C4SAM

WHITEPAPER · VERSION 1.0 DRAFT · NOVEMBER 2026

Identity Governance

From accounts to accountable access

How C4SAM connects people, technical identities, ownership and recertification across shared directories, and carries decisions from HR events into controlled change

Audience: CIO, CISO, IT Operations, Internal Audit | **Scope:** Executive and operating model | **Version:** 1.0 draft · November 2026

> **Positioning statement —** C4SAM Identity Governance is a visibility, accountability and execution layer. It does not replace Active Directory, Entra ID, the HR system, SAP or the ticketing system. It reads them, resolves every account to a person or an owner, lets humans confirm what may stay, and carries approved decisions back into the target systems under controlled conditions.

Contents

Document purpose and important qualification

1. Executive summary
- 1.1 Benefits by stakeholder

2. Why account-centric administration breaks down
- 2.1 Ten questions most organizations cannot answer
- 2.2 The two hardest cases

3. The C4SAM identity model
- 3.1 The person as the unit
- 3.2 Matching rules and the clarification list
- 3.3 The identity graph

4. Non-human identities
- 4.1 Inventory
- 4.2 Ownership with two owners
- 4.3 Expiry, use and orphaning

5. Ownership and recertification
- 5.1 Owner proposals from the source systems
- 5.2 Campaign types and baseline intervals
- 5.3 Decisions, revocation and evidence

6. Lifecycle from the HR system
- 6.1 Event, rule, plan, approval, execution
- 6.2 Mover and leaver
- 6.3 Writeback and the closed loop

7. Shared directories and tenants

8. Read before write

9. Captain Sam and sovereign AI

10. The operating model
- 10.1 Roles
- 10.2 Decision cadence

11. Governance, control mapping and limitations
- 11.1 Control mapping
- 11.2 Limitations

12. Implementation
- 12.1 Scoping dimensions
- 12.2 Five phases

13. Measurement

14. Three scenarios

15. Recommendations for CIOs and CISOs

A. Appendix: connector and permission reference

B. Appendix: audit event contract (excerpt)

C. Appendix: baseline policy template

D. References

E. Appendix: glossary

F. Appendix: capability maturity matrix

About C4SAM

Document purpose and important qualification

This whitepaper explains the C4SAM Identity Governance approach for senior executives, security leaders, IT operations and audit functions. It describes the business problem, the identity model, the ownership and recertification process, the HR-driven lifecycle, the handling of organizations that share one directory, the governance controls, and a phased implementation.

> **Important qualification**
>
> The capabilities in this paper are labeled by maturity. Production means in use on live data in the C4SAM Cockpit. Reference means implemented and demonstrated on reference or laboratory data and adapted per installation. Roadmap means designed and scheduled, built on customer request. The capability maturity matrix in Appendix F is authoritative. Framework references to BSI IT-Grundschutz, NIST, ISO/IEC 27001 and NIS2 describe which evidence the platform supports. They are not compliance determinations; those remain the responsibility of the organization and its auditors.

All default values described here (review intervals, validation periods, matching rules, approval paths) are the C4SAM baseline policy as of November 2026. Each organization starts from the baseline and adapts it to its own requirements. Screenshots show the C4SAM reference installation with laboratory data; names and addresses are pseudonymized.

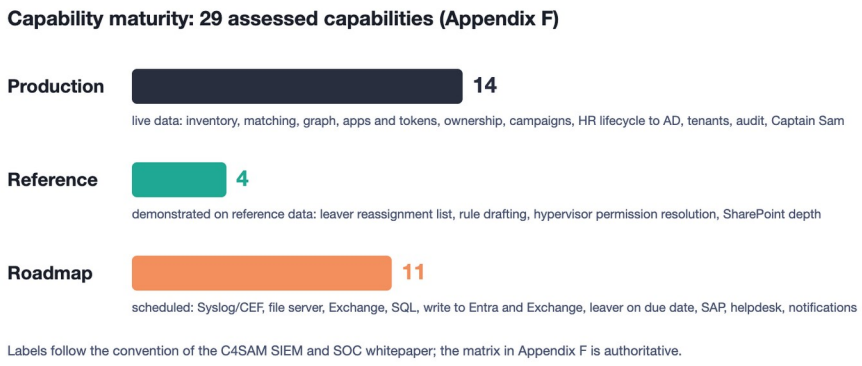


Figure 1 — Maturity of the 29 assessed capabilities: 14 production, 4 reference, 11 roadmap. The matrix in Appendix F lists every capability.

1. Executive summary

The question that access management programs actually need to answer

Most organizations do not lack identity data. They lack the connection between it. Accounts live in Active Directory, Entra ID, GitLab, SAP and a dozen applications. People live in the HR system. Ownership lives in spreadsheets, if anywhere. Nobody can quickly say which accounts belong to one person, who owns a service account, whether that owner still works here, or who can effectively read a given folder. The result is slow answers, orphaned privilege, and audit evidence that has to be rebuilt by hand from tickets and e-mails.

C4SAM Identity Governance connects these sources in one model. Connectors read directories, cloud tenants, the HR system, business applications and infrastructure. Every account, token, application registration and shared resource is resolved to a person or to a named owner. Where resolution is ambiguous, the case goes to a clarification list instead of a wrong assignment. Owners are proposed from the source systems and confirmed by humans. Recertification campaigns run once or recurring, and every decision is recorded with time, person and reason. Joiner, mover and leaver events from the HR system turn into plans that wait for approval before anything is written.

Three properties make the approach different. First, the **person is the unit**, not the account; responsibility is assigned to people, and the model knows when a person changes role or leaves. Second, **non-human identities are first-class citizens**: service accounts, API tokens, enterprise applications, client secrets and automations get the same inventory, ownership and review as personal accounts. Third, the platform **reads before it writes**: transparency and confirmation come first, write access is enabled per target system after a dry-run period, and every write runs through a plan that was approved.

The goal is not another directory. The goal is one accountable picture that answers, for every account and every right: whose is it, who confirmed it, and when was that last checked.

> **Core message for leadership**
>
> Identity governance fails when it starts with provisioning. It succeeds when it starts with ownership. C4SAM establishes who is responsible for every identity, human or technical, before it automates anything.

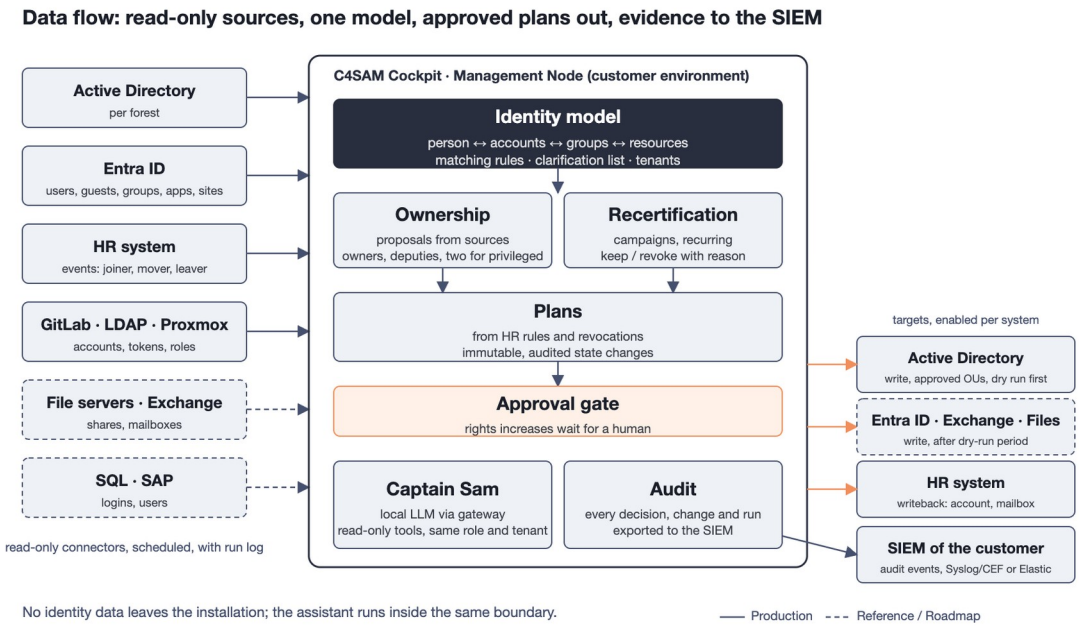


Figure 2 — Data flow: read-only connectors feed one identity model inside the customer's Cockpit; ownership and recertification produce plans that pass an approval gate before any write; audit events go to the customer's SIEM. Dashed sources and targets are roadmap.

