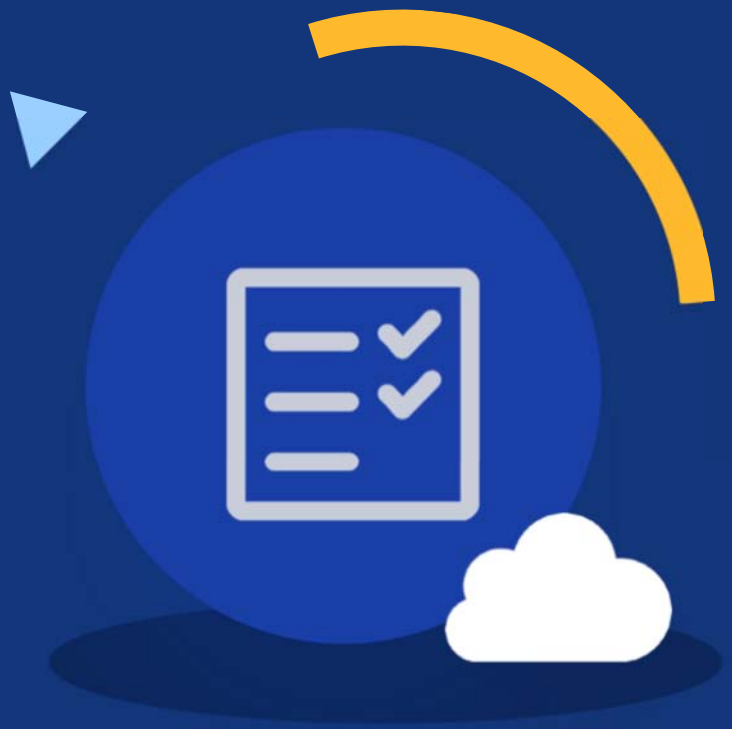
onna

E–BOOK:

Rethinking Information Governance

In the Age of Unstructured Enterprise Data



Contents

01.

Intro: Rethinking Information Governance

Information Governance:

A strategic framework to help businesses manage their information in a way that maximizes value and minimizes risk.

Overview

Information governance is defined in many ways, but at its core, it's a strategic framework to help organizations manage their information in a way that maximizes value and minimizes risk. From information's inception all the way to its archival and eventual disposal, its lifecycle can take many right and wrong turns and have real impacts on your business — which is why having a strong information governance program is crucial.

Yet, having a strong information governance program can look different for every organization. Depending on your size, industry regulations, use of on-prem or cloud-based tools, and other factors, you'll need to implement your own unique policies and procedures to match your goals. Regardless of these factors, the main elements of information governance that organizations care about largely remain the same. We're here to break down exactly what those elements are and reach beyond a one-size-fits-all strategy when it comes to security, privacy, compliance, and so much more.

About this eBook

In this eBook, we'll uncover how the concept of information governance has evolved over time, examine what we see as the most critical interdisciplinary elements of IG, address dynamics between information governance leaders and stakeholders, and develop a flexible, holistic approach for any organization that wants to advance their information governance efforts.

02.

The Evolution of Information Governance

Early Stages of Information Governance

Before the digitization of information, the sophisticated information governance frameworks we know today didn't exist.

Most enterprise information was governed through old-school records management, where businesses manually retrieved, archived, and disposed of documents. This job was typically done by a sole records manager focused on a single sector of the business like finance or HR. Outside of this narrow framework, there were no policies or procedures around the handling of internal information.

It was only when more complex information systems like computers, the internet, and email started to emerge that businesses began to rethink their processes. Not only did the nature of information itself become more complex, but its production increased at enormous rates across the business. The risks that came with these new technological developments forced teams to take a hard look at how their information was being managed. It soon became clear that traditional records management couldn't keep up, and there needed to be a more holistic approach to information. Thus, the concept of information governance was born.

The Formation of CGOC and IGPMM

We can't discuss the evolution of information governance without providing background on ARMA, the Association of Records Managers and Administrators – and CGOC, the Compliance, Governance and Oversight Counsel.

