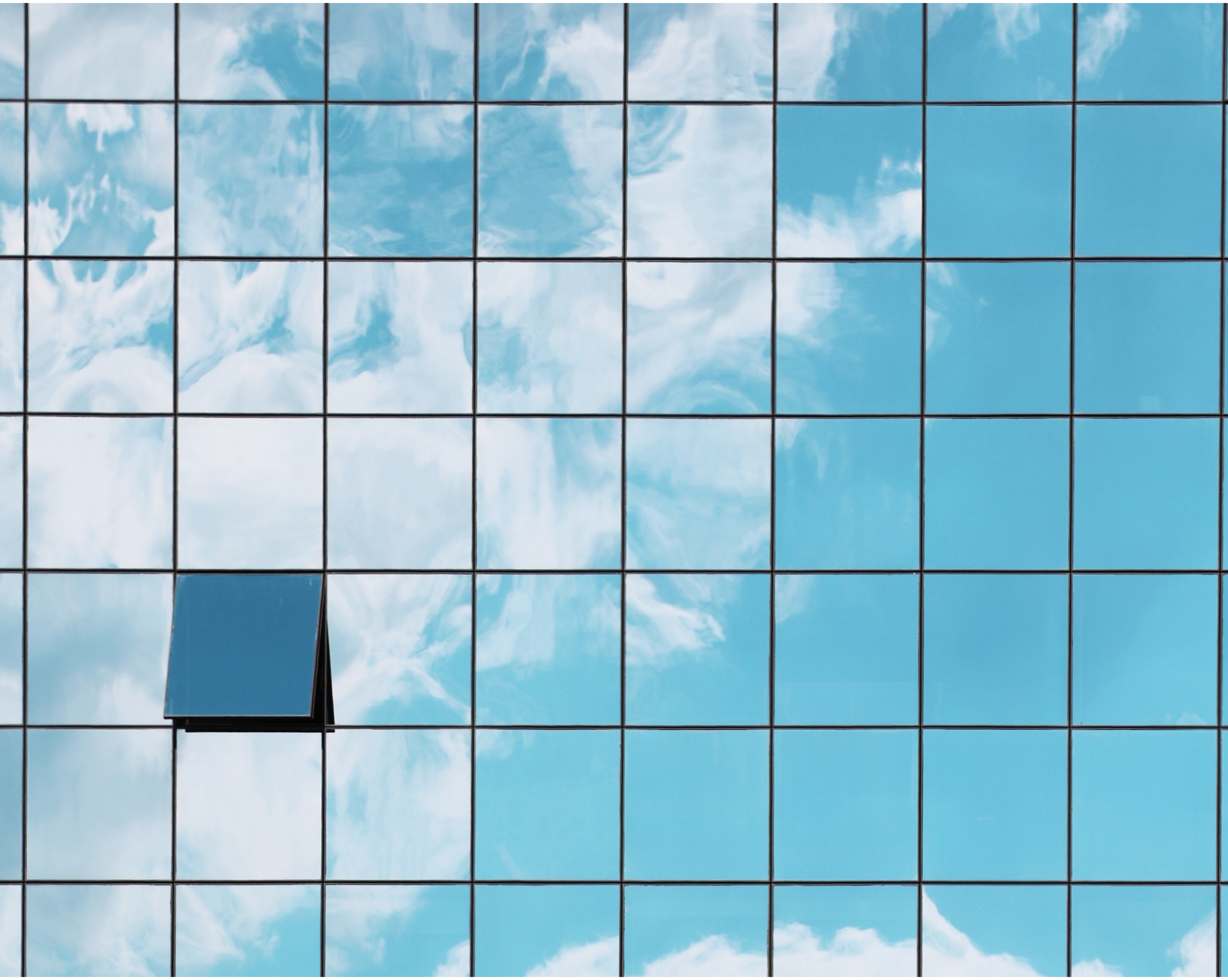
We use terms like “governance,” “strategy,” and “management” after the words content, data, document, information, knowledge, and record, but we frequently use these termsimproperly. For instance, records managers tend not to utilize a term such as “records governance” or “records strategy.” However, they likely should use these terms to describe the high-level planning, policy, and coordination that records managers do.

