RICOH
imagine. change.

Mitigating risk through information governance

Using automation to elevate corporate strategy, compliance and information security initiatives

Turning data into information

In many industries, from healthcare and education to government, financial services, manufacturing and more, the immense volume of data being generated daily can be overwhelming. That data is measured in terms of bytes, which are the units of memory it occupies on a computer or server. While data is measured in bytes, to fully grasp the incredible depth of it being produced and occupying expensive on-premises servers and cloud services, we are now creating zettabytes (ZB) of data — a measure that wasn't even available as a storage option on computers until 2021.[1]

Today's deluge of data can be unwieldy without the right systems and processes in place to discern its meaning. The acceleration of data is so shockingly pervasive that organizations are being forced to not only manage and secure the data they have — but to get ahead of this data storm as it continues to compound.

Much of this data can be highly valuable to an organization — but only when you have the tools and processes in place to derive value and meaning from it. **By turning raw data into structured, searchable and actionable information, organizations can uncover insights and empower better decision-making.**

But how? For years, **Enterprise Content Management (ECM)** solutions were commonly used in government, healthcare and education where compliance was a key requirement. ECM solutions centralize and organize information and automate document and multimedia file storage, management, organization, and distribution.

However, with the proliferation of hybrid and remote work, ECM has become a mainstream, competitive advantage for many other industries due to its power to effectively manage information and enable efficiency, increase productivity, reduce errors, and enhance business outcomes.

221 ZB

Global data growth by 2027, a 28.2% CAGR.[2]

7 PB

Petabytes of data will be created per second by 2026.[3]

[1] PCMag. "Seagate Is the First Company to Ship 3 Zettabytes of Hard Drive Storage." April 8, 2021.

[2,3] IDC Global DataSphere, April 2023 forecast.

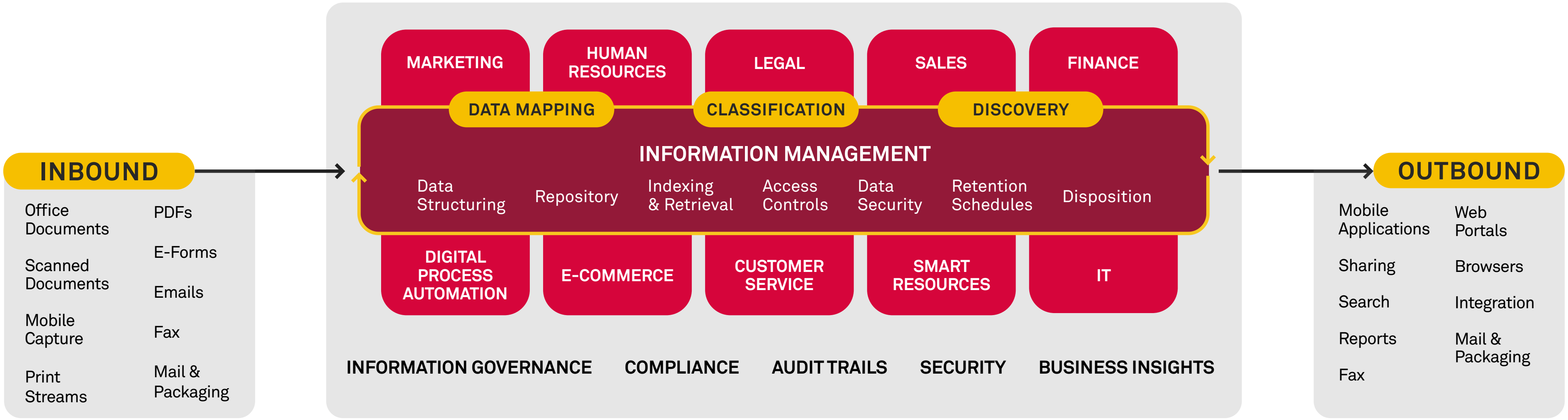
Making information governance a priority

Protecting your information **starts with knowing what you have, where it's located and the risk it could pose if it's not protected**. Once data is turned into information, organizations must understand how and where that information comes into the business (inbound information); how that information will be used and by whom, and what applications will need to use that data (through-bound); and finally, where that information will go or be stored (outbound). Throughout this journey, compliance, risk and security must play a major role.