ARMA was formed in 1975 as first an educational resource for records management, but later expanded out to information management professionals across the globe. CGOC was established in 2004 to help organizations maintain more modern and robust information governance programs. Until their formation, there was virtually no thought leadership guiding organizations on information governance best practices. Over the last decade or so, CGOC and ARMA have grown to forums of thousands of legal, IT, records and information management professionals who conduct research and discuss challenging topics in discovery, analytics, privacy, governance and more.

CGOC, ARMA, and EDRM (a leader in the eDiscovery world) developed the first Information Governance Reference Model (IGRM) which aimed at boosting IG adoption by fostering collaboration between disparate but overlapping IG functions.[1] Later on, CGOC developed the Information Governance Process Maturity Model (IGPMM), which has become a standard framework in evaluating the maturity of IG programs. Since its creation, there's been a mass migration to cloud applications, adoption of AI and machine learning, and increasing data privacy regulations. Needless to say, today's enterprise information challenges are a bit more complex, leading to an update to the Maturity Model that reflects modern day challenges.

Click here to preview the latest IGPMM model.
Note: The full model is available via membership.

IG Today

The ability to work anytime, anywhere has skyrocketed productivity and afforded organizations a new level of convenience and efficiency. As a result, exponential amounts of enterprise information is being produced in multiple different apps, and the volume is only increasing. In fact, companies use 88 applications on average to power their workforce, a 21% increase from just three years ago.[2] And if that's not assuring enough, it's estimated that the global datasphere will grow to 175 ZB by 2025, with more data being stored in enterprises than all of the world's existing endpoints.[3]

Needless to say, today's organizations are faced with the overwhelming challenge of managing, finding, and leveraging their information. From privacy and compliance to security and eDiscovery, enterprise information is no longer something that merely needs to be stored. Today, it's a major part of our economy, a valuable knowledge asset, and many times, a significant liability. Similar to the digital revolution, we're in the midst of a powerful technological shift pushing us to seriously rethink information governance as a top priority.

On average, companies use 88 applications to power their workforce.

How should we think about information governance in the age of data overload?

- How will we manage information that's siloed in a hundred different places, across multiple sectors of the business?
- How will we promote IG leadership?
- How do we satisfy stakeholders with competing priorities?
- How will we keep up with new regulations, while making the right decisions when certain regulations don't yet exist?

These are the questions we'll answer in this eBook as we rethink information governance. It's our hope to help business leaders take advantage of this defining moment in time and understand why this discipline is perhaps the most critical part of their business' success in the years to come.

03.

The Elements of Information Governance

IG Elements

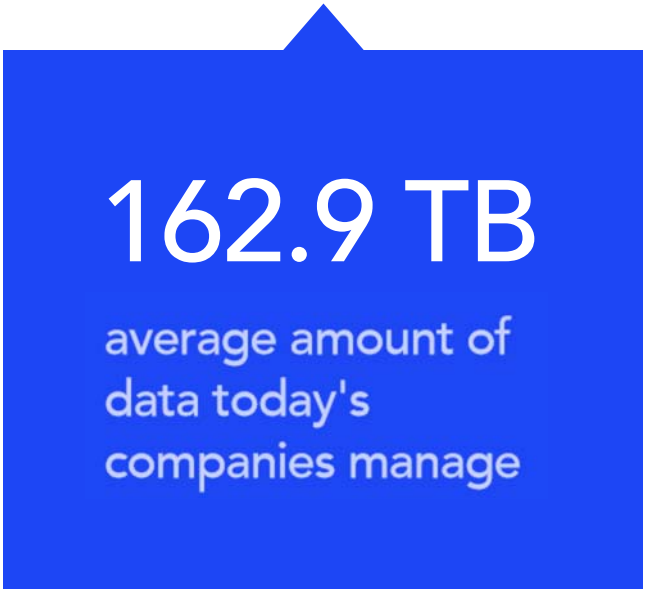
When hearing Information Governance, people tend to think of a lot of different things.

Information governance is viewed through a variety of lenses based on the viewer's background or role. Some view IG through an IT or security lens, where others see legal and compliance issues. The truth is, information governance is comprised of all of these elements. When prioritized correctly, these elements drive strong information governance programs. It's important to note that many elements are interdisciplinary and may vary depending on the company's size, industry, and level of maturity.

