

SECURITY & ASSURANCE / 2025

Access management assessment

NIST SP 800-53 Rev. 5 · Cross-framework evidence review

EXECUTIVE ASSESSMENT

Account-management practices are documented and in use. Exception follow-up remains unverified.

The policy, account inventory and operating records show account-management practices in use. Three review exceptions lack recorded resolutions. AC-2 is recorded at maturity 2 of 5; the available records do not yet establish consistent follow-through.

4

Evidence files

8

Mapped controls

1

Control assessed

ENGAGEMENT

Production applications and the identity platform, including Canadian offices and cloud hosting.

Maya Chen

12 Nov 2025

Illustrative engagement for ACME Inc.

IN THIS REPORT

Scope and method	02
Control assessment	03
Evidence coverage	04
Findings and follow-up	05

What this assessment covers

ASSESSMENT BOUNDARY

The engagement focuses on account ownership, access approval, periodic review and removal across production applications and the identity platform. The NIST moderate impact baseline provides the framework context. ISO 27001 mappings identify where the same evidence is relevant.

INCLUDED	NOT ESTABLISHED
Access-control policy; production account inventory; review decisions and exceptions; one leaver-access record.	Complete testing of all framework requirements, population-wide effectiveness, or ISO conformity. A mapping alone is not an assessment result.

HOW THE CONCLUSION WAS REACHED

- 01 Read the requirement in context**

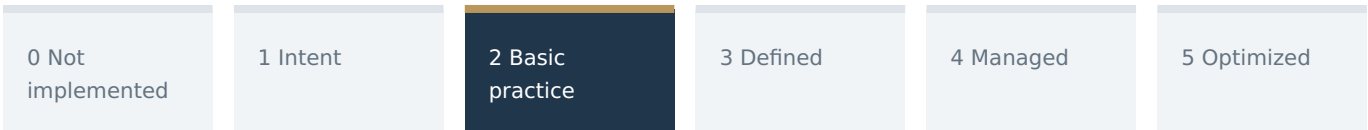
Review the framework boundary and control expectations before considering what the evidence supports.
- 02 Compare policy with operating records**

Distinguish a stated requirement from a completed activity. Use the inventory, review register and leaver ticket together.
- 03 Resolve missing context with the assessor**

Record what the assessor verified with the client. Update the rationale and gaps without treating the original file as if it contained those later facts.

READING THE MATURITY RESULT

Maturity describes the process demonstrated by the available evidence. It is separate from a conformity decision. For AC-2, operating records support basic practice; exception closure and consistent follow-through remain unverified.



A missing record limits what can be concluded. It does not, by itself, establish that the activity never occurred. The findings on page 5 identify the specific remaining limitation.

NIST SP 800-53 REV. 5 / AC-2

Account management

2 / 5

Basic practice

Version 2 · 12 Nov 2025 · Maya Chen

ASSESSMENT RATIONALE

The policy assigns account responsibilities. The account register, leaver ticket, and review register show the process in use. Three review exceptions are listed without a recorded resolution.

BASIS FOR THE CONCLUSION

E01 · Access policy

Assigns account responsibilities and requires approvals, periodic review and removal of inappropriate access.

E02 + E03 · Review and account registers

Identify the account population, reviewers and decisions. The original review register leaves three exception closures unrecorded.

E04 · Leaver ticket

Demonstrates one completed access removal, including completion time and service-desk verification.

Identified gap

The review register does not record how the three access exceptions were resolved.

RECORDED PROGRESSION

V1 · Maturity 1

10 Nov 2025

V2 · Maturity 2

12 Nov 2025

Evidence coverage

Four files relate to eight distinct controls across NIST and ISO. The register below preserves the role of each source; the matrix shows where it is relevant.

- E01

access-management-policy.pdf
Defines account ownership, access approvals, least privilege, and quarterly reviews. Reviewers must record exceptions and track them to resolution.
- E02

q1-access-review.xlsx
The register records the Q1 review of production accounts, with reviewers and decisions. Three access exceptions are listed; the register does not include their resolution.
- E03

account-register.csv
Lists production accounts, owners, status, and assigned roles. Administrator accounts are identified separately. It is a point-in-time inventory, not a record of approvals or review completion.
- E04

leaver-access-ticket.pdf
Records a departing employee’s account being disabled and access removed from the identity platform. The ticket includes the request, completion time, and verification by the service desk.

CONTROL MAPPING MATRIX

Framework / control	Requirement	Supporting files
NIST / AC-1	Policy and procedures	E01
NIST / AC-2	Account management	E01, E02, E03, E04
NIST / AC-6	Least privilege	E01, E02, E03
ISO / A.5.15	Access control	E01
ISO / A.5.16	Identity management	E01, E03
ISO / A.5.18	Access rights	E01, E02, E04
ISO / A.8.2	Privileged access rights	E02, E03
NIST / PS-4	Personnel termination	E04

AC-2 is the assessed control in this report. The other seven rows show evidence relevance; they do not imply a maturity or conformity result.

What to carry forward

OPEN / AC-2 / EXCEPTION FOLLOW-UP

Three review exceptions need verified closure.

The review register does not record how the three access exceptions were resolved. The missing records limit support for a consistently defined process. They do not establish that the exceptions were never resolved.

RECOMMENDED FOLLOW-UP

Retain a small set of review measures

Record planned and completed review dates, overdue reviews and exception age. Use those records to establish whether the defined process is operating within its agreed expectations.

Keep closure evidence beside each exception

Link the access change or closure ticket to the review decision. This makes the resolution inspectable without relying on later verbal confirmation.

Prepare the next assessment from current records

Refresh the account population, include the latest completed review and retain the relevant leaver records. Compare them with the earlier versions before revising the conclusion.

CONTEXT STILL TO ESTABLISH

Three access exceptions lacked recorded resolutions.

The register identifies three exceptions without closure records. Verify their resolution with the system owner, record the supporting access changes, and establish whether the same review process is used consistently.

NEXT REVIEW

Confirm whether performance measures and linked closure records have become part of the review process. Retain the current evidence alongside the resulting version.