



**Manage your  
documents effectively**

---

**EQUINITI**  
ICS



## Contents

.....  
The Evolution of Document Management  
.....

Why the public sector need document  
management systems  
.....

Secure sharing  
.....

Future challenges  
.....

Document management implementation checklist  
.....





# The Evolution of Document Management

Gone are the days when document management constituted an overstuffed filing cabinet. Now, document management solutions can be used to systematically organise and process both paper and digital documents, but this isn't without its challenges.

Juggling both physical and digital documents requires an amalgamation of processes to be put in place to centralise and classify documents from different sources. Then there's the third element – unstructured data – which is set to further complicate how an organisation captures, categorises and manages documents.

Scanning plays a pivotal role in digitalising hard copy information. Documents can be converted into a range of formats such as PDF, Word, JPEG and TIFFS and can even be automatically interpreted. For instance, Optical Character Recognition (OCR) can convert scanned images to text automatically while imaging software can be used to scan and annotate documents from any source, removing the need for manual data entry.

Yet digitalisation isn't just about the conversion of paper to digital formats. It has the power to fundamentally change the way we work. By reducing our dependency on physical documents we can make data more accessible and easier to share, reducing costs and streamlining business processes. It's this reasoning that was behind the UK government's 'Digital by default' mandate.

To facilitate this, the government set out guidelines for the adoption of open standards which would see documents converted into standard formats in a bid to eradicate data silos and to foster data interoperability.

However, once it became clear that the majority of documents no longer needed to reside on closed networks such as the PSN (Public Sector Network) due to advances in cloud computing (GDS stated that the public cloud was safe to use for "the vast majority of government information and services" back in January 2017) the need to prescribe document formatting seemed redundant as most documents would in all likelihood be published digitally.

Cloud adoption also paved the way for synchronisation which has enabled document handling to evolve, so that instead of being constrained to a desktop PC where documents are stored on a local network or 'My Documents' folder, the user can access data from any location via a central shared repository. Platforms such as SharePoint have been instrumental in taking document management to the next level, enabling documents to be synchronised and rules imposed to ensure secure data sharing.

One of the biggest advantages of this synchronisation is version control and permissions management. If rule sets are applied to track the manipulation of data – from the creation of a document through to editing and deletion – it's possible to provide multi-party access. This means that more than one user can access and manipulate the document at any given time, from any location; a capability which has in turn paved the way for collaborative working.



## Why the public sector need document management systems

Data governance is becoming increasingly important in the public sector to ensure information is shared securely.

There's a realisation that data needs to be made more widely available so that departments can prevent duplication of effort, citizens can benefit from joined up services, and civil servants can work more collaboratively.

As the Digital Strategy states, government "must maintain the confidence and trust of those who provide us with their data: that it will be kept safe and secure: that it will be handled legally, responsibly and ethically". It warns that any failure to do so will result in strict penalties for misuse. Yet the strategy also calls for data to become "open by default". So how can public sector organisations make data both open and secure?

The first step is outlining how data will be stored, archived and retrieved securely is a document and records management policy which many government bodies already have in place. This provides organisations with a uniform

set of requirements which align to the Digital by Default mandate by reducing reliance on paper-based documents, making documents available in common formats (in keeping with the open standards advocated for government data and technology), and promoting accessibility through support for data over any device.

What's missing - and is going to become increasingly important in the future - is a reference to how data will be shared.

For data to be shared, public sector organisations must have the requisite infrastructure in place, encompassing storage, software tools, networks, cyber security and data management. In real terms, this means a solution capable of facilitating data discovery, building taxonomies and of managing data using automated tools. Only a dedicated document management system can perform all of these functions, providing end-to-end lifecycle management.





## Secure sharing

Electronic document management systems facilitate secure data sharing in the following ways:

- **Data discovery:** siloed data can be identified and tagged from across disparate systems or locations. A 'Redundant, Obsolete, Trivial' (ROT) analysis can be carried out to determine which data needs to be retained. Even 'dark data' can be mapped
- **Disparate data formats:** documents can be scanned or converted into digital open standard formats. Even images can be scanned and the contents automatically converted to text
- **Centralisation:** documents are filed in taxonomies in a central archive, eliminating the problem of data loss and making search and retrieval easier. Filing is performed automatically using Artificial Intelligence and pattern-matching to read and categorise content. Documents can also be flagged for retention, disposal or review
- **User access:** permission-based access allows authenticated users to access and manipulate documents ensuring staff can collaborate effectively and securely. Changes are tracked showing when a document has been edited for auditing purposes
- **Secure storage:** confidential data can be encrypted and provision is made for secure data disposal at end of life
- **Compliance:** automatic compliance with FOIA, DPA and GDPR requirements. For example, tools facilitate search across structured and unstructured data for Personal Identifiable Information (PII) in keeping with the demands of the GDPR.