Governance and strategy are, for the information profession, interchangeable terms. For example, information governance and information strategy refer to the same work, whereas information management is different.

The terms “governance” or “strategy” should be used to describe high-level planning, policy, and coordination. Whereas the term “management” should be used to describe the tactical execution of said planning, policy, and coordination. The two sides must coexist.


ARMA INTERNATIONAL®
Governance
High Level Planning, Policy, & Coordination
Strategy
Management
Tactics, Interpretation, & Execution.

Presented here are two foundational concepts included in the ARMA Guide to the Information Profession (arma.org/arma-guide), available for free download. Additional foundational concepts include "Records Management in Flux," "Information Lifecycle," "Capture, Digitization, Imaging, Native Creation, Scanning, & Upload," "Information Assurance vs. Information Security," and "Backup, Business Continuity, Disaster Recovery, and Information Assurance."



Judge's Ruling May Provide Clues to the Outcome of Employee's 'Dropbox' Privacy Suit

Earlier this year, a judge from the Western District of Pennsylvania acted on behalf of employee privacy rights when she partially denied a public employer's motion to dismiss a suit that accused it of violating the plaintiff's Fourth Amendment rights.

As summarized on Mondaq.com, Elizabeth Frankhouser, an employee of an educational facility, used her personal Dropbox account to store personal and workplace data. Hence, a link to Dropbox was on her workplace screen, though no data contained in the account was on that device because Dropbox data is stored in the cloud. The account was password protected as well.

The employer allowed the use of that Dropbox account for work-related matters, which resulted in Frankhouser adding a mix of workplace content to her personal content, which included photos that "could be considered borderline explicit." An IT administrator was aware of a spreadsheet on the employee's device that included passwords, and he used it to access the Dropbox account. There, he came upon the "borderline" photos and forwarded them to higher authorities in the school district. Soon, the district forced Frankhouser to resign for storing inappropriate content on workplace computers, which violated the employer's policies, according to the Mondaq article.

"Not surprisingly," writes the article's authors, "Ms. Frankhouser filed a lawsuit alleging Fourth Amendment violations and invasion of privacy claims along with additional federal and state law claims."

The plaintiff claimed she had a reasonable expectation of privacy because she did not view or store the photographs on the workplace computer – Dropbox stores them in the cloud. In response, the defendants called for dismissal because Frankhouser didn't have an expectation of privacy because she often accessed the account at work; and she violated company policy by having the photos in her account.

Judge Kim R. Gibson sided with Frankhouser, citing the content was neither housed on nor accessed via the workplace computer or servers. In declining the request for dismissal, Gibson affirmed that Frankhouser had a reasonable expectation of privacy because the Dropbox account was her own account, was password protected, and was never used to access or download the photos while on the employer's system.

The authors (Ingrid A. Beattie, Cynthia J. Larose, and Jennifer R. Budoff) note that "while this case is in the early stages of litigation . . . this decision certainly raises considerations for employers to face." They suggest that workplace policies (which are rarely failsafe) include a statement that the employer has the right to monitor employees' emails and actions while using their devices; and that employers should prohibit the use of certain applications like Dropbox and anything cloud-based that might mingle personal and private data.

Goals of New Canadian Digital Charter Include Assuring Privacy, Eradicating Hate Online

Jeff Whited

Multiple news outlets are reporting on Canada's new digital charter, which comprises 10 principles that are based on Canadian values that should guide all future government policies, legislation, and programs.

When introducing the charter late last month, Navdeep Bains, minister of Innovation, Science, and Economic Development, emphasized that data will drive business in the new digital economy. But he also noted that privacy, security, and "trust" are fundamental priorities, suggesting that Canadians must be able to trust their information is being used properly.