1.1 Benefits by stakeholder

Stakeholder	Primary benefit
CISO	Orphaned privilege, unowned technical identities and expiring secrets become visible and reviewable; evidence for NIS2 and ISO 27001 is produced in operation
CIO	One platform for identity visibility, recertification and lifecycle, operated on the same Cockpit as monitoring and automation; no second data model
IT Operations	Fewer tickets for access questions, provisioning from HR events instead of manual steps, revocations as approved plans instead of ad-hoc changes
HR	The HR system stays the leading source; the IT side reports back account and mailbox, and departures trigger a controlled process
Business and resource owners	Review tasks arrive with context (who, since when, used when), decided in a portal or in conversation with the assistant

Stakeholder	Primary benefit
Internal Audit and auditors	Campaign reports, revocation lists, approval trails and audit events exportable to the SIEM; the question "who had access in March" becomes a query

2. Why account-centric administration breaks down

The account is the wrong unit of accountability

Directory administration is built around accounts. Accounts are created, grouped, granted and, eventually, disabled. This works for a single directory with a few hundred users. It stops working when a person holds six accounts across four systems, when half of the privileged identities are technical, and when ten organizations share one Active Directory.

2.1 Ten questions most organizations cannot answer

The following questions come up in nearly every assessment. Each has an owner somewhere in the organization. Very few can be answered in ten minutes.

#	Question	Why it is hard today
1	Who has access to what, across all systems?	Each system knows a part; none knows the person
2	How many accounts belong to one person?	No system carries the employee number consistently
3	Which service accounts, API tokens, app registrations and client secrets exist?	Created by many hands, inventoried by none
4	Who owns them, and is that person still here, in the same role?	Ownership lives in spreadsheets without a link to HR
5	What happens to a person's technical identities when they leave?	Leaver processes disable the user account and stop there
6	Who is an administrator, by which path?	Nested groups, roles and app permissions hide the path
7	Who sees across organizational boundaries?	Shared directories have no notion of organization
8	Who can effectively read folder X, or stop virtual machine Y?	Inheritance and propagation require resolution, not listing
9	Can we show the auditor who had access, who approved it and when it was reviewed?	Evidence is reconstructed from tickets and mails
10	What happens when a token lands in a public repository?	Nobody can say whose it is or what it can do

2.2 The two hardest cases

Two cases deserve special attention because conventional tooling handles neither.

The identity that works at night. Service accounts, API tokens, application registrations, certificates, shared mailboxes and automations have no employee number, no manager and no leaving date. They are created for a project and outlive it. Their permissions accumulate because nobody reviews them, and their secrets expire without warning because nobody owns the calendar. In most environments the number of technical identities exceeds the number of people, and the number with a known owner is a small fraction.

The owner who left. Ownership recorded once is ownership lost. People change departments, roles and employers. A service account whose owner left two years ago keeps running with the rights it had. When something breaks, or when an auditor asks, the organization discovers that the only person who knew what the account does is no longer reachable. The failure is not that the owner was never recorded. It is that nothing connected the record to the HR event that invalidated it.

> **Practice note: counting technical identities**
>
> A useful first exercise is to count. In Entra ID alone: app registrations, enterprise applications, service principals and their credentials. In Active Directory: accounts with no HR person, accounts with passwords that never expire, accounts with a last logon older than 90 days. In source control and automation: personal access tokens and their owners. The totals are usually the first moment leadership understands the size of the unowned estate.

3. The C4SAM identity model

One person, all accounts; one resource, one owner

3.1 The person as the unit

The model starts from the HR system as the leading source for people: employee number, organizational unit, manager, start and end date, employment class (employee, external, guest). Every account from every connector is matched to a person. Accounts that belong to no person are not discarded; they become findings with their own workflow.

The result is a People view: one row per person with HR identity, organizational unit, class, accounts per source and owner roles. From the person, the Explorer opens the graph: directory accounts, application accounts, group memberships, project access, owned resources. The People view and the Explorer are production capabilities; they are the entry point for every access question.

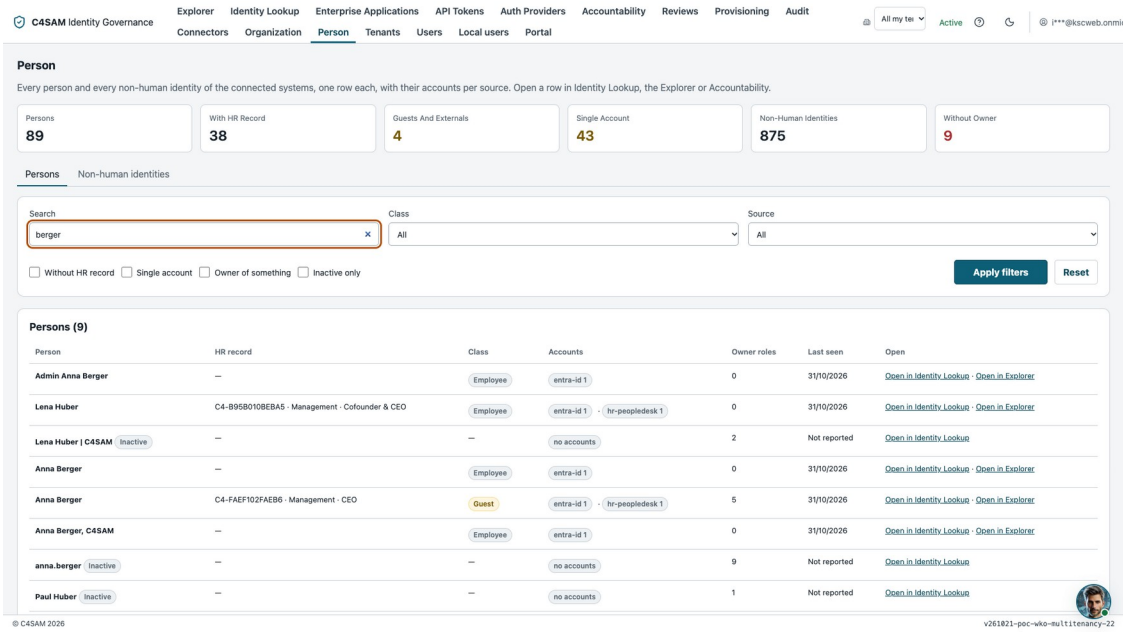


Figure 3 — The People view: one row per person with HR record, class, accounts per source and owner roles. Several rows for one surname show why the clarification list exists: matching is confirmed, not assumed.