Companies must consider the risks: information loss, privacy, cyber threats, theft, accidental or intentional destruction of critical data, denial of service attacks, and malicious code, among others. Security is not just about checking boxes during the procurement process — it's quickly becoming a significant market driver as more businesses mandate compliance, requiring partners and vendors to meet strict security and privacy standards. In today's world of increasingly complex and sophisticated cyberattacks, security should be expected throughout the enterprise — yet, for many, it is a competitive advantage.

> **The framework and practice of incorporating compliance and security with company information is how we define information governance.**

Maintaining control of your information while complying with regulations will mitigate risks. Information governance focuses on how to create, capture, manage, administer, collaborate and dispose of organizational information. It takes a coordinated effort and strategy of orchestrating people, process and technology. In layman's terms, think of it as a giant checklist to keep customer, partner and internal information secured and compliant.



Setting the stage: here's why it matters

The data analysis, research and studies on cybersecurity and information governance tell us business information is at risk. A holistic, data-driven approach throughout the entire organization is needed to achieve success. Otherwise, customer trust and experience, compliance, and profitability are at risk.

11%

Only 11% of companies say that they have full commitment and support for information governance from the organization and executives.[4]

1 ECM

A centralized enterprise management system would benefit companies by improving compliance 42%, customer insight 38% and security of content 38%.[5]

73%

Of businesses have experienced at least one significant disruption caused by a third party within the last three years.[6]

58

Class action lawsuits undergoing litigation from 23 customers seeking indemnification from Progress Software, owner of the breached MOVEit file transfer tool.[7]

11 seconds

A ransomware attack occurs every 11 seconds.[8]

13-14-21

Massive application sprawl has a typical employee using 13 back-office systems, 14 software applications and 21 online tools every day.[9]

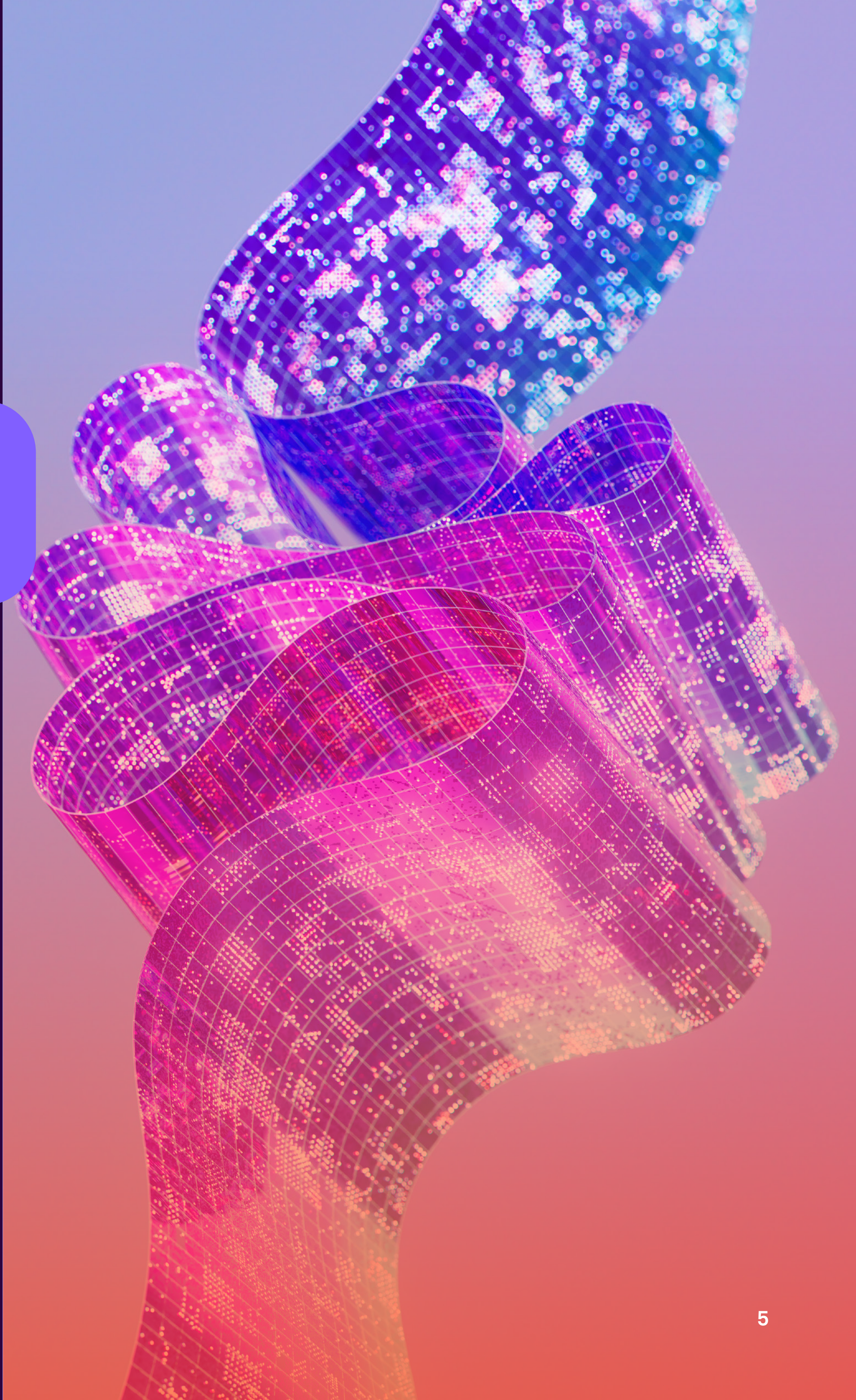
[4] AIIM. "How to Develop a Relevant and Effective Information Governance Strategy." 2022.
[5] IDC. "State of Content Services Survey." June, 2023, n=714.
[6] KPMG. Third Party Risk Management Outlook 2022.
[7] The Record. "Progress Software facing dozens of class action lawsuits, SEC investigation following MOVEit incident." October 12, 2023.
[8] Security Boulevard. "The Most Pressing Cybersecurity Challenges of 2023." February 2023.
[9] IDC. "Intelligent Digital Workspace (IDW) Market Survey. May 2022, N=609.