Bains also said he'd work with the government to review and possibly reform PIPEDA, the Statistics Act, and the Privacy Act.

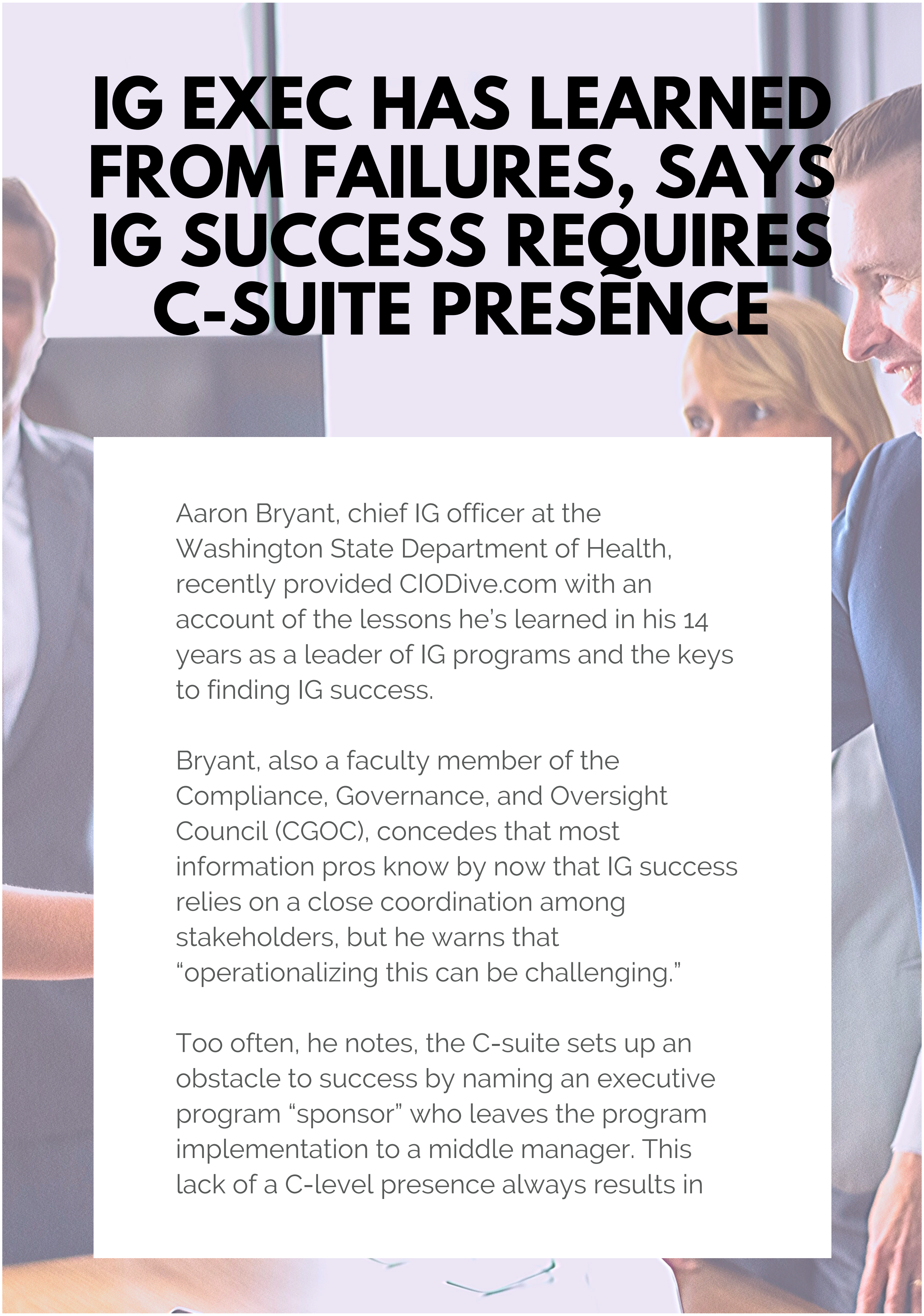
A pair of Canadian law firms are among those outlets that have covered the story; each provides a summary of the principles: the Bennett Jones blog and the McCarthy Tetrault blog.