Information Security

Security is truly the foundation of a strong information governance program. Organizations house hundreds of thousands of sensitive records including business and consumer data — and to find or leverage any of it, you first need to first make sure it's protected. The average company manages 162.9TB of data — without robust security measures in place, that data becomes vulnerable to high-profile hacks and data breaches.[4]

Compromised enterprise data not only has hard-hitting legal implications, but also costs — the average total cost of a data breach ranges from $2.2 million for incidents with fewer than 10,000 compromised records to $6.9 million for incidents with more than 50,000 compromised records.[5] And at the rate enterprise data production is going, the latter seems more likely. Not only is it important to have strong security to prevent these attacks, but also to contain them if they do happen.



The 2019 IBM Cost of A Data Breach Report found that implementing a crisis response team can reduce the cost of a breach by as much as $14 per compromised record from the average per-capita cost of $148. Similarly, extensive use of encryption can cut the cost by $13 per capita.[6] It's also critical to have a spokesperson (like a CIO or CSO) to drive customer and employee trust initiatives after the breach.

Even if your business isn't at a CIO or CSO stage, having a data response plan and a head security engineer to reassure people can help mend damages.

Information Privacy

Not only should your information be secure, but it should only be accessed by the appropriate people. This is why security and privacy go hand in hand in when it comes to information governance. From the risk of data loss or misuse of confidential company IP to the growing pressures of GDPR and CCPA, prioritizing privacy in your information governance program is a must. Whether that means better defining the information lifecycle or following the Principle of Least Privilege for all of your user permissions, having a strong privacy culture minimizes risk and regulatory mishaps.

While it may be up to your IT team to get privacy measures in place, it ultimately takes company-wide cooperation to ensure they're actually working. It's a good idea to provide employee training and awareness activities, and strictly enforce and monitor policies. Some guidelines might include how login credentials are shared, how sensitive information like PII (Personal Identifiable Information) is shared, password strength, and setting up two-factor authentication. The more educated your team is on the importance of privacy, the more likely they are to hold themselves accountable which reduces internal threats.

Regulatory Compliance

Closely tied with privacy and security, compliance is another critical aspect of information governance. Over the last few decades, data privacy laws like GDPR, CCPA, SOX, PCI DSS, and HIPAA have cropped up, forcing companies to double down on their security, privacy, and discovery efforts. Although the costs of these efforts aren't cheap, it is 2.7x more costly for an organization to not implement compliance measures such as in-house legal expertise, yearly compliance audits, and centralized governance technologies.[7]

The average cost of compliance for businesses is $5.47 million vs. $14.82 million for non-compliance, which is a whopping difference of $9.35 million annually.

But non-compliant businesses risk incurring much more than a hefty fine — loss of customer trust, a damaged reputation, and long-term revenue loss are just some of the repercussions.

Although less regulated and younger companies can get away with putting off core compliance initiatives to save money and time, it only hurts them in the long run. Especially because more and more companies are working towards making global data protection policies standard. Implementing compliance initiatives is no easy feat, but the alternative is much more costly and data privacy laws will inevitably get more complex as time goes on.

Legal Operations

Legal operations also feed into a strong information governance program, and vice versa. From eDiscovery and legal hold, to retention policies, having information properly governed helps business leaders take on litigation, audits, or internal investigations that come their way. Outlining how information should be identified, classified, preserved, archived, and disposed of is crucial to minimizing risk, reducing costs, and augmenting transparency across the organization.

Due to the amount of unstructured data in today's organizations, automating eDiscovery, legal hold, and retention workflows has become the new standard. This is especially true for those that work largely with cloud-based applications and storage. The right automation tools will centralize, index, process, and preserve all of your enterprise information so that you can easily find what you need, collect it for review, and produce defensible evidence.

Bottom line, the most prepared legal teams have strong information governance programs. Adopting eDiscovery tools that automate legal processes on an ongoing basis is the best way to stay proactive and find what you need at a moment's notice — which is a quintessential piece of information governance.

