box

5 Steps to Good Governance

Transforming your governance strategy

Table of contents

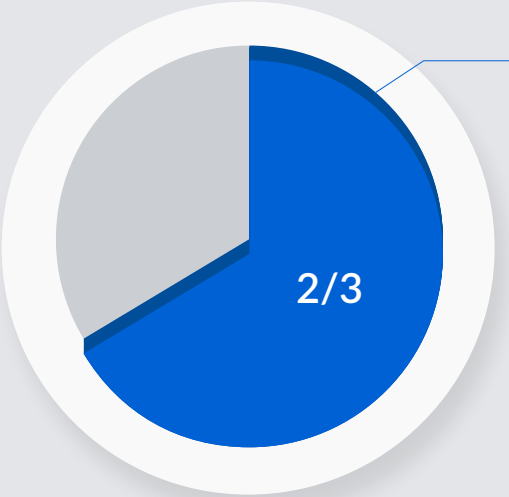
Unstructured data is on the rise

In fact, nearly 75% of senior executives believe the volume of data that organizations deal with will increase at least threefold in the next two years[1]. And with more content comes a related challenge: information governance.

It's no small task to appropriately manage, govern, retain, and dispose of all this content. Legacy governance systems are expensive and difficult to manage, and manual processing is seldom up to the task. In fact, two thirds of organizations in an AIIM survey estimated that over 60% of their information sprawl was due to unstructured content[2]. When you have unstructured content spread across different systems, it can simply be too difficult to keep track of where content lives and whether you're properly governing it.

By centralizing content on a single system and surfacing it across your line of business applications, you make governance efficient, seamless, and automatic. You protect your organization while letting employees focus on growth.

This guide will take you through five steps to establish a solid information governance program at your company.



Two thirds of organizations in and AIIM survey estimated that over 60% of their information sprawl was due to unstructured content