Mack Lamoureux, writing for Vice.com, recently reported the new charter is designed to help thwart online extremism and disinformation. Prime Minister Justin Trudeau says Canada will respond in meaningful ways if tech companies fail to reign in misinformation on their platforms.

In a recent speech in Paris, at the Viva Technology conference, Trudeau spoke at length about the Christchurch, New Zealand, shooting, and said he was ready to work with the private sector to eradicate violent and terrorist content.

"The platforms are failing their users and they're failing our citizens," he said. "They have to step up in a major way to counter disinformation. If they don't, we will hold them to account and there will be meaningful financial consequences."

According to the Vice article, Facebook, Microsoft, Twitter, Google, and Amazon have all signed on to this Christchurch Call for Action. The U.S. government has so far decided against joining the effort.

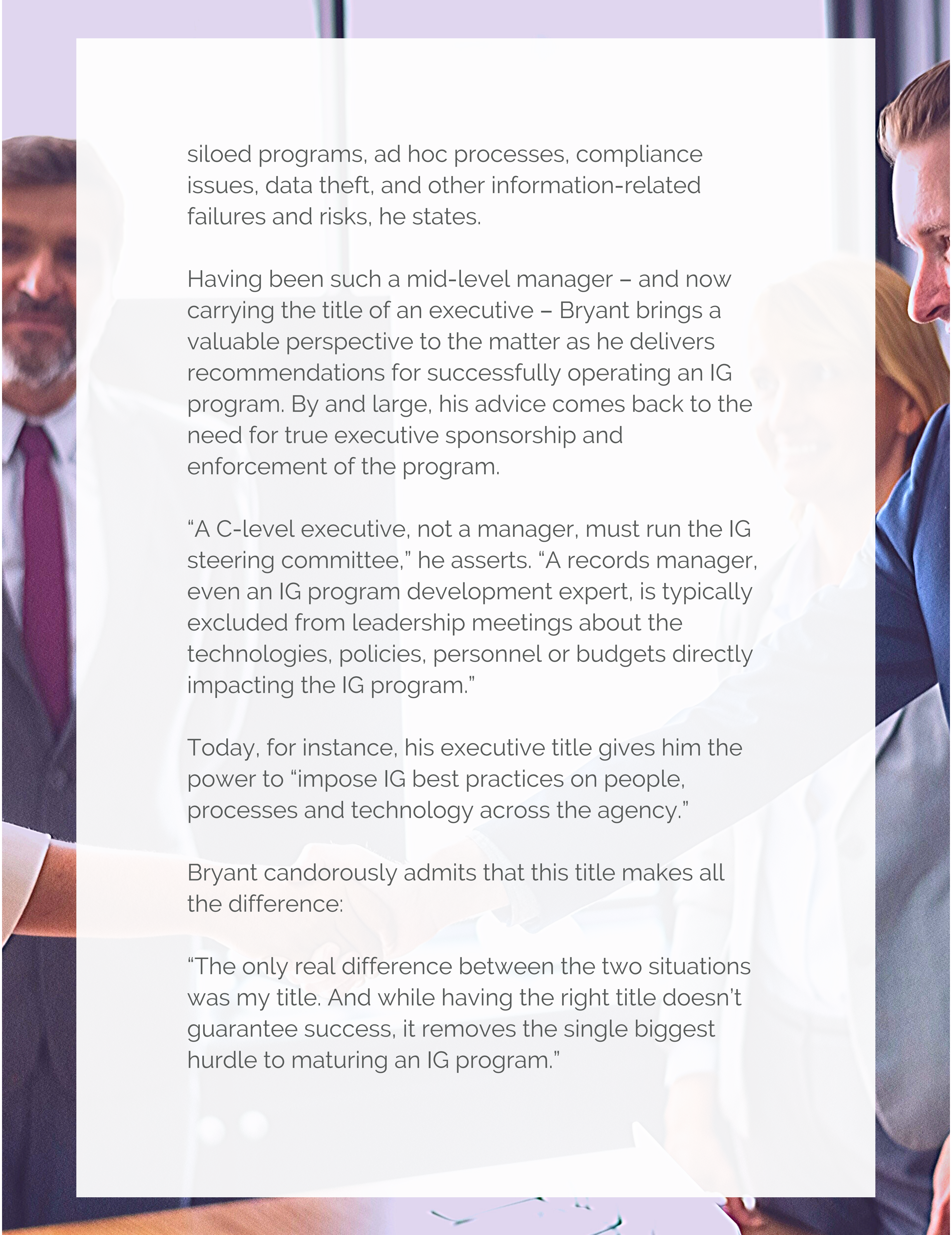


IG EXEC HAS LEARNED FROM FAILURES, SAYS IG SUCCESS REQUIRES C-SUITE PRESENCE

Aaron Bryant, chief IG officer at the Washington State Department of Health, recently provided CIODive.com with an account of the lessons he's learned in his 14 years as a leader of IG programs and the keys to finding IG success.