Business Insights

At this point, it may seem like information governance is all about minimizing risk, but it's also about maximizing value. Once you've implemented the preliminary processes we just discussed, information governance can start to provide major value for your organization. When unstructured data is unified, protected, and discoverable, that data turns into contextual knowledge. Using machine learning and analytics, companies can start to identify trends and insights that give them a competitive edge and inform key business decisions in times of both crisis and opportunity.

Although achieving business insights tends to be the holy grail of information governance, the truth is it's hard to attain. The majority of organizations don't have a mature enough IG posture to find insights let alone find data itself. The key lies in being proactive rather than reactive, which means filling gaps in your program before you inevitably have to. The best information governance supports clean data that subsequently produces smarter, more accurate business insights.

The key lies in being proactive rather than reactive, which means filling gaps in your program before you inevitably have to.

04.

IG Leadership & Stakeholders

Leadership & Stakeholders

When it comes to the C-Suite and upper-level management, IG hasn't always been at the top of the agenda. We've seen a steady rise in IG leadership, but the reality is it's still a tough sell in many organizations.

We can attribute this fact largely to its multidisciplinary nature for a few reasons:

1. Since so many elements of IG are complex, interwoven, and unique to each organization, the concept itself is widely misunderstood and therefore its value is harder to demonstrate.
2. In a similar way, IG activities are dispersed across the business often getting grouped in with their sub-disciplines rather than the IG program at large.
3. There's usually a handful of stakeholders involved in IG, (such as legal, privacy, and analytics) each with competing priorities which creates friction in process and decision-making. For example, your analytics team may want to keep all of your data to maximize their sample size whereas your legal team may want to delete half of your data to avoid future liabilities.
4. Since IG is multi-disciplinary and balances a vast array of interests, finding someone with the right background to approve IG projects is hard to do.

So, without an IG champion in the C-Suite, who do companies turn to make decisions? For many, it's outside counsel who act as advisors outlining risk and reward. Although this can be helpful for deliberation, many teams continue to feel frustrated in who gets the final say. Not to mention, billing outside counsel is expensive. Other companies have "IG steering committees" or "data governance boards" which are essentially formal bodies dedicated to making IG decisions. With a 26% rise in the number IG Steering Committees in the last three years,[8] the need is clearly defined, however the committee members and leaders may vary.

Members	Leaders
IT	CIO
Security	CISO
Legal	Chief Legal Officer
Risk Management	CFO
Business Operations	Chief Data Officer
Audit & Compliance	CEO
Trust & Safety	COO
Finance & Tax	
HR	

Despite having an existing committee, many companies still struggle to take responsibility over different departments, coordinate between stakeholders, and balance risk and reward across all information in all its forms. The need for more IG leaders at the C-Suite level is clear, however they're still the minority. By better defining IG, assessing our own programs, and spreading awareness of its value, we can change this.

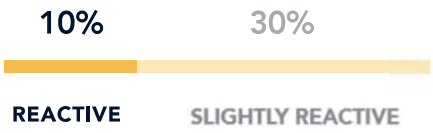
05.

Proactive vs. Reactive IG

Proactive vs. Reactive

Regardless of whether or not you have IG support in the C-Suite or a strong steering committee, a successful information governance program is within your reach. But to get there, you have to figure out just how proactive or reactive your current IG efforts are — Proactive being the most effective, and reactive being the least effective. Depending on the size of your company, how regulated your industry is, and how maturely established you are in elements previously discussed, you can land in a reactive state, proactive state, or somewhere in the middle. The key is figuring out where, so you can better forge your path to IG success. No one is perfectly proactive, so we expect most if not all organizations to land somewhere in the middle to lower range.

In a survey... In a survey by IGI, Information Governance professionals were asked to characterize the posture of their IG programs.

