Commercial off-the-shelf applications

# Commercial off-the-shelf applications

We have developed a series of logging requirements for Commercial off-the-shelf (COTS) applications, such as Software-as-a-Service (SaaS) solutions or where applications are not so customised that they can reasonably be considered bespoke/custom for the Ministry of Justice (MoJ).

## Baseline Maturity Tier

### 1. User directory services

Log Collection Principle(s): 1, 2

User directory services, or interactions with them, must create and forward Authentication and Authorisation events.

User directories within application environments can be rich and diverse, such technologies include:

* Active Directory (AD)
* Azure Active Directory
* OpenLDAP
* Amazon Web Services (Accounts and Incognito)
* Okta
* Auth0
* Github.com (acting as an identity provider)
* Google Workspace (acting as an identity provider)
* Oracle identity stores
* Local user stores within operating systems leveraged by tenant applications

These event types must be logged and forward:

1. Account creation
2. Account lockout
3. Account reinstatement
4. Account authentication failures
5. Account authentication successes after 1 or more failures
6. Account password changes
7. Group membership addition / deletion (in particular, any group that gives admin access)
8. Group creation
9. Privilege modification for users (for example, role delegation through AWS IAM)
10. Multi-factor authentication state, such as:
    1. Enabled
    2. Disabled
    3. Reset/rotation
    4. Recovery method used

### 2. Authenticated user activity events

Log Collection Principle(s): 6

Applications should create viable user activity audit information for authenticated users to reasonably identify which authenticated user took which action.

1. User/group identifier(s)
2. Action/query
3. Response size
4. Response time

## Enhanced Maturity Tier

### 1. Data store events

Log Collection Principle(s): 6

Temporary data stores (such as intermediate queues) and permanent data store (such as databases) are key data locations and all interactions should be highly auditable.

1. Data store identifier(s)
2. Credential identifier(s)
3. Query
4. Query response size
5. Query response time

### 2. Unauthenticated user activity events

Log Collection Principle(s): 6

Where unauthenticated users interact with applications (for example, a MoJ Google Workspace document available on the general Internet through relaxed access controls), associated audit information must be created.

1. End-client identifier(s)
2. Query metadata:
   1. Destination identifier (such as target hostname, TCP/UDP port and/or full URI)
   2. Query type (for example, HTTP GET or HTTP POST)
   3. Query size
3. Response size
4. Response time