3.2 Matching rules and the clarification list

Matching combines deterministic and rule-based steps: employee number carried in a directory attribute, verified e-mail, naming conventions, and explicit links set by an administrator. Each match carries a method and a confidence. Ambiguous

or conflicting matches go to a clarification list rather than being forced. The list is a work queue with an owner, and its size is a quality metric reported in the pilot.

Duplicate detection runs before account creation in the lifecycle (Section 6): a joiner whose name matches an existing person is flagged, not provisioned blindly.

3.3 The identity graph

Accounts, people, groups, applications, resources and credentials are nodes; membership, authentication, ownership and access are edges. The graph is what makes path questions answerable: who is an administrator, by which path; who effectively has access to a resource, through which groups. Privileged flags, first and last seen, and source identifiers are carried on the nodes and shown in the Explorer. The graph is production for directory, cloud, HR and source-control sources; resolution of effective permissions on infrastructure resources is reference (Appendix F).

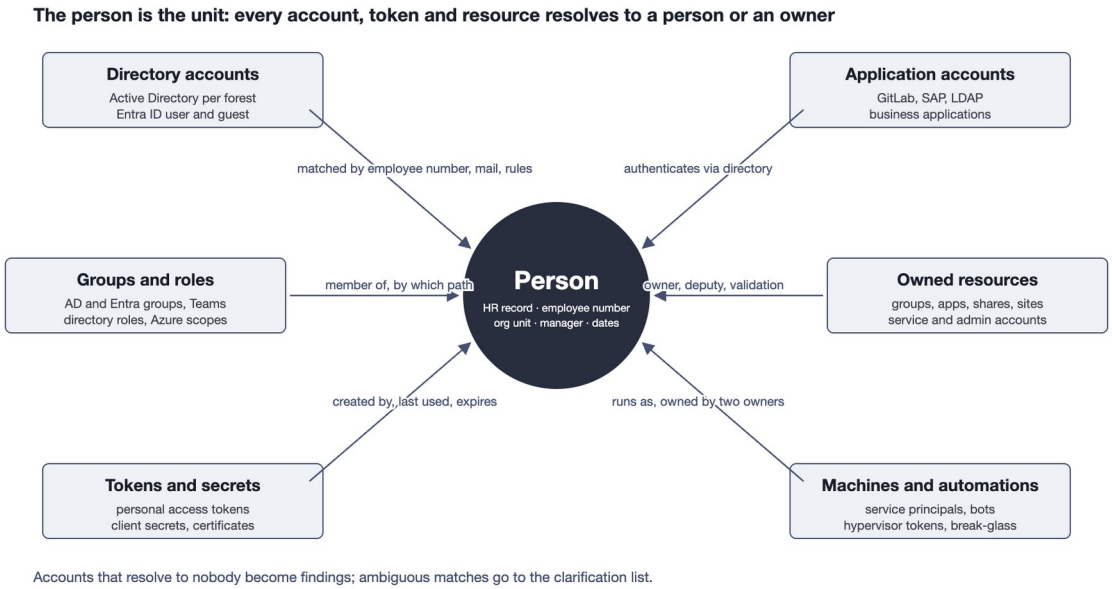


Figure 4 — The identity model: the HR-anchored person at the center, with directory and application accounts, groups and roles, tokens and secrets, owned resources and machine identities resolved to it.

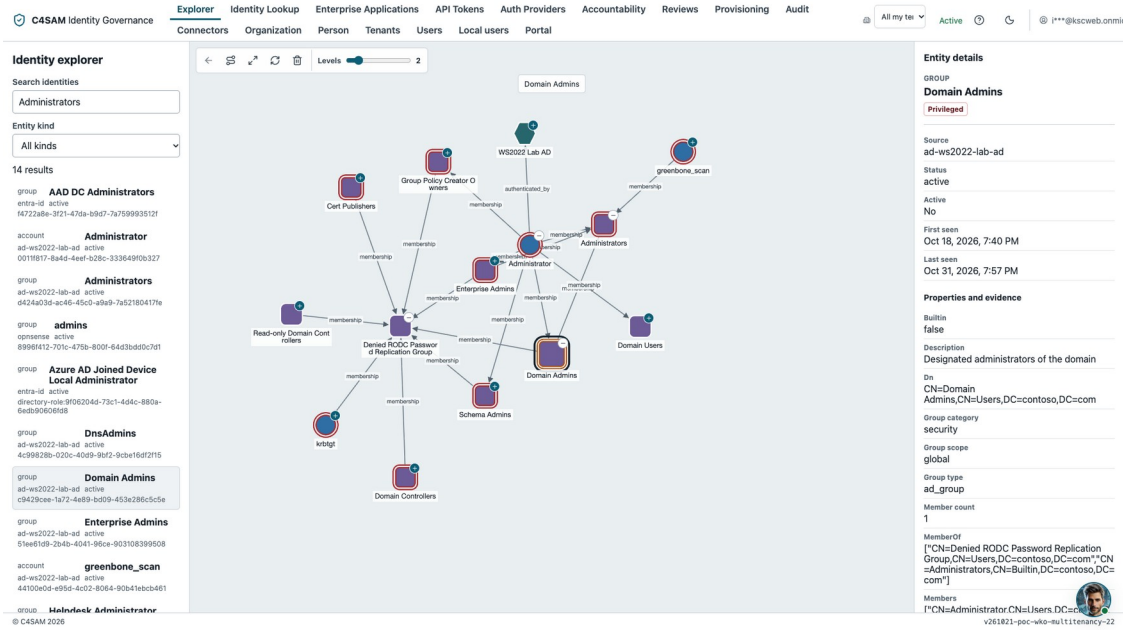


Figure 5 — The Explorer resolves the path to privilege: the Domain Admins group with its nested memberships, the Administrator account and the directory it authenticates against, two levels deep.

4. Non-human identities

Inventory, ownership, expiry

4.1 Inventory

The platform collects technical identities with the same connectors that collect personal accounts, and treats them as resources with their own lifecycle:

Identity type	Source	Collected attributes
Service and admin accounts	Active Directory, Entra ID	Creator where known, last logon, password policy, group memberships, privileged flag
Application registrations and enterprise applications	Entra ID	Owners, permissions granted, client secrets and certificates with expiry, sign-in activity
Personal access tokens	GitLab, Cockpit API	Owner, scopes, expiry, last use, "unused 90 days" flag
Shared and functional mailboxes	Exchange Online	Full-access and send-as permissions, owner proposal (roadmap connector)
Machine identities	Hypervisors, automation	Tokens and roles on pools and paths, propagation (reference)
Break-glass accounts	Directory, Cockpit	Owner, last use, reason log

Expiring credentials of enterprise applications were the original trigger for this capability in the C4SAM environment: a secret that expired without a responsible person. Since then the application list is sorted by expiry by default.