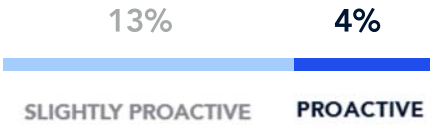


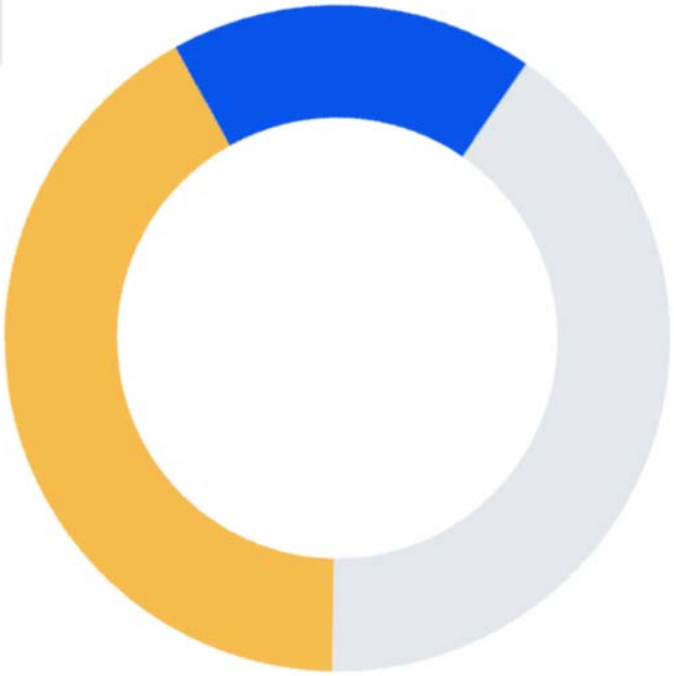
Reactive

40%

Proactive

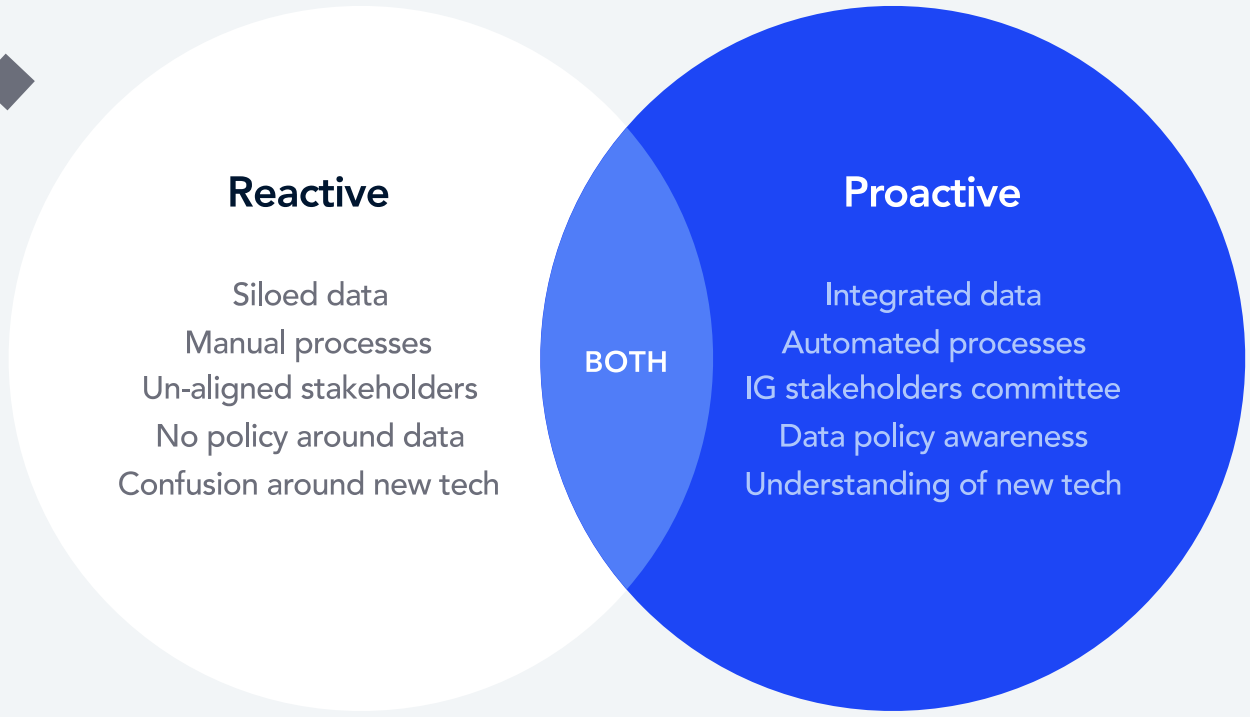
17%





Somewhere in the middle

43%



Note: Above are some general aspects of reactive vs. proactive IG programs for you to reference as benchmarks. Please know this is by no means an exhaustive list and is meant to be a sanity check of basic IG considerations.

