cloudficient

# Identity drift in eDiscovery

Why current custodian information may not explain the people, relationships, and sources that mattered during the case window.

An employee may still appear in the organization's records, and their email account may still exist. Yet that information may not reflect their role, responsibilities, or access to information when the events in question occurred.

During the case window, the person may have held a different role, reported to another manager, belonged to different teams, used other accounts, or worked in repositories that are no longer associated with them. If identification begins with current information alone, those earlier relationships may not be visible when scope decisions are made.

**These ordinary business events lead to identity drift, where today's records can diverge significantly from what was true during the period in question.**

## Identity changes while obligations remain

Organizational change is routine. Employees move between departments, assume new responsibilities, join (or leave) projects, change legal entities and leave the organization. Mergers, reorganizations, and platform changes can alter accounts, reporting lines, group memberships, and source ownership at the same time. Modern collaboration platforms add complexity by allowing employees to work across departments, projects, shared documents, and repositories that may not be associated with their primary role or department.

**As those changes accumulate, the current custodian record may no longer show:**

- The person's role, department, manager, or team during the relevant period
- The accounts, groups, collaboration spaces, and shared repositories connected to that role during the relevant period
- Whether the person was active, had changed responsibilities, or had left the organization when a relevant event occurred

## Current identity can shape historical scope

Custodian and source decisions are often made prior to and/or during the preservation phase and generally, before collection efforts begin. The information available at that point directly impacts and influences the scope of preservation and collection: who is included, which repositories receive attention, and where preservation is applied.

When historical identity is unavailable, a team may identify the correct individual but still miss important sources connected to that person's responsibilities during the case window. A current department may point to the wrong business function. Current group membership may omit a former project team. A present-day OneDrive or mailbox may not reveal work performed through a shared site, channel, group account, or earlier identity.

**The result is not necessarily a missing custodian. It may be an incomplete explanation of why that custodian mattered and where their relevant work occurred.**

That uncertainty can also move downstream. Teams may compensate by broadening scope, adding sources as new facts emerge, or revisiting preservation and collection decisions later in the matter.

## Permission does not establish activity

A permission may show that someone could access a repository or document. It does not establish that the person opened, edited, downloaded, shared, or relied on the content. Where an available Microsoft 365 user activity record shows a recorded action, that activity can provide a different form of information about the relationship between the person and the source.

**The distinction matters:**

Organizational and identity information can help establish an individual's responsibilities and relationships to potentially relevant sources during the case window.

Permissions can show potential access during the period for which those records are available.

Recorded activity can show particular actions captured by the available record.

If activity records do not cover the relevant period, the person's actual activity may remain unknown. Current permissions should not be substituted for missing historical evidence. Taken together, these elements help to establish a contextual nexus between the individual, the source and the potentially relevant content.

## Identity history supports better-informed decisions

Examining identity over time connects a person to the organizational and technical environment that existed when the relevant work occurred.

**Maintaining that information can help teams:**

- Identify potentially relevant custodians and other relevant people using responsibilities from the relevant period
- Investigate shared repositories, collaboration spaces, accounts, and groups connected to those responsibilities
- Explain how identity and source information informed preservation and collection scope

Historical identity does not determine relevance or replace legal judgment. It gives the people making those decisions better information while scope can still be influenced.

It also creates a clearer record of how the matter developed. If a custodian or source is added, removed, or treated differently, the team can connect that decision to the information available at the time rather than relying on a present-day view of the organization.

## The question is whether the past can still be explained

A current directory can answer who someone is now. A historical matter may require a more refined and focused approach: who they were, what responsibilities they held, which organizational relationships applied, and which systems and repositories were connected to their work during the relevant period. Mapping permissions, access and actual activity provides targeted insight into an individuals connectivity to specific data and the relevant issues.

When those connections are maintained, identification can reflect the organization as it existed when the events occurred. When they are unavailable, the resulting uncertainty should remain visible rather than being replaced with current-state assumptions.

**Identity drift cannot always be eliminated. It can, however, be recognized and addressed before today's custodian record becomes the default explanation for yesterday's events.**

NEXT STEP

**Refining Matter Scope Beyond Custodian Lists**

Use identity, custodian knowledge, activity, and repository context to make earlier, better-informed eDiscovery decisions.

Request the guide →