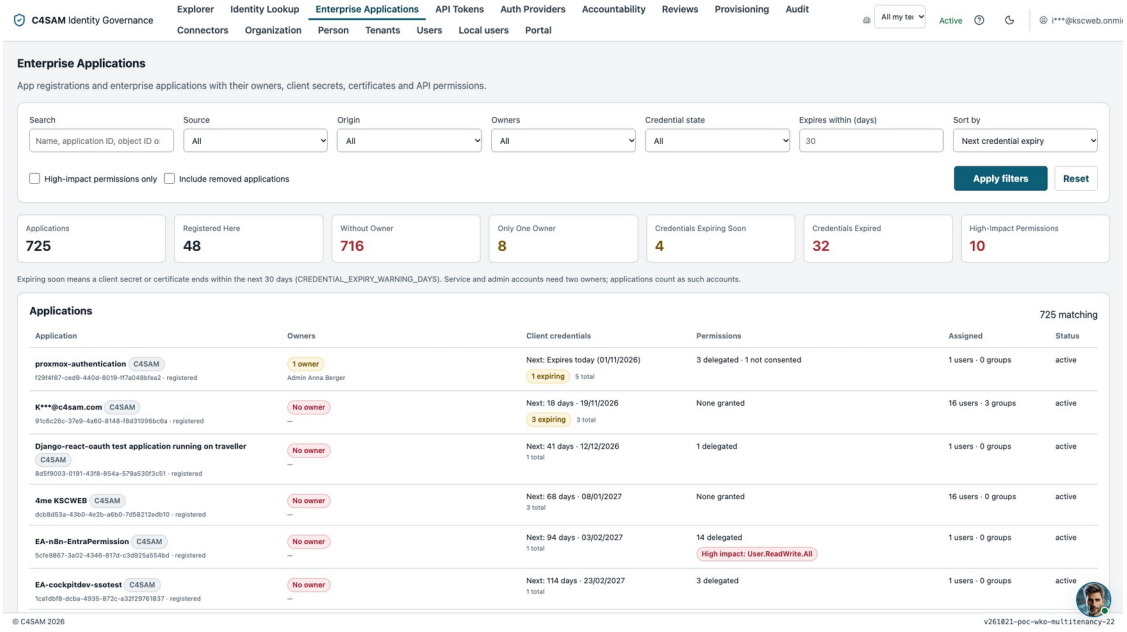


Figure 6 — Enterprise applications sorted by next credential expiry: 716 of 725 without an owner, credentials expiring within 30 days, high-impact permissions flagged.

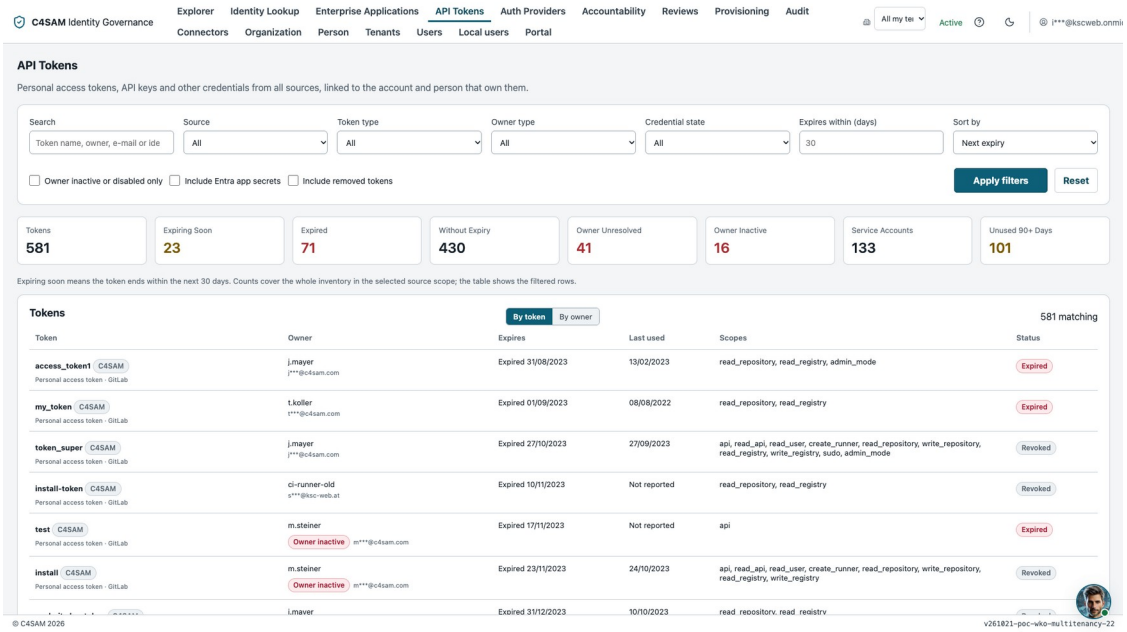


Figure 7 — API tokens across sources with owner, expiry, last use and scopes; counters for unresolved and inactive owners and for tokens unused for 90 days.

4.2 Ownership with two owners

Every technical identity needs an owner. Privileged technical identities, service accounts with administrative rights, and break-glass accounts need two owners

and a validation interval. The baseline is 90 days; organizations choose between quarterly and semi-annual validation. Ownership is tied to the HR person, not to a name string. When the HR system reports a role change or a departure, every resource owned by that person is flagged, and a successor is proposed from the organizational chart.

4.3 Expiry, use and orphaning

Three conditions turn a technical identity into a finding: a credential that expires within a configurable window, a token or account unused for a configurable period, and an identity without a living owner. Findings appear in the findings report of the pilot and feed the campaigns in Section 5. A token found in the wrong place can be resolved in minutes: whose it is, what it can do, where it was last used.

5. Ownership and recertification

Responsibility nobody has confirmed is not responsibility

5.1 Owner proposals from the source systems

Owner assignment does not start from an empty list. Proposals come from the source systems: group managers in Active Directory, application owners and sponsors in Entra ID, creators of tokens, site administrators in SharePoint, usage patterns on shares. The Accountability view lists resources with their proposed owners and the owner state. An administrator or the proposed owner adopts, delegates or rejects. Without an owner there is no reviewer, so resources without owners are the first campaign target.

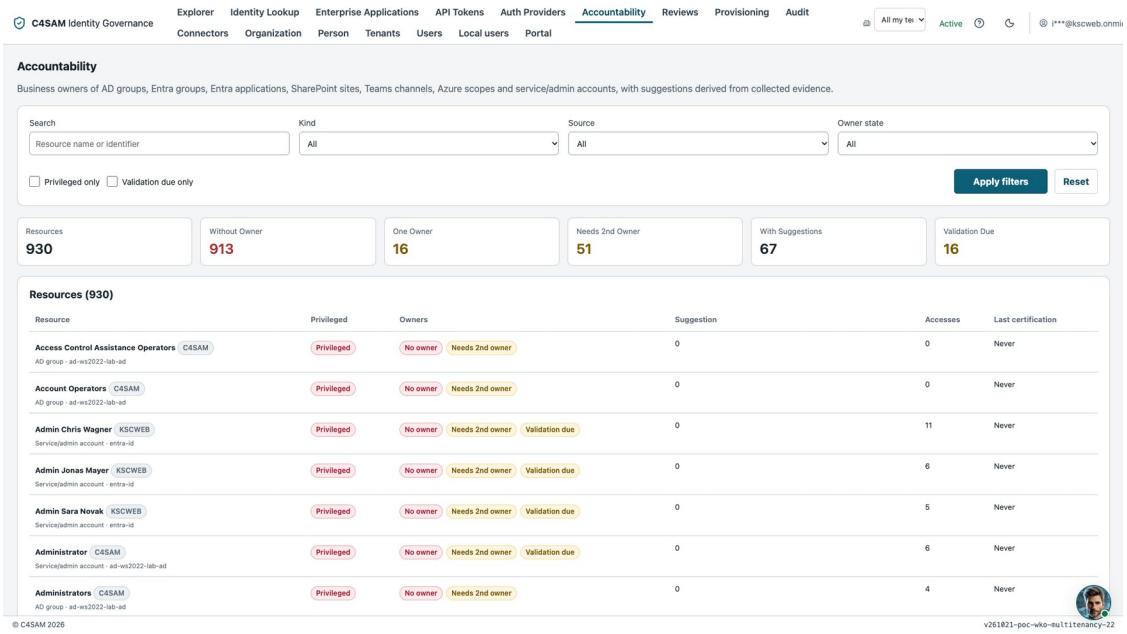


Figure 8 — Accountability: privileged groups and service or admin accounts with owner state, second-owner requirement and validation due; suggestions come from collected evidence.