Bryant, also a faculty member of the Compliance, Governance, and Oversight Council (CGOC), concedes that most information pros know by now that IG success relies on a close coordination among stakeholders, but he warns that "operationalizing this can be challenging."

Too often, he notes, the C-suite sets up an obstacle to success by naming an executive program "sponsor" who leaves the program implementation to a middle manager. This lack of a C-level presence always results in



siloed programs, ad hoc processes, compliance issues, data theft, and other information-related failures and risks, he states.

Having been such a mid-level manager – and now carrying the title of an executive – Bryant brings a valuable perspective to the matter as he delivers recommendations for successfully operating an IG program. By and large, his advice comes back to the need for true executive sponsorship and enforcement of the program.

“A C-level executive, not a manager, must run the IG steering committee,” he asserts. “A records manager, even an IG program development expert, is typically excluded from leadership meetings about the technologies, policies, personnel or budgets directly impacting the IG program.”

Today, for instance, his executive title gives him the power to “impose IG best practices on people, processes and technology across the agency.”

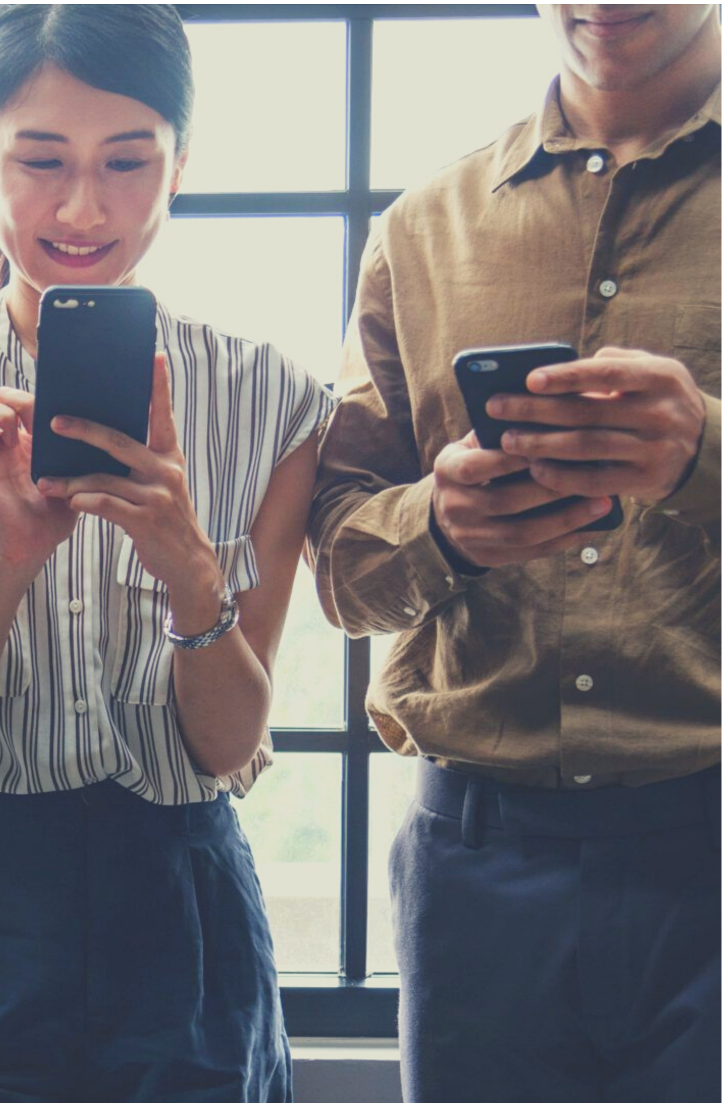
Bryant candorously admits that this title makes all the difference:

“The only real difference between the two situations was my title. And while having the right title doesn’t guarantee success, it removes the single biggest hurdle to maturing an IG program.”

ARMA Q&A

GDPR REGULATIONS AND ELECTRONIC RECORDS

"WHAT ARE THE GDPR REGULATIONS FOR PERSONAL DATA IN ELECTRONIC RECORDS SUCH AS SOCIAL MEDIA, VIDEO, AND INSTANT MESSAGES?"



Since May 28, 2018, the General Data Protection Regulation (EU) (2016/679) (GDPR) has been in force. The GDPR is not new; it is an updated replacement for the now repealed Data Protection Directive (1995/46/EC).

Article 3 of the GDPR states that it applies to the processing of personal data by a controller or a processor, whether inside or outside the European Union (EU). A controller is an organization or individual who processes personal data. For example, a controller could be a retailer with an online store that stores its customers' information. A processor is an organization or individual who processes personal data on behalf of the controller. A processor could also be a cloud service provider storing personal data for clients. Organizations located outside of the EU doing business in EU states could be subject to the GDPR if those organizations process personal data from an EU state.

The GDPR increases fines for noncompliance to a maximum 20 million EUR or 4% of the total annual worldwide turnover, whichever is higher.

Also, the GDPR is subject to whatever data protection legislation is passed by specific EU states.

Some find the GDPR to be long and complex and it is. But, at its heart, the GDPR operates on a basic principle: an organization can only work with the personal data of an individual if it is permitted by law or with the consent of that individual.

Article 5 of the GDPR requires that personal data be processed lawfully, fairly, and in a transparent manner. Further, Article 5 requires that personal data shall only be collected for specified, explicit, and legitimate purposes and not further processed in a way that is incompatible with those purposes.

Electronic records are not defined in the GDPR. However, electronic records, such as social media, video, and instant messages, come under the GDPR umbrella since they could be "personal data." Personal data is given a wide definition in Article 4. It means "any information relating to an identified or identifiable natural person." The focus in the GDPR is neither on the format of the record nor on the specific technology producing the record. Instead the focus is whether the record identifies a natural person. Examples of information in an electronic record that identify a natural person include a person's name, cell phone number, ID number, email address, and location data or online identifier, like an IP address or cookie.

What is new in the GDPR is that Article 5 applies the principle of accountability, in that the controller of personal data must ensure compliance with the GDPR and prove that compliance.

Whether they are controllers or processors of personal data, organizations can prove their compliance with the GDPR by maintaining records of their processing activities. Organizations can designate a data protection officer to ensure GDPR compliance. Organizations can conduct data protection impact assessments to identify and implement measures to mitigate risks to personal data protection.

about the author

Stuart Rennie

For the past 18 years, Stuart has been the Legislation and Law Reform Officer at the Canadian Bar Association, British Columbia Branch (CBABC). He provides consulting advice on proposed BC legislation, advises lawyers on BC statutes and regulations and provides policy and information governance advice.

