CAPABILITY BRIEF · 04 / 04

acsense

Compliance & Assurance

Continuous compliance validation, drift detection, and audit-ready evidence for your IAM tenant. Map every change to regulatory frameworks automatically.

Identity is Tier-0 infrastructure. Every employee, application, partner, and AI agent authenticates through it. When configurations drift from compliance baselines, when audit evidence is assembled manually, when NHI activity goes untracked, the consequences compound. Regulatory findings. Audit failures. Unquantified risk.

Identity providers do not validate compliance. They do not map IAM changes to regulatory frameworks, score your compliance posture, or produce audit-ready evidence. Compliance teams assemble it manually, often weeks after a change that already put the organization out of compliance.

Acsense Compliance & Assurance closes the gap. Continuous validation against SOC 2, ISO 27001, DORA, NIS2, NIST SP 800-53, APRA, and FISMA. Every IAM change mapped to regulatory controls automatically.

One platform. Any IDP. Tenant-level compliance assurance from a single control mapping to a full audit report, without manual evidence collection.

Always
Audit-ready compliance posture

7+
Regulatory frameworks mapped

IDP-Agnostic
One compliance baseline, any IDP

> *"Identity providers guarantee their own uptime, not your compliance posture. The compliance evidence gap is the most time-consuming, recurring audit risk in enterprise IAM."*
>
> Reflecting the AWS Shared Responsibility Model

22% of breaches start with stolen credentials. Credential-based breaches take **246 days** on average to identify and contain. Identity attacks rose **32%** in H1 2025.

SOURCES: VERIZON DBIR 2025 · IBM COST OF A DATA BREACH 2025 · MICROSOFT DIGITAL DEFENSE REPORT 2025

Compliance is continuous, but most teams still review annually

Regulatory frameworks like SOC 2, ISO 27001, DORA, and NIST SP 800-53 require continuous evidence that identity controls are enforced. But most IAM teams assemble compliance evidence manually: exporting logs, cross-referencing policies, building spreadsheets. By the time the evidence is ready, the environment has already changed.

Identity providers keep a record of what happened. Turning that record into compliance evidence requires more: mapping changes to regulatory controls, scoring compliance posture continuously, detecting compliance drift before auditors do, and tracking non-human identity activity. Without that layer, the gap between what regulators ask for and what exists is filled by manual labor.

How Acsense Compliance & Assurance works

STAGE 1

Map to Frameworks

Every IAM change automatically mapped to standard frameworks (SOC 2, ISO 27001, DORA, NIS2, NIST, APRA, FISMA) and custom frameworks your team defines.

→

STAGE 2

Validate + Score

Continuous compliance scoring. Drift detection flags deviations from the compliance baseline in real time.

→

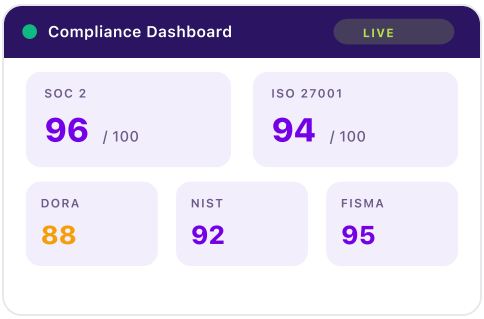
STAGE 3

Report + Remediate

Audit-ready reports on demand. NHI audit trails included. (Coming Soon) Automated remediation for common drift patterns.

Continuous validation, framework by framework

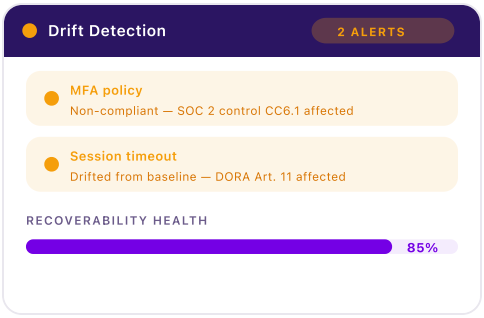
Acsense Compliance & Assurance validates your IAM tenant against regulatory frameworks continuously. Every change is mapped, scored, and documented. Compliance drift is detected automatically. Audit reports are produced on demand, not assembled manually.



