COMPLIANCE · TEMPLATE

# Evidence Pipelines 101: How to *Stop* Reconstructing Audit Artifacts Quarterly

KAANSYSTEMS.COM/LIBRARY/EVIDENCE-PIPELINES-101 · MAY 30, 2026

## ABOUT THIS TEMPLATE

Audits ask for evidence of controls in operation, not just controls in design. The pipeline that produces that evidence continuously, instead of reconstructing it under deadline.

## THE TEMPLATE

The map below ties controls to evidence sources. Run through it for your environment; anywhere you can't fill in a source, query, or retention value is a gap to close before your next audit.

| CONTROL AREA | EVIDENCE TYPE | SOURCE | SAMPLE QUERY | RETENTION |
|---|---|---|---|---|
| Identity — privileged access | Auth + assumption events | CloudTrail `AssumeRole`, Identity Center login | `WHERE eventName='AssumeRole' AND user_arn LIKE '%admin%'` | 7 years |
| Identity — terminations | Account deactivation events | Identity Center, HR system join | `WHERE event='UserDeactivated' AND timestamp > <termination_date>` | 7 years |
| Change management — production | Merged PR + approver list | GitHub Audit Log | `WHERE action='pull_request.merged' AND repo IN <prod_repos>` | 7 years |
| Change management — infrastructure | Terraform apply events | TF Cloud / Atlantis | `WHERE event='terraform.apply' AND workspace LIKE 'prod-%'` | 7 years |
| Configuration — S3 encryption | Resource config snapshots | AWS Config | `SELECT resourceId WHERE configuration.encryption.status='Disabled'` | 7 years |

| CONTROL AREA | EVIDENCE TYPE | SOURCE | SAMPLE QUERY | RETENTION |
|---|---|---|---|---|
| Configuration — SG rules | Resource config snapshots | AWS Config | `SELECT resourceId WHERE configuration.ipPermissions[*].cidrIp='0.0.0.0/0'` | 7 years |
| Data access — PHI tables | DB audit log | RDS audit, application audit | `WHERE table_accessed IN <phi_tables> GROUP BY user` | 7 years |
| Data access — S3 PHI buckets | Object-level events | CloudTrail data events | `WHERE eventSource='s3.amazonaws.com' AND requestParameters.bucketName=<phi_bucket>` | 7 years |
| Secrets — rotation | Secret rotation events | Secrets Manager | `WHERE event='SecretRotated' AND age_days > 90` | 7 years |
| Secrets — credential revocation | Credential deletion events | IAM access keys, app secrets | `WHERE event='AccessKeyDeleted'` | 7 years |

Fill in the queries with your environment's specifics. Fill in the retention column based on your regulatory mix. The format is what matters: control mapped to source mapped to query mapped to retention.

## WHAT THIS BUYS YOU

The first audit after this is in place feels different. Instead of three engineers and two weeks, it's one engineer and two days. The auditor stops asking "can you produce this?" and asks "show me the query." You demo. They check the retention. Move on.

The second audit feels like maintenance. The third audit, the auditor stops asking because the answers have all been pre-generated.

The same pipeline doubles as your incident-investigation substrate. The next security incident, your team doesn't reconstruct the timeline from console screenshots. They query it.