5.2 Campaign types and baseline intervals

Campaign type	Scope	Baseline interval	Reviewer
Guests and externals	Entra guest accounts per organization	60 days, recurring	Owner, else sponsor, else administrator

Campaign type	Scope	Baseline interval	Reviewer
Service and admin accounts	Privileged and technical accounts	90 days, two owners	Both owners
Privileged groups	Directory and Entra groups with administrative effect	Quarterly	Group owner
Enterprise applications	App registrations and service principals	Quarterly	Application owner
Teams and channels, SharePoint sites	Collaboration resources, top level	Semi-annual	Site or team owner
Shares and mailboxes	File server shares, shared mailboxes	Semi-annual (roadmap connector)	Resource owner
Azure scopes	Role assignments on subscriptions and resource groups	Quarterly	Scope owner

Recurring campaigns schedule themselves. A run with nothing to review closes itself and remains as evidence. Reviewer selection, escalation and deputy rules are policy.

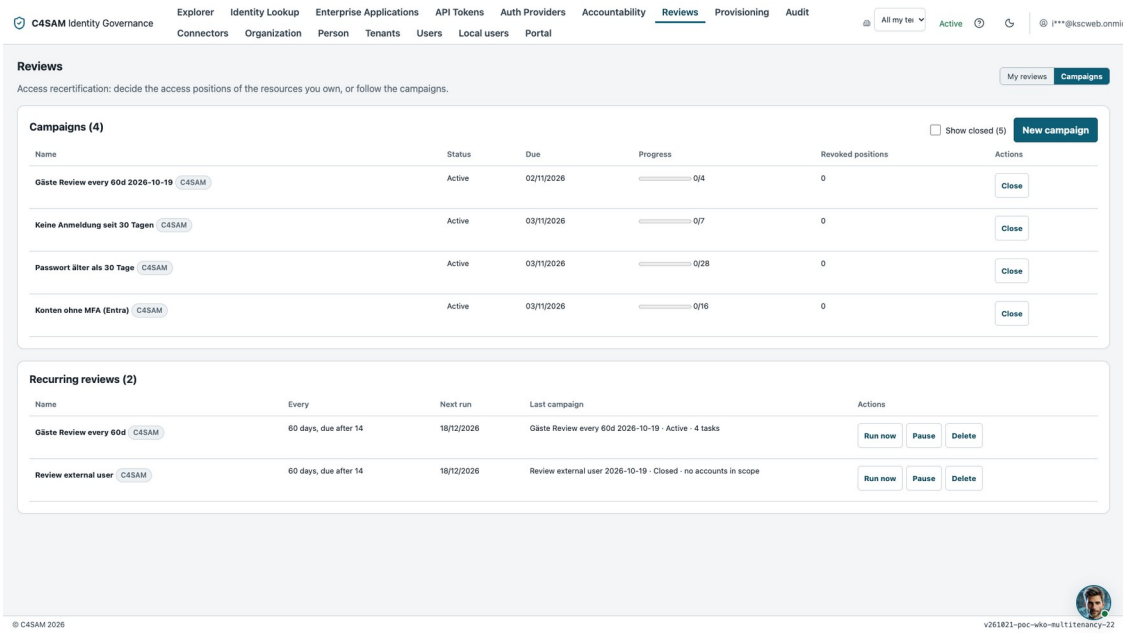


Figure 9 — Campaigns and recurring reviews: a guest review every 60 days, due after 14, next run scheduled; closed runs remain as evidence.

5.3 Decisions, revocation and evidence

Each task is decided as keep or revoke with a reason. Revocations are collected in a revocation list. Where write access to the target system is enabled (Section 8), the revocation becomes an approved plan and is executed; where it is not, it is a documented order carried out by an administrator and confirmed back. Either way the campaign report holds the decision, the decider, the time and the outcome. Reports and lists export as CSV, and every decision is an audit event (Appendix B).

> **Practice note: honesty about revocation**
>
> A revocation is not done when the reviewer clicks. It is done when the right is gone in the target system. C4SAM shows both states separately: decided and executed. Organizations should report the gap between them; it is the most useful indicator of whether the process has teeth.

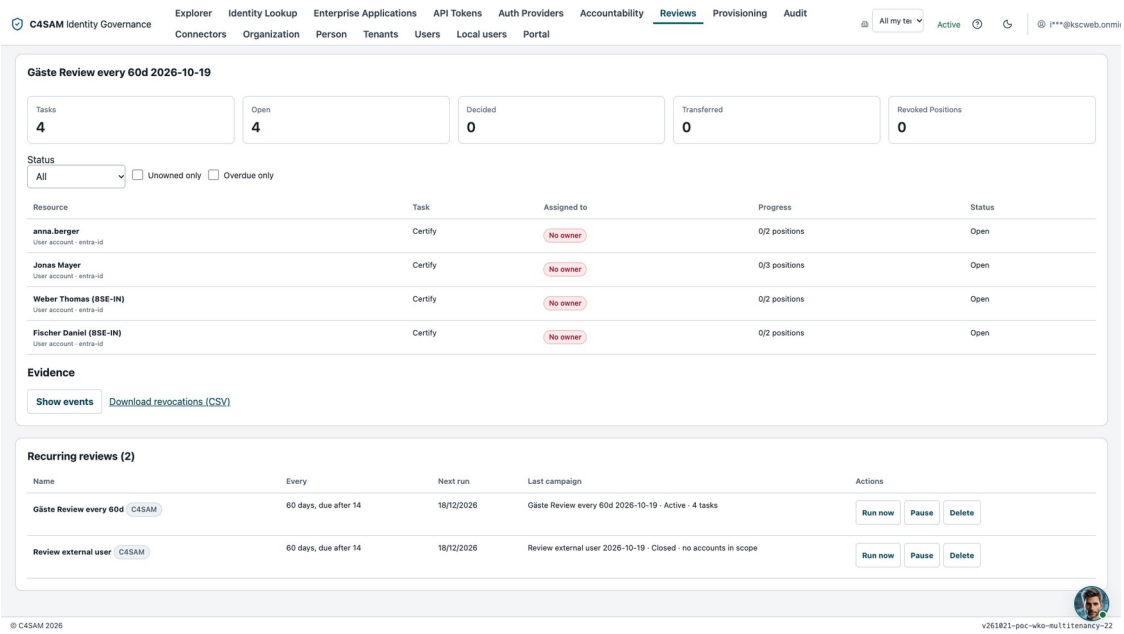


Figure 10 — One campaign: tasks per resource, assignment, progress per position, and the evidence section with event log and revocation list export.

6. Lifecycle from the HR system

Nothing is written without a plan, and no plan without approval

6.1 Event, rule, plan, approval, execution

The HR system emits events: employee created, changed, left. Rules match on organizational unit, employment class and attributes. A matching rule produces a plan: the exact actions in the target systems (create account, add to groups, set attributes, create mailbox). The plan waits for approval in the portal. Rights-increasing plans always require approval; the approver sees the rule, the person and every action. After approval, the connector executes the plan, and the result links the new account to the HR person in the identity model.