3 key elements of information governance

Your mantra for information governance and security should be: Know what you have, know why you have it, and know what the risk is for keeping it.

To do that, automation solutions like ECM, intelligent document processing (IDP), and robotic process automation (RPA) are helpful in managing your data and information throughout its lifecycle. Here are some of the essential elements you need to create your information governance approach — along with some other important things to consider:

1. A system for information and records management
2. Laser focus on knowing where your information lives
3. Automated processes are integral



1. A system for information and records management

Information and records need an ECM solution or repository where documents and files are classified or indexed and searchable in a digital format. Best practices and processes for managing the documents and their lifecycle are an integral part of information governance.

Here's how a typical document goes through its workflow and lifecycle:

1. The document or media is digitized or scanned.

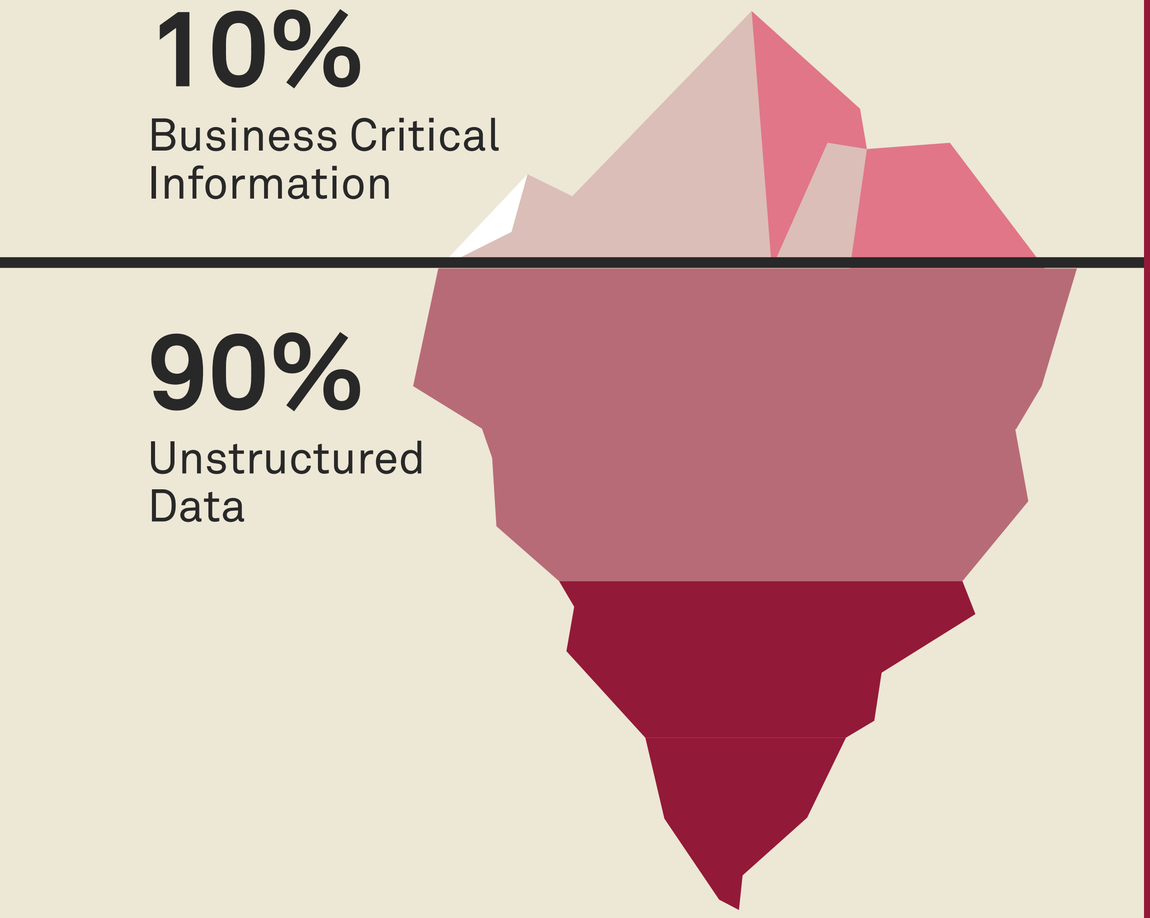
2. The document is sent into an IDP or capture solution, which transforms unstructured, semi-structured and structured data through classification, extraction, validation and exportation into any other type of application or workflow, such as an ECM, ERP, CRM, RPA, iPaaS, or other systems.

3. The digital document is then managed in the repository or application, where its information can be discovered, tracked, analyzed, managed, and ultimately archived, preserved or safely disposed of based on business rules or compliance standards.

About 90% of company documents, PDFs and media files are considered unstructured data, which is information that is not structured in a database format, making it difficult to search, manage, protect, and use.[10] Having unstructured data presents many risks, which is why any type of unstructured documents or images should be converted and digitized into structured information and securely managed across the organization. Protecting your data and minimizing risks is not just an IT responsibility — it must be a company-wide effort.

[10] IDC. "High Data Growth and Modern Applications Drive New Storage Requirements in Digitally Transformed Enterprises," July 2022.

