AUDIT READINESS

CROSS-FUNCTION · HR · FINANCE · OPERATIONS · LEGAL

Audit-Ready File Management

Turning the file audit from a paper-and-people exercise into a scoped, time-bound login — conducted remotely, and logged end to end.

Objective: make every function audit-ready by default — digitizing legacy physical files, streamlining existing digital records, and giving auditors controlled, time-limited access to exactly the files within their scope.

The Challenge

- **Paper-heavy audits.** Files were retrieved, photocopied, boxed and carried to wherever the auditor was sitting.
- **All-or-nothing access.** Handing over a cabinet or a shared drive exposed far more than the audit scope required.
- **No expiry.** Once access was granted, there was no clean way to withdraw it when the audit closed.
- **No trail.** Nobody could say afterwards which files an auditor had actually opened or taken away.

The Kleeto Approach

Kleeto DMS digitizes legacy physical files and streamlines existing digital records into a single searchable repository across HR, Finance, Operations and Legal.

The audit then runs inside the system. An **auditor account** is created with its own credentials, and its rights are scoped by function, department, location and document type.

Each login also carries a **validity window** — when the audit period ends, the account expires on its own, with every view and download already on record.

How an Audit Runs on Kleeto DMS

01
Create the Account
An auditor account is set up in the DMS with its own login credentials.

02
Scope the Rights
Access is defined by function, department, location and document type, plus a login timeline.

03
Audit Remotely
The auditor signs in to the web UI from anywhere and views or downloads only permitted files.

04
Access Expires
When the defined duration ends, the login lapses automatically — no manual revocation.

Auditor rights are scoped on four axes

Plus a login validity window set for the audit period.

FUNCTION
HR, Finance, Operations or Legal — only the function under audit.

DEPARTMENT
Narrowed further to the specific teams in scope.

LOCATION
Restricted to a plant, branch, region or single site.

DOCUMENT TYPE
Down to the record types the auditor is entitled to see.

Core Capabilities

Secure Auditor Access

Dedicated auditor accounts with restricted access rights.

- By function &
- department By location
- and site

Time-Bound Credentials

Logins carry a defined validity window for the audit.

-
- Set for the audit period
- Expires when the audit
- ends No manual

Remote Audits

A web-based UI opens the audit to any location.

- Audits scheduled online
- Only permitted files
- shown No physical file

Audit-Ready Across Every Function

HR

Employee files, statutory records and lifecycle letters.

Finance

Invoices, vouchers, receivables, payables and reimbursements.

Operations

Process records, supporting documents and site files.

Legal

Contracts, agreements, addendums and litigation documents.

How the Audit Control Works

CONTROL	HOW IT WORKS	WHY IT MATTERS
Scoped access rights	Rights are set by function, department, location and document type	The auditor sees only what is in scope
Time-bound credentials	The login lapses when the defined duration is complete	No lingering access after the audit closes
Remote, logged access	Auditors work in the web UI while activity is	Audits run from anywhere, with a full trail

The Result

Files stay e-audit ready before every review. Auditors get precisely the access they need, for exactly as long as they need it, from wherever they are — and the organization keeps a record of everything they viewed. No paper, no manual file keeping, no time lost to physical audits.

80M+	20M+	18M+	ISO & GDPR
Finance files	HR files	Legal and other	aligned security