[1] *bit.ly/32nldda*
[2] *bit.ly/32nldda*

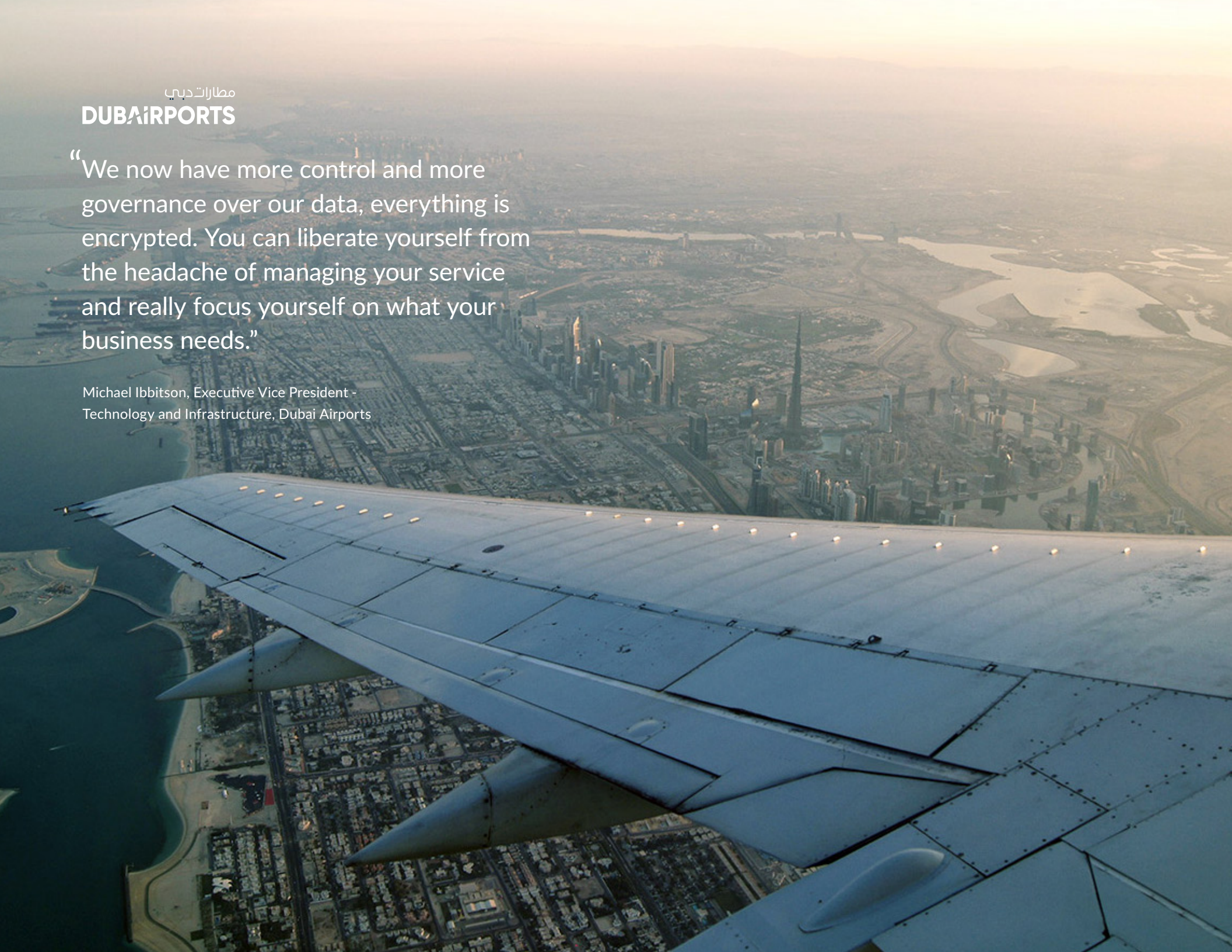
Step 1: Start early

There's no time like the present to start tackling information governance. Most organizations have to adhere to multiple regulations, and it's likely yours does as well.

Seventy-five percent of organizations must adhere to at least two regulations, according to AIIM, and many companies are subject to an even greater number of privacy (GDPR, CCPA, etc.) or industry (FINRA, PCI, etc.) policies. At the same time, fewer than one in three organizations have confidence that their retention policies could stand up to regulatory scrutiny.[3]

Reasons for not dealing with information governance	A very good reason to deal with it
"Tools for information governance are complicated and costly to maintain."	The costs of proper retention. Save your business money by preventing problems from the get-go: • Nearly 400 million pounds levied from the UK's FCA in 2017 due to record-keeping violations[4] • HIPAA fines for large healthcare organizations have averaged over $2 million over the last few years[5]
"Our employees should focus on growing the business; training them on compliance issues is distracting and time-consuming."	• Without good governance guardrails, employees get bogged down in manual retention processes; for example, 46% of organizations spend 6+ hours per week in each department managing manual retention of content[6], keeping employees from more strategic activities • Over 50% of senior executives deem the ability to transform compliance process and automate information management as highly important to an organization[7]
"The risk of deleting data outweighs that of keeping it."	• Keeping sensitive information, like credit card data and personally identifiable information (PII) beyond its business use can lead to regulatory non-compliance and fines[8] • 38% of senior executives believe that regulatory action from loss/exposure of personally identifiable information poses the greatest risk to their company

[3]*bit.ly/2APaCtQ*, [4]*https://bit.ly/2vRBuL6*, [5]*https://bit.ly/2T5FD5X*,
[6]*bit.ly/2APaCtQ*, [7]*bit.ly/32nldda*, [8]*https://bit.ly/2SVCUND*



"We now have more control and more governance over our data, everything is encrypted. You can liberate yourself from the headache of managing your service and really focus yourself on what your business needs."

Michael Ibbitson, Executive Vice President - Technology and Infrastructure, Dubai Airports

Step 2: Get all stakeholders onboard

It's a good idea to assign one person to take the lead on information governance for your organization. But you will need buy-in from executives and other stakeholders across your company to be successful.

Employees need to get their work done one way or another, and if they are not invested in your system, they will find a way to work outside of it. Show stakeholders how you will make their lives easier so they are motivated to participate in the process.