2. Laser focus on knowing where your information lives



To increase security and optimize storage costs, IT teams must have knowledge of company information and where it’s located, the risk it presents, and whether that information needs to be retained.

It’s critical that organizations understand the difference between sensitive or regulated information, which requires security, privacy, and discovery controls, records, which require classification, storage, access, retrieval and disposition controls, and unstructured **ROT data (redundant, obsolete or trivial data)**, which is costly to store and increases the organization’s exposure to cyber threats.

It is estimated that ROT data accounts for a minimum of 25-30% of company data, with other sources saying it’s often much higher. Once an organization can weed out and reduce its ROT data, it can reduce storage costs and invest security where it matters most.

Protecting sensitive data, such as personally identifiable information (PII) and payment card industry (PCI) information, is critical in mitigating potential risks. This type of information commonly includes names, addresses, dates of birth, social security numbers, passwords, credit card numbers, banking information, or contracts. Therefore, establishing a secured information technology and management infrastructure will provide a foundation for maintaining compliance for both structured and unstructured data. This brings us to a closer examination of information security practices.

1 Encryption

Data encryption should be applied to documents, files, messages, or any other form of communication over a network. Additionally, it is a best practice to have end-to-end encryption for all devices, software, and storage solutions.

While data and information security should be a top priority for all staff, you can't rely on them to know when or how data should be encrypted. When developing your organization's encryption policy, you'll first want to get an accurate picture of where all your data resides, how much of it is confidential or valuable (a potential target for cyberattacks or bad actors), and the risks it presents to your organization. Cleaning up unstructured data and conducting a data protection impact assessment will enable you to develop a comprehensive data security strategy. Encryption will help fortify your overall company security.