The sequence is deliberately visible at every step. Nothing is written by a rule alone. Plans are immutable once created; their state changes (planned, approved, executing, done, failed with reason) are audit events.

6.2 Mover and leaver

A department change adjusts group memberships according to the rules of the new unit and removes those of the old one. A departure disables the account on the effective date and produces a second list: every service account, token, application and shared resource owned by the departing person, each needing a new owner. The second list goes to the manager with a deadline. The lifecycle does not end at the user account.

Removals in mover and leaver plans take effect without an approval step by default, because delay is the risk; organizations can require approval for them as policy.

6.3 Writeback and the closed loop

After an account is created, the platform writes the account name and mailbox back to the HR record, optionally after approval. HR therefore sees what IT provisioned, and the person's record is complete in the leading system. The loop closes where it started.

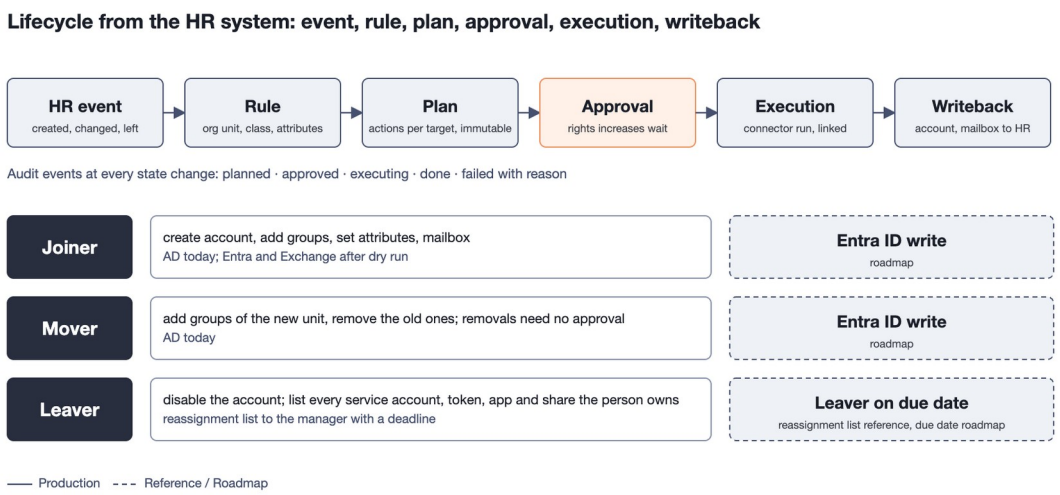


Figure 11 — The lifecycle pipeline: HR event, rule, plan, approval, execution, writeback, with joiner, mover and leaver handling per target. Solid elements are production, dashed ones roadmap.

7. Shared directories and tenants

Many organizations, one directory, hard separation

Groups with subsidiaries, chambers, public administrations, hospital networks and universities share directories and cloud tenants. The platform models each organization as a tenant with hard separation in the database: each tenant sees only its identities and resources, roles apply per tenant, and connectors to shared sources carry assignment rules (a guest account belongs to the inviting organization, a user with a given domain belongs to that organization, an account in a given organizational unit belongs to the matching tenant). Accounts that no rule assigns go to a clarification queue at the shared level.

A break-glass view across all tenants exists for emergencies. It requires a reason, is time-limited, and is logged as an audit event with the identity of the person who used it. Multi-tenancy is production; it was built before recertification and provisioning because the data model of a shared estate decides everything that follows.

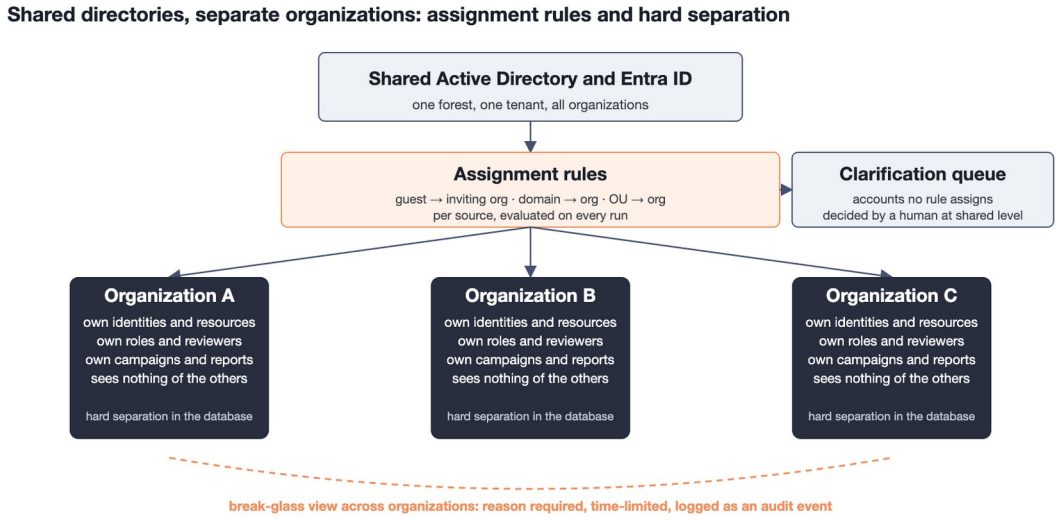


Figure 12 — Shared directories, separate organizations: assignment rules map accounts of a shared directory to tenants; unassigned accounts go to a clarification queue; break-glass access across tenants is justified, time-limited and logged.

8. Read before write

Transparency first, confirmation second, execution last

All connectors start read-only. The platform earns write access per target system, in this order:

1. **Read.** The connector collects on a schedule with a run log; coverage is declared, not assumed.
2. **Confirm.** Owners are assigned and the first campaigns run; the organization sees whether the picture is trustworthy.
3. **Dry run.** Write actions are generated as plans and shown with a preview, but not executed, for a defined period and a minimum number of actions without deviation.
4. **Enable.** Write access is switched on for that target system, with a separate write account tested by connection check, restricted to approved organizational units, with administrative groups excluded from automatic handling.

Write to Active Directory is production under these rules. Write to Entra ID, Exchange and file servers follows the same path and is roadmap (Appendix F). Until a target is enabled, revocations and provisioning for it remain documented orders.

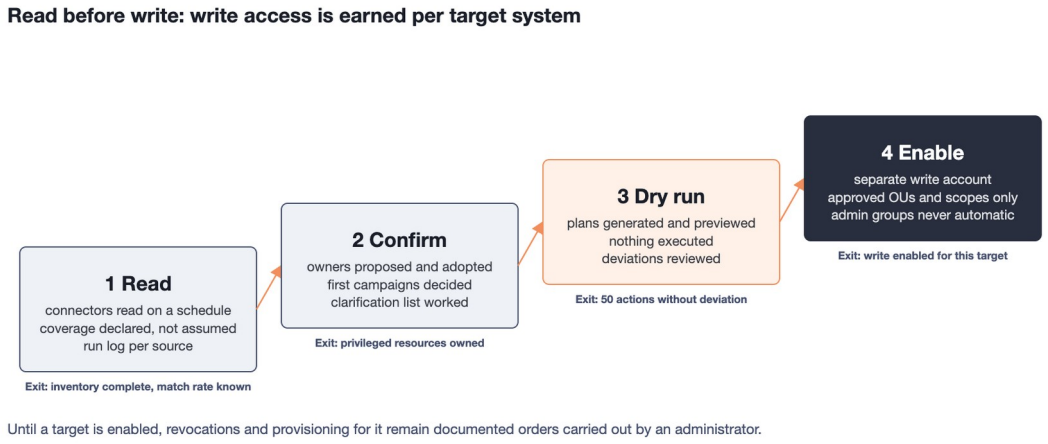


Figure 13 — Read before write: four steps per target system, each with an exit criterion, from read-only collection to enabled write access.