It's only by putting in place a document management system that can automatically identify, classify and track data handling that public sector organisations can begin to move towards the democratisation of data envisioned in the Digital Strategy.

To become 'open by default' organisations will also need to revise their document management policies to support wider and inter-departmental data and even commercial access.

The Digital Economy Act makes provision for such data to be made available to businesses with a recognised public interest, such as utility providers, for example, making it imperative government organisations look to open up access beyond their immediate networks.

To systematically capture and control data in line with compliance requirements the public sector needs effective document management. Armed with a watertight policy and Artificial Intelligence powered document management platform, organisations can provide the assurance and evidence needed to demonstrate that data is being handled securely and responsibly.





Shared or collaborative working practices bring real cost benefits and productivity gains and it is now a recognised and supported mode of working within government. Employees in disparate locations can access and work on the same documents and discuss and exchange ideas without having to physically meet, resulting in faster more accurate working and flatter structures. For example, on the SharePoint platform, teams can be formed by department, division or project to work on specific documents or be given access to certain resources, creating a multi-layered intranet. Employees can then simultaneously access collective resources such as files, data and apps.

## Future challenges

**For the public sector, these advances in document management have led to fundamental changes. Now the priority is not just bringing data online but making that data accessible on any device, making it more malleable, and easier to download and store.**

The latest guidance on open standards for government requires that all users both within and outside of government are able to:

- Access and read information
- Store a local copy of the information they are viewing
- Print a copy of the information they are viewing
- Preserve information for archiving or as a record
- Make sure that the information they are creating can be viewed in the way they were intending
- Be able to create accessible content and to use accessibility tools with information in online and offline formats
- Access information on a device and platform of their choice, for example a laptop, tablet or smartphone
- Be sure of the integrity of specific information
- See previews of statistical information.







This clearly sees data becoming more answerable to user needs with multiple modes of access. Supporting the user in this way will require automated document management, with processes such as document discovery, classification, filing and retrieval performed using tools that can use Artificial Intelligence to automatically scan and interpret data, allocate access privileges and track document manipulation.

In the future, document management in government will morph again. The growth in data from both structured and unstructured sources will make discovery and classification even more pressing as the data mountain grows. This has the potential to provide the public sector with a rich mine of information to deliver even more effective e-government services, provided the document management is in place to sort, classify, organise and protect access to this content.



# Document management implementation checklist

Tick the list item to check you've completed

|   |   |   |
|---|---|---|
| <b>01</b><br><br>Project initiation & planning<br><input type="checkbox"/> | <b>02</b><br><br>Define requirements<br><input type="checkbox"/> | <b>03</b><br><br>Develop, test and implement a solution<br><input type="checkbox"/>      |
| <b>04</b><br><br>Carry out transfer<br><input type="checkbox"/>            | <b>05</b><br><br>Test for continuity<br><input type="checkbox"/> | <b>06</b><br><br>Delete content and remove redundant systems<br><input type="checkbox"/> |



## Your checklist guide

### 1. Project initiation and planning

- Define high level aims and objectives
- Identify resource and budget
- Liaise with third party suppliers
- Define success criteria
- Identify risks and issues

### 2. Define requirements

- How and why does the business need to use the information?
- What functionality do you need from a new document management system?
- Identify risks and issues of migration

### 3. Develop, test and implement a solution

- Agree roles and responsibilities for developing and testing
- Identify risks and issues

### 4. Carry out transfer

- Agree responsibilities
- Identify risks and issues
- Agree timing for the transfers
- Define and test migration process

### 5. Test for continuity

- Test migrated content
- Evaluate results

### 6. Delete content and remove redundant systems

- Agree date and time for deleting content and removing redundant systems



**Contact Details:**

eqcontent@equiniti-ics.com  
@EquinitiICS