WHY ARE BUSINESSES OPTING FOR EDGE, AI, AND IOT – AND ARE THEY WISE TO DO SO?

Jeff Whited

Edge computing is increasingly associated with at least two “trending” terms in the IT and information arenas: Internet of Things (IoT) and artificial intelligence (AI). Broadly speaking, the term refers to computing that’s done at or near the source of the data. Today, a great percentage of data is stored in the cloud and may therefore be located continents away. These great distances can result in delays in computing, which can impact an organization’s capacity to optimally analyze and leverage its data.

But edge computing tends to solve such latency problems, and this speed is largely what makes it one of the next big things. With similar speed, the topic is finding its way into the public domain.

Writing for InformationWeek.com, author Lisa Morgan submits that IT organizations should think about establishing edge gateways to support IoT devices, which are notorious for generating overwhelming quantities of data that are repetitive or lacking a useful context. Morgran writes that “The gateway analyzes data at the edge, sending the meaningful information . . . back to the enterprise.”

But she also quotes Arif Mustafa, a director at Info-Tech Research Group, who advises against assuming the data flow will necessarily be of a high quality, and who believes there can be data connectivity issues with other systems: “If you think about fragmentation of the devices and protocols and on top of it you have to integrate with legacy systems, connectivity becomes a challenge and it’s one of the biggest factors that should be taken into account,” he says.

Morgan’s article discusses associated business challenges that are all-too familiar, such as implementing these technologies before having a business strategy in place, for instance, and failing to consider the privacy and security requirements.

Said Mustafa: “When artificial intelligence and IoT merge, that makes security even more complicated."

Teradata’s Bob McQueen tells Morgan that data governance should not be backed into. “The strategy should be preplanned and incrementally developed as you develop your smart data management approach.”

An item on HelpNetSecurity.com summarizes an industry study that suggests edge computing is on the rise in IoT deployments. The study, conducted by Strategy Analytics, indicates that data will be processed via edge computing in nearly six of ten IoT deployments by 2025, a trend that’s driven by more efficient use of the network, by security concerns, and by response time.

Andrew Brown, a Strategy Analytics executive, says the trend makes sense for businesses because "Taking a more efficient and optimized approach in terms of what data is sent to the cloud, with reductions in traffic volumes, has positive net effects both on the security of the data being sent and the cost of sending data to the cloud."

SVP David Kerr of Strategy Analytics is careful to remind us of the challenges that remain, such as "immaturity of the current market and perceptions among customers that they have no need to change their current setup."

John Koon, writing for SensorMag.com, aligns with the popular belief that the boost in edge computing is driven largely by the shifting focus from "collecting massive data to meaningful use of analytics."

He provides a helpful illustration by suggesting that a smart thermostat may send its temperature readings every five seconds – useless, repetitive data that builds up fast and hogs the network bandwidth. "On the other hand," writes Koon, "a sudden change of temperature from ambient to 400 °F may indicate a fire or explosion nearby. Knowing when such a drastic change occurs constitutes 'meaningful use.'" And with edge computing, the cloud servers won't perform all of the processing, but sensors at the edge of the network will pitch in, thus resulting in quicker notification of such anomalies. "With edge computing, a smart thermostat will only send data to the cloud server if the readings exceed the temperature profile."

Koon takes a wholly optimistic view of the teaming of AI and edge computing, citing the value of smart sensors, in particular: "Coupled with smart sensors, the edge domain will take over local decision making. This is particularly useful in building smart cities, performing cybersecurity duties, and carrying out many of the automated functions."

As with any hot topic, information pros and governance stakeholders will continue to debate the benefits, risks, and challenges inherent in edge computing, a solution that might evolve too fast for definitive agreement on these benefits, risks, and challenges. For a fresh, detailed, and expert look at this and other cutting-edge topics, plan to attend ARMA InfoCon 2019 this October in Nashville. To see the schedule of events and sessions, visit arma.org/infocon – and check back often for updates.