Executives

Protect the business from excessive litigation costs, compliance risks, and the bad press that comes with them.

Legal

Maintain chain of custody on content and manage ediscovery; minimize costs and reduce legal exposure from subpoenas or data spoliation.

HR and Finance

Ensure proper retention and disposition of employee and financial records.

IT and Security

Confirm classification levels and other requirements for protecting sensitive documents.

Compliance and records managers

Ensure the most important regulations and internal policies for document compliance and retention are met.

End users

Preserve the ability to get work done without friction from security, governance and compliance requirements.

COALFIRE

“We could not have asked for a more tailored solution for governance around the specific workflow we have to support, right out of the box. This was so much of a slam-dunk it was obvious.”

Robert L. Flores, Vice President of
Information Technology Services, Coalfire

Step 3: Proactively set guardrails for document lifecycle management

Protect sensitive or regulated data by applying intelligent policies that automatically follow your content. When you set guardrails for your users — from classification levels and retention/deletion timeframes, to rules for external sharing — you make adhering to governance requirements much easier on your teams.

Here's a handy checklist for how to get started:

- ☐ **Retention policies**
  Determine time periods for which you will retain content, and set disposition actions for when the retention period ends

- ☐ **eDiscovery support**
  Implement legal holds to preserve content for eDiscovery, and maintain audit trails of employees' content changes to avoid spoliation.

- ☐ **Compliance support**
  Configure policies to comply with regulations like FLSA, OSHA, and SOX as well as industry-specific regulations like FINRA for financial services or HIPAA for healthcare.

- ☐ **Deletion control**
  Decide who can permanently delete items from the trash. Create an automatic email archive of user activities.

- ☐ **Data Protection**
  Protect high-value data from accidental or malicious deletion by setting protective policies.

- ☐ **Content archival**
  Remove redundant, outdated or trivial information to simplify how teams get work done and find relevant content for eDiscovery.

AMTECK

"The legal hold and discovery process was a driving factor for us in choosing Box Governance."

Drew Phillips, Director of IT, Amteck

Step 4: Keep it simple

Don’t succumb to analysis paralysis and worry about accounting for every last use case before implementing your information governance plan. Instead, work with broad strokes to apply appropriate policies to as much content as possible — especially for high-risk or regulated departmental content.

Here’s how we’ve seen forward-thinking companies keep information governance simple, secure, and seamless:

“Big bucket” strategy

Group your content into big buckets wherein you apply appropriate policies. For example, rather than having separate policies for all accounts payable files (vouchers, invoices, receiving reports, purchase orders, checks, etc.), bucket them into one policy based on the most high-risk content.