2 Ransomware protection and containment

There are two critical layers to ransomware security — prevention and mitigation. Preventative solutions detect ransomware signatures and behaviors, stopping them from getting past the perimeter, whereas ransomware containment stops outbreaks of malicious encryption if it breaks through safeguards. The software focuses on the outcome of ransomware and rapid illegitimate encryption. It stops encryption at the source or root file, isolating and containing it to prevent further spread.

Ransomware containment is a critical last line of defense to an organization's security infrastructure, filling the perilous gap between devices and file shares where organizations often lack the essential defenses. Having a containment solution in place ensures that if an attack happens, you can respond quickly enough to protect the majority of your information.

3 Authentication

According to research, only 13% of employees at small to medium businesses (SMBs) are required to use multi-factor authentication (MFA), which uses several modes of identification to login or gain access to an application, compared to 87% of employees at companies with 10,000+ employees or more.[11] This means there is still room for improvement in this area.

Preventing the misuse of resources reduces operating costs, restricts user activity to enforce accountability, and provides insight to spot irregularities through reporting. Printing rules can include setting page limits by device, restricting color usage, enforcing duplex, restricting access to certain settings, and more. Budgetary account limits for copying and printing can be set up by the user — and include tracking walk-up activity at a multifunction printer.

If users must authenticate to print, the print rules you set are automatically enforced and activity is attributed back to the user. This can associate document printing, scanning, and faxing to a specific client/matter for the purpose of billing, which enables detailed activity reports around a project or confidential topic.

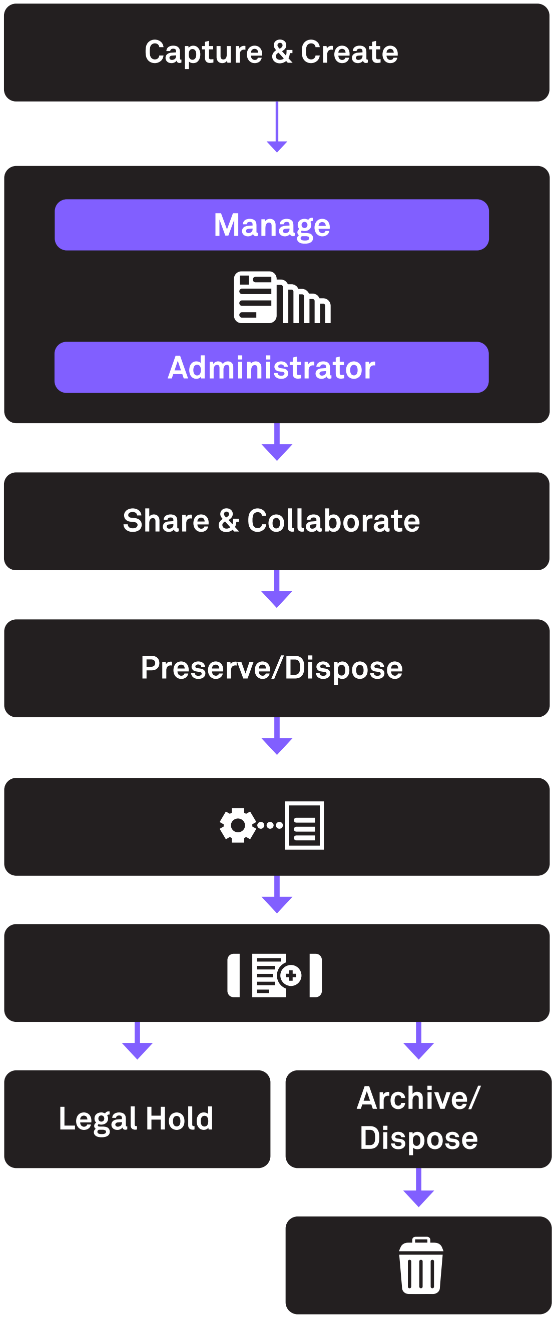
[11] Zippia. "17 ESSENTIAL MULTI-FACTOR AUTHENTICATION (MFA) STATISTICS [2023]." February 6, 2023.