Consider these questions....

1. Is your main motivator for IG only when regulatory, compliance or legal obligations pop up?

   - [ ] No, proactive
   - [x] **Yes, reactive**

2. Is a main motivator to also reduce long-term cost and risk?

   - [x] **Yes, proactive**
   - [ ] No, reactive

3. 32% of compliance costs come from payments to consultants, auditors or other outside experts. If able, do you see value bringing these efforts in-house?

   - [x] **Yes, proactive**
   - [ ] No, reactive

4. Are you able to leverage information to extract business value?

   - [x] **Yes, proactive**
   - [ ] No, reactive

06.

Ways to Advance IG in Your Business Today

Assemble an IG Committee

As we know, a successful IG program requires the balance of multiple disciplines, which means balancing the priorities of multiple stakeholders. Although stakeholders may be focused on different areas of IG, coming together to understand bigger picture goals can help teams deliberate efficiently, especially if you're running into conflicting interests often. Everyone wants to save costs, minimize risk, and have stronger business processes when issues arise, so why not work together to make it happen? Fostering a culture where everyone is on the same team is crucial for long-term success.

Revisit policies and procedures

After you've assembled your Information Governance committee, reviewing policies and procedures is a must. Your IG policies are a foundational piece of your IG program. They're influential in how you handle your information, how stakeholders make decisions, and what standards you set for the technologies you work with. You should also take this time to consider data mapping or do an information audit to see what policies need to be reformed.

Your team should be asking the what, where, and why of information's existence: Why are we holding on to it? What value does it have? What risk does it represent? Whether it be for data retention, defensible disposal or privacy and security, having thoughtful guidelines for the handling of your information before situations arise makes for a much more proactive and effective program.

Educate Employees

You can outline all of the policies you'd like, but getting any IG program off the ground takes active participation and support from employees. To do this, we urge IG professionals to educate their teams on the importance of their work. Consider launching an IG awareness campaign to teach your team about the many different facets of your program, and how it applies to their roles and the technologies they use. From online courses and security training to implementation review processes, there are plenty of ways to foster IG knowledge and enforce good practice.

Get to know your technology

The reality is that many information governance stakeholders don't understand the platforms in their tech stack, which is problematic when it comes to governing their information. When onboarding new technology, getting involved early and often in the implementation process is key. Make an effort to understand what the technology is, why your team needs it, and how they're going to use it. Having this level of transparency with your team from get-go will help mediate any concerns you might have and clue them into the "why" behind them. Also, get to know your vendors! Having candid conversations about their eDiscovery, security, and compliance features will help you better understand the limitations of the platform and the gaps you need to fill. Understanding these gaps is the first step towards finding a solid solutions partner or building an effective solution of your own.

Think about the future

As we enter a new decade, we're seeing more and more businesses adopt cutting edge technology and cloud-based workplace applications. With the ability to work anytime, anywhere, the rate at which we're working is accelerating, and consequently, so is the production of our data. Information is taking on new formats and accumulating in more silos than we can count, making knowledge increasingly harder to control, and this trend isn't going anywhere anytime soon.

So, how can we keep up? The answer lies somewhere in between the cooperation of technology vendors and the organizations that use them. We're entering a world where compliance, discovery, and security features are not only becoming a standard for workplace apps, but also a competitive edge. However, it takes businesses vocalizing their needs to help technology vendors build their platforms with their struggles in mind.