Self-governing documents

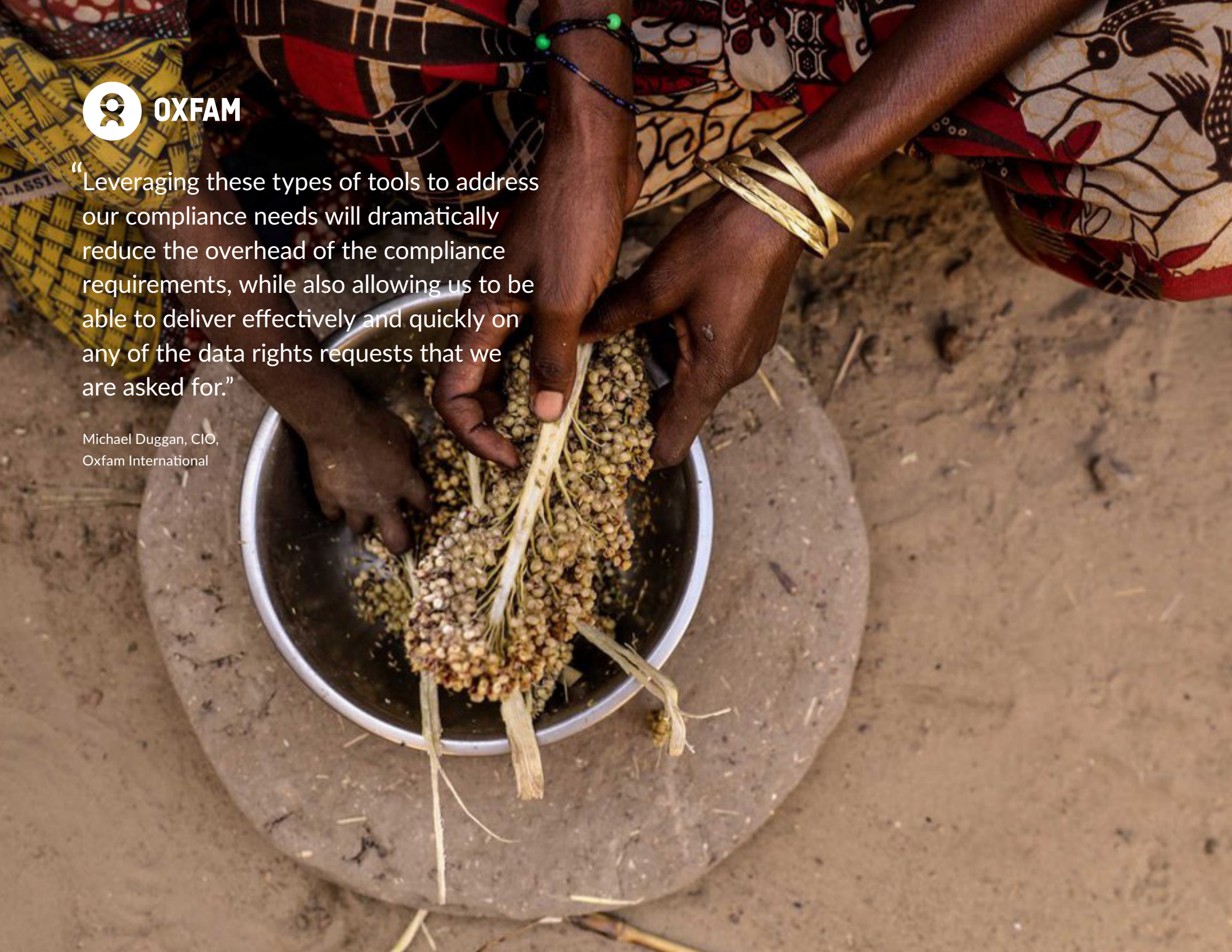
Make retention simple for users and administrators so they don’t have to interact with files in a separate, siloed repository or go through cumbersome, manual processes. Instead, use lifecycle management policies that follow documents where people engage with them across all their workplace applications.

Classification cues

Remind employees what category a document falls into (contract, employee record, etc.) and if it contains sensitive data with visual cues. If a file meets a specific confidentiality or regulatory threshold, proactively set the right lifecycle management and security guardrails. This takes the burden off the user.

Seamless eDiscovery

Preserve content for subpoenas or legal action without impacting user productivity or requiring significant time and effort from your legal or IT teams.



"Leveraging these types of tools to address our compliance needs will dramatically reduce the overhead of the compliance requirements, while also allowing us to be able to deliver effectively and quickly on any of the data rights requests that we are asked for."

Michael Duggan, CIO,
Oxfam International

Step 5: Talk to our experts

No business can afford to wait when it comes to information governance. With the high costs of regulatory exposure, the challenges of manual retention and the growth of unstructured content, the time to act with implementing a robust governance program is now. By centralizing your content in a single system in the cloud, you can remove the traditional barriers to effective governance, enable your employees and protect your business for the future.

To learn more, visit box.com/security/governance-and-compliance

box

Box (NYSE:BOX) is a leading Cloud Content Management platform that enables organizations to accelerate business processes, power workplace collaboration, and protect their most valuable information, all while working with a best-of-breed enterprise IT stack. Founded in 2005, Box simplifies work for 68% of the Fortune 500, including AstraZeneca, General Electric, JLL, and Nationwide. Box is headquartered in Redwood City, CA, with offices across the United States, Europe, and Asia.

To learn more about Box,
visit www.box.com