Continuous Compliance Validation

Every IAM change is automatically mapped to the regulatory controls it affects. Compliance posture is scored continuously across SOC 2, ISO 27001, DORA, NIS2, NIST SP 800-53, APRA, and FISMA. Deviations are flagged the moment they occur, not weeks later during an audit prep cycle.

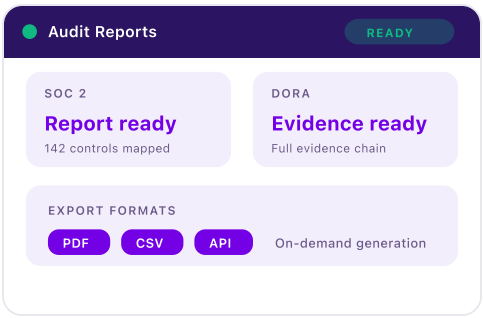
7+ frameworks · Continuous scoring · Auto-mapping



Continuous Drift Detection + Recoverability Health

Detects when IAM configurations drift from the compliance baseline and surfaces the specific controls affected. Recoverability Health scoring validates that the organization can recover to a compliant state at any time, not just that it is compliant right now.

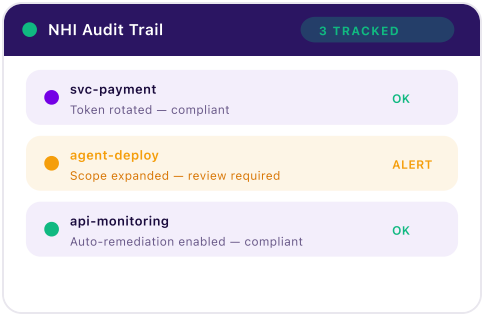
Compliance drift · Recoverability health · Control mapping



Compliance Scoring + Audit Reports

Quantified compliance scores per framework, updated continuously. Audit reports produced on demand with the full evidence chain: change history, control mapping, compliance posture at any point in time. No manual spreadsheets. No last-minute evidence assembly.

On-demand reports · Evidence chain · PDF / CSV / API



NHI Audit Trails

Non-human identities (service principals, API tokens, AI agent bindings) are tracked with the same compliance rigor as human identities. Full audit trails for every NHI change. As your NHI surface grows with AI agents and service principals, every new binding is automatically tracked, audited, and scored against your compliance frameworks.

NHI tracking · NHI surface growth · Agent bindings

Real scenarios. Real assurance.

Compliance & Assurance operates continuously across every IAM object. Four scenarios from real regulated environments. Each at the tenant level, regardless of which IDP is running underneath.

WHEN THIS HAPPENS

SOC 2 auditor asks for IAM change evidence

Acsense: On-demand audit report with full change history, control mapping, and compliance posture at any point in time.

Audit-ready in minutes, not weeks of manual assembly.

WHEN THIS HAPPENS

DORA deadline requires proof of ICT resilience

Acsense: Continuous compliance scoring against DORA controls. Recoverability Health score proves recovery capability. Evidence exported directly.

Regulatory evidence produced continuously, not assembled under deadline pressure.

WHEN THIS HAPPENS

Service principal scope drifts beyond approved access

Acsense: NHI Audit Trail flags the scope expansion. Drift detection identifies the non-compliant state. Automated remediation reverts to approved scope.

NHI compliance maintained without manual intervention.

WHEN THIS HAPPENS

Weekend config change violates MFA policy baseline

Acsense: Continuous drift detection flags the deviation. Compliance score drops and alerts fire. One-click remediation restores the compliant config.

Compliance restored before the next business day.

Why Acsense for Compliance & Assurance

Continuous, not periodic

Compliance is validated every time something changes, not once a quarter. Deviations are flagged in real time, not discovered during audit prep.

Recoverability Health scoring

Not just "are we compliant now" but "can we recover to a compliant state." A quantified measure of resilience that regulators increasingly ask for.

IDP-agnostic by design

One compliance baseline regardless of which IDP runs your tenant. The same framework mapping