Instead of running from the complexity of new platforms, organizations should seek to understand them. The fact is that new technologies are bolstering people's productivity, so why not embrace that? It's impossible to monitor how people interact with new platforms without understanding the technology itself, so IG professionals need to be experts on what lives in their tech stack. It's only when IG professionals take time to do this that that they truly begin to see what other stakeholders need to be involved and spot gaps in process and collaboration. It takes a holistic effort from multiple sides of an organization to manage information successfully — and the organizations that recognize this will be leading the future of information governance.

Onna's Knowledge Integration Platform (KIP)

Onna is a Knowledge Integration Platform that unlocks enterprise knowledge from today's most popular workplace applications. We help businesses automate their enterprise needs for information governance, eDiscovery, compliance and more in a single platform. We centralize otherwise fragmented and unutilized knowledge from any number of our turnkey integrations, like Slack, G Suite, Microsoft 365, Box, and more to get your information enterprise-ready. Our open API allows us to integrate with any cloud-based or on-premise platform, for optimal control and visibility into your most critical information. Once an organization's tech stack is connected to Onna, their potential is limitless. Teams can unify, search, protect, automate, and build on top of their proprietary knowledge to leverage it in new and intuitive ways.

Curious how Onna can assist your IG initiatives?

Reach out to us here.

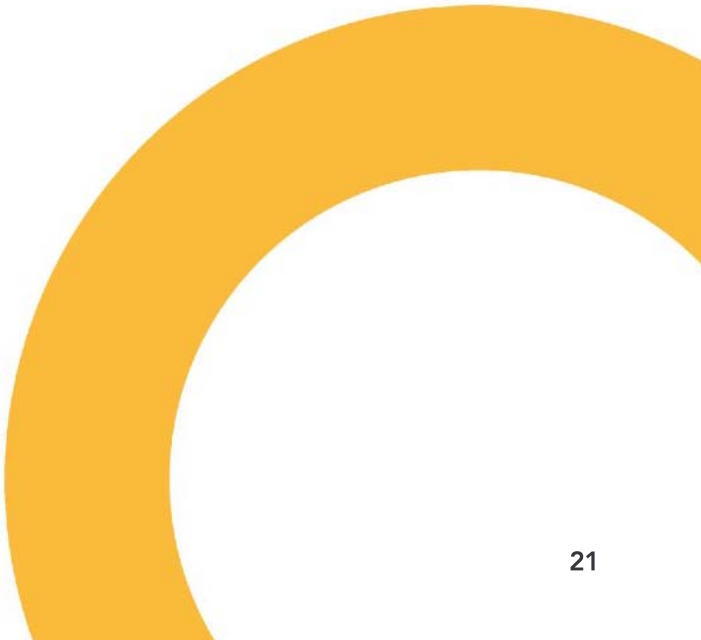
Terms

Stakeholder – A leader in an organization whose role is relevant in the scope of IG.

Organization – Any company of any size, from non-profit organizations to for-profit businesses.

Datasphere – quantifies and analyzes the amount of data created, captured, and replicated in any given year across the world. It also looks at how much of that data is stored across various storage components (IDC).

IG – Commonly used abbreviation for information governance.



Notes

[1] Smallwood, Robert “Information Governance: Concepts, Strategies and Best Practices” Hoboken, New Jersey: John Wiley & Sons Inc. [2020]

[2] Okta, "Businsses @ Work Report" (Okta, 2020).

[3] International Data Corporation, “The Digitization of the World — from Edge to Core” (International Data Corporation (IDC), 2018).

[4] International Data Group, “Data and Analytics Survey 2016” (International Data Group, 2016)

[5] Ponemon, L. (2018, July 11). Calculating The Cost of A Data Breach In 2018, The Age of AI and the IoT

[6] IBM, “2019 Cost of A Data Breach Report” (IBM, 2019).

[7] Ponemon Institute LLC., “The True Cost of Compliance with Data Protection Regulations” (Ponemon Institute LLC., December 2017)

[8] Information Governance Initiative, “Information Governance Initiative IGI State of the Industry Report 2016-2017” (Information Governance Initiative LLC., September 2017)

[9] Information Governance Initiative, “Information Governance Initiative IGI State of the Industry Report 2016-2017” (Information Governance Initiative LLC., September 2017)