3. Automated processes are integral

Many daily tasks involve business processes, workflows and transactions — much of which can be automated. Common processes where intelligent business platforms, such as data capture and workflow applications, can be applied are:

- Invoice processing
- Loan processing
- Claims management
- Human resources onboarding
- Patient records and forms
- Student transcripts and records
- Maintenance and sales orders

Automating processes offers a multitude of benefits and can uncover new possibilities for the way people work — but digitized data requires focused protection from the point of origin and throughout its lifecycle. For example, decreasing repetitive tasks (through automation tools like RPA and workflows) will help mitigate risks, deliver faster results and accelerate approvals.



40%

Cost-savings from Ricoh customers using information governance, while meeting security, sustainability and compliance objectives.[12]

Creating an information governance strategy and rules around business processes will benefit your organization in many ways:

- Avoid penalties and fines
- Build customer and supplier trust
- Maintain compliance and audits
- Combat potential security breaches, threats and attacks
- Better manage IT costs
- Accelerate processes to enhance customer experience
- Help employees break down productivity barriers to become more efficient
- Easy integration into other applications
- Enable a data-driven culture with ongoing operational process improvement

[12] Ricoh Document Governance. https://www.ricoh.co.uk/business-services/all-services/application-services/document-governance/.

What should you do next?

While there are many complexities around information governance, management and security, the key takeaway is to understand what information, documents and data you have, and how it is used and managed throughout its lifecycle. Once you do this, you'll be in a better position to mitigate risks and tackle compliance challenges head-on.

Modern, automated solutions, paired with ECM — from capture and workflows to devices, security and overall management — can not only be a competitive advantage but also serve to future-proof any business. Analyst research suggests that if all information, documents and applications were integrated and centralized, the top three benefits would be compliance, customer insight and content security.[13]

Leadership will need to convey the importance of information governance and security protocols by having the entire company comply with its guidelines. It's not just the IT team who should be at the table, but the collective organization. Fostering a data-driven culture must be top-of-mind. This often means embracing a "zero trust" mentality, which calls for a multi-layered security approach, including authentication, encryption and cybersecurity frameworks. Similarly, creating a strategy that permits the free flow of information to those who need the information but protects it at the same time.

[13] IDC. "State of Content Services Survey." June 2023.

7 steps to jumpstart your information governance program

These steps will help you build, promote and nurture a culture of information governance as you continue on your digital maturity continuum.

1. Identify your personally identifiable information (PII), payment card industry (PCI) information and intellectual property (IP) information.

2. Understand and comply with GDPR, HIPAA, SEC, PIPEDA/DCIA/CCPA, and other regulations.

3. Identify ROT information and remediate.

4. Isolate information that is not required beyond the purpose of its collection, such as credit card numbers or specific identification.

5. Archive what is of business or cultural value.

6. Monitor data stores regularly.

7. Continually review company policies for records and security.

Mitigating risk through information governance

Information governance and information security are ingrained in our values — a commitment we do not take lightly. Whether you're stuck in a data deluge, work in a highly regulated industry, lack resources or experience, or want the assurance of utilizing highly secured services, software, and devices, we aim to gain your trust by having the highest security standards in the industry.

Our depth of experience in consulting and applying a multi-layered approach can be leveraged across your organization from strategy, devices, software, services, support, training, and more. Let us help you in your digital information services journey.

Want to learn more? Visit Ricoh-usa.com or contact a Ricoh enterprise content management, information governance or security expert today.

Ricoh, a trusted partner

At Ricoh, we're empowering our customers to respond to our changing world with actionable insights. We believe having access to the right information translates to better business agility, more human experiences, and the ability to thrive in today's age of hybrid and borderless work. Through our people, experience, and solutions, we create competitive advantage every day for over 1.4 million businesses around the globe. To us, there's no such thing as too much information.

RICOH
imagine. change.

Ricoh USA, Inc. 300 Eagleview Boulevard, Exton, PA 19341 | 1-800-63-RICOH

The content of this document, and the appearance, features and specifications of Ricoh products and services are subject to change from time to time without notice. Products are shown with optional features. While care has been taken to ensure the accuracy of this information, Ricoh makes no representation or warranties about the accuracy, completeness or adequacy of the information contained herein, and shall not be liable for any errors or omissions in these materials. Actual results will vary depending upon use of the products and services, and the conditions and factors affecting performance. The only warranties for Ricoh products and services are as set forth in the express warranty statements accompanying them.