9. Captain Sam and sovereign AI

Ask the system instead of searching menus

Captain Sam is the assistant inside the Cockpit. It answers questions about access ("which privileged groups have no owner"), helps with operation from the product manual, and drafts rules ("everyone in Engineering gets a directory account and the Engineering group") that a human reviews and creates. Three properties matter for governance:

- It runs on a language model in the customer's environment, reached through the Cockpit's LLM gateway. No identity data leaves the installation.
- It has read-only tools and sees only what the signed-in person sees: the same role, the same tenant, addresses masked as in the API.
- It knows the manual and the platform's limits; when it does not know, it says so.

Captain Sam is production for questions and manual help, reference for rule drafting, and roadmap for agentic pre-triage of findings. Creating, approving and executing remain human actions.

10. The operating model

Shared accountability across security, HR, IT operations and resource owners

10.1 Roles

Role	Responsibility
Identity governance owner (security)	Policy: matching rules, campaign intervals, approval paths; review of findings
HR process owner	Quality of the leading source; event timeliness; employment classes
IT operations	Connectors, write accounts, dry-run review, execution of documented orders
Resource owners	Adoption of ownership, review decisions, deputies
Tenant administrators	Assignment rules and roles for their organization
Internal audit	Independent use of reports and audit events; sampling of decisions

10.2 Decision cadence

Weekly: clarification list and findings with the operations team. Monthly: campaign completion, revocation gap, expiring credentials with the security owner. Quarterly: policy review, maturity matrix, write-access enablement decisions with the steering group. Annually: control mapping review with audit.

11. Governance, control mapping and limitations

11.1 Control mapping

The platform supports evidence for the following controls. It does not certify compliance with them.

Capability	BSI IT-Grundschutz	NIST CSF 2.0 / SP 800-53	ISO/IEC 27001:2022	NIS2
Person-centric inventory of all accounts	ORP.4.A1, A7	PR.AA-01; AC-2	A.5.16 Identity management	Art. 21(2)(i)
Ownership of technical identities, two owners for privileged	ORP.4.A5, A8; OPS.1.1.2.A21	PR.AA-01, PR.AA-05; AC-2(7), AC-6	A.5.16, A.8.2 Privileged access rights	Art. 21(2)(i)
Recertification campaigns with evidence	ORP.4.A3, A12	PR.AA-05; AC-2(3), AC-2(j)	A.5.18 Access rights review	Art. 21(2)(i), (f)
HR-driven joiner, mover, leaver	ORP.4.A2, A3	PR.AA-01; AC-2(1), PS-4, PS-5	A.5.18, A.6.5	Art. 21(2)(i)
Credential expiry and token inventory	ORP.4.A8, A23	PR.AA-01; IA-4, IA-5	A.5.17 Authentication information	Art. 21(2)(j)
Effective access resolution and privileged paths	ORP.4.A9, A11	PR.AA-05; AC-6(1), AC-6(9)	A.5.15, A.8.2, A.8.3	Art. 21(2)(i)
Tenant separation, break-glass logging	ORP.4.A10; OPS.1.1.2.A6	PR.AA-05; AC-3, AU-2	A.5.15, A.8.3	Art. 21(2)(i)
Audit trail and SIEM export	OPS.1.1.5	DE.CM-03; AU-2, AU-6, AU-12	A.8.15 Logging	Art. 21(2)(b), (f)

References are to the 2023 IT-Grundschutz-Kompendium, NIST CSF 2.0 (2024), NIST SP 800-53 Rev. 5, ISO/IEC 27001:2022 Annex A, and Directive (EU) 2022/2555. Organizations map to their own control catalog; the table is a starting point.

11.2 Limitations

- Matching quality depends on the HR system carrying stable identifiers and on directories storing them. Where they are missing, the clarification list grows and manual linking is required.
- SharePoint is read at site and library top level by design; deeper folder permissions create review volumes nobody completes.
- OneDrive reading is built but off by default; it requires a data-protection decision.
- Effective-permission resolution on infrastructure (hypervisors, file servers) is reference and roadmap respectively; results depend on the completeness of group and role data.
- Write access to cloud and collaboration targets is roadmap; until enabled, revocations there are documented orders.
- Captain Sam answers from collected data as of the last run; it cannot query points in time, send mail or act on targets.
- Guest invitation and blocking require write access to Entra ID and follow its enablement.

12. Implementation

12.1 Scoping dimensions

Number of organizations and forests; HR system interface (REST, events, export) and identifier quality; cloud tenant layout and permission model for read access; number of file servers, shares and shared mailboxes; business systems in scope; SIEM product and protocol; hosting of the Management Node; approval and security review lead times.

12.2 Five phases

Phase	Content	Exit criteria
P1 Pilot	Cockpit installed in the customer environment; directories, cloud tenant and HR connected read-only; tenants configured; first findings report	100 % of directory and tenant accounts inventoried; at least 95 % of active accounts matched to a person; tenant separation tested; findings report delivered
P2 Governance	Owner workshops; owner proposals confirmed; campaigns for guests, service and admin accounts, privileged groups and applications; SIEM export; notifications	At least 90 % of privileged resources with owners; 100 % of admin accounts with two owners or open task; first campaign round at least 80 % complete in time; audit events in the SIEM
P3 More sources	File servers (effective rights), Exchange (shared mailboxes), SharePoint depth, SQL, hypervisors; adaptation to naming and share structure; campaigns for shares and mailboxes	100 % of named shares and mailboxes as resources; effective-access report verified on samples; runs stable for two weeks
P4 Write access	Entra ID as provisioning target; revocation as action; portal requests executed; leaver on effective date; Exchange and file servers writing; per target: dry run, connection test, approval process, enablement	Dry-run protocol per target with at least 50 actions without deviation; joiner, mover, leaver end to end; revocation executed within 24 hours; no write outside approved scope

Phase	Content	Exit criteria
P5 Business systems	SAP user management, helpdesk reset and unlock with evidence, telephony, license assignment	End-to-end tests in the business systems; helpdesk actions with audit entry

Operations after the pilot are optional and follow the Cockpit operating model.

13. Measurement

Indicator	Definition	Target direction
Match rate	Active accounts resolved to a person	Up; pilot target 95 %
Unowned privileged resources	Privileged groups, apps and accounts without a confirmed owner	Down to zero
Owner validity	Owners whose HR status is active and role unchanged since confirmation	Up
Campaign completion	Tasks decided within the campaign window	Up; baseline 80 %
Revocation gap	Time and count between decided and executed revocations	Down
Expiring credentials handled	Credentials renewed or retired before expiry	Up
Joiner lead time	HR event to usable account	Down; target under one hour excluding approval
Leaver completeness	Technical identities of leavers reassigned within the deadline	Up
Clarification backlog	Open items on the clarification list	Down
Audit answer time	Time to produce access history for a person or resource	Down to minutes

14. Three scenarios

A token in a public repository. A developer's personal access token appears in a public repository. The security team searches the token identifier. The platform shows the owner, the scopes, the last use and the systems reached. The token is revoked at the source, the event is an audit entry, and the owner's other tokens are listed for review. Elapsed time: minutes.

The owner who resigns. An infrastructure engineer who owns 23 service accounts, four application registrations and two break-glass accounts gives notice. The HR event produces the leaver plan and the reassignment list. The manager assigns successors from the proposals within the deadline; two accounts nobody claims are disabled after a dry-run check of their last use. Nothing breaks on the last day because every automation has a new owner before then.

The auditor's question. An auditor asks who had access to the payroll share in March, who approved it and when it was last reviewed. The campaign report of the share, the decision history and the effective-access snapshot answer the question in one export. The follow-up question, whether the three externals on the list were reviewed in the guest campaign, is answered from the same system.

15. Recommendations for CIOs and CISOs

1. Make the person the unit of accountability. Require that every account, human or technical, resolves to a person or a confirmed owner, and measure the share that does not.

2. Treat technical identities as the first review target, not the last. They outnumber people and are least owned.

3. Tie ownership to HR events. An owner who left is not an owner; the process must notice without a human remembering.

4. Start read-only and confirm before you automate. Earn write access per target system with a dry-run record.

5. Separate organizations in the data model, not only in the org chart, if directories are shared.

6. Produce evidence in operation. Campaign reports, approval trails and audit events should be a by-product of daily work, not a quarterly project.

7. Keep the assistant inside the fence: a local model, read-only tools, the same permissions as the person asking.

A. Appendix: connector and permission reference

Connector	Mode	Minimum permissions	Maturity
Active Directory	Read; write optional	Read account per forest; write account restricted to approved OUs	Production
Entra ID (users, guests, groups, Teams, enterprise apps, SharePoint sites, Azure scopes)	Read	Application permissions: User.Read.All, Group.Read.All, Application.Read.All, Directory.Read.All, Sites.Read.All, Reports.Read.All; sign-in activity needs Entra ID P1	Production
HR system (reference: PeopleDesk)	Read events; writeback optional	REST or export with employee number, org unit, dates	Production (reference HR), customer adapter per installation
GitLab	Read	Read API token with user and token scope	Production
LDAP	Read	Bind account	Production
Hypervisor (Proxmox)	Read	API token with audit role	Production inventory, reference permission resolution
Exchange Online	Read; write roadmap	Exchange.ManageAsApp with view-only roles	Roadmap
File servers (Windows)	Read; write roadmap	Read account with share and NTFS read	Roadmap
SQL Server	Read	Login with view server state and definition	Roadmap
SAP	Read; write roadmap	Service user with user administration display	Roadmap

Connector	Mode	Minimum permissions	Maturity
SIEM export	Write events	Syslog/CEF target; Elastic integration existing	Elastic production, Syslog/CEF roadmap

B. Appendix: audit event contract (excerpt)

Every audit event carries: event id, timestamp (UTC), tenant key, actor (person or system), actor role, subject (resource or identity with source identifier), action (proposed, adopted, decided keep, decided revoke, plan created, plan approved, plan executed, plan failed, break-glass used, connector run), reason text, outcome, correlation id (campaign, plan or run). Events are immutable, exportable to the SIEM, and retained per policy.

C. Appendix: baseline policy template

Parameter	Baseline	Range
Guest review interval	60 days	30 to 180 days
Service and admin account validation	90 days, two owners	90 or 180 days
Privileged group and application review	Quarterly	Monthly to semi-annual
Unused credential threshold	90 days	30 to 180 days
Credential expiry warning	30 days	14 to 90 days
Rights-increasing plans	Approval required	Fixed
Rights-removing plans (mover, leaver)	No approval	Approval optional
Dry-run before enablement	50 actions without deviation	20 to 200
Break-glass duration	8 hours with reason	1 to 24 hours
Match confidence for automatic link	High (employee number or verified mail)	Policy

D. References

BSI, IT-Grundschutz-Kompendium, Edition 2023: ORP.4 Identitäts- und Berechtigungsmanagement; OPS.1.1.2 Ordnungsgemäße IT-Administration; OPS.1.1.5 Protokollierung.

NIST, Cybersecurity Framework 2.0, February 2024: PR.AA Identity Management, Authentication and Access Control; DE.CM Continuous Monitoring.

NIST, SP 800-53 Rev. 5, Security and Privacy Controls: AC-2, AC-3, AC-6, AU-2, AU-6, AU-12, IA-4, IA-5, PS-4, PS-5.

NIST, SP 800-63-4, Digital Identity Guidelines (2025).

ISO/IEC 27001:2022, Annex A: 5.15 Access control, 5.16 Identity management, 5.17 Authentication information, 5.18 Access rights, 6.5 Responsibilities after termination, 8.2 Privileged access rights, 8.3 Information access restriction, 8.15 Logging.

Directive (EU) 2022/2555 (NIS2), Article 21(2): (b) incident handling, (f) assessing effectiveness, (i) access control and asset management, (j) multi-factor authentication.

C4SAM, True Risk Priority whitepaper, v1.2, October 2026, for the shared context model.

C4SAM, Unified SIEM and SOC whitepaper, v1.3, July 2026, for the alert pipeline and sovereign AI infrastructure.

E. Appendix: glossary

Term	Meaning
Person	The HR-anchored identity to which accounts and ownership are attached
Account	A login in a source system (directory, application, cloud)
Non-human identity	Service account, token, application registration, certificate, machine identity, functional mailbox
Owner	The person accountable for a resource or identity; privileged resources require two
Campaign	A recertification run over a resource type with tasks, reviewers and a window
Plan	The set of actions derived from a rule for a lifecycle event, awaiting approval
Dry run	Plan generation without execution, used to prove a write path before enablement
Tenant	An organization within a shared installation with hard data separation
Break-glass	Time-limited, logged access across tenants or to emergency accounts
Clarification list	Queue of accounts and matches that need a human decision
Effective access	The resolved result of direct, group, nested, role and propagated permissions

F. Appendix: capability maturity matrix

Capability	Production	Reference	Roadmap
Person-centric inventory (AD, Entra, HR, GitLab, LDAP)	●		
Matching with clarification list, duplicate detection	●		
Identity graph and Explorer	●		
Enterprise applications with credential expiry	●		
Personal access tokens with owner and use	●		
Owner proposals and adoption (Accountability)	●		
Two owners and validation for service and admin accounts	●		
Recertification campaigns, recurring, with evidence	●		
Revocation list and executed revocation (AD)	●		
HR events, rules, plans, approval, execution to AD, writeback	●		
Leaver reassignment list for technical identities		●	
Multi-tenancy with assignment rules and break-glass	●		
Audit events to Elastic	●		
Audit events via Syslog/CEF to any SIEM			●
Captain Sam: questions, manual help	●		
Captain Sam: rule drafting		●	
Captain Sam: agentic pre-triage of findings			●
Hypervisor resources and tokens (Proxmox)	●		
Effective permission resolution on hypervisor		●	

Capability	Production	Reference	Roadmap
File server effective access, campaigns			●
Exchange shared mailboxes, campaigns			●
SharePoint site depth, OneDrive top level		●	
SQL Server roles and logins			●
Write to Entra ID (accounts, groups, guests)			●
Write to Exchange and file servers			●
Leaver on effective date, attribute reconciliation			●
SAP user management			●
Helpdesk reset and unlock with evidence, telephony, licenses			●
E-mail notification and escalation			●

About C4SAM

C4SAM, the Cockpit for Security, Automation and Monitoring of the IT infrastructure, helps organizations understand and secure their digital infrastructure by connecting operational visibility, vulnerability information, business and service context, and controlled response. Identity Governance extends that mission from assets and vulnerabilities to the people and technical identities that hold access, and from finding unowned privilege to confirming and removing it. C4SAM GmbH, Pülslgasse 4a, 1230 Vienna, Austria. office@c4sam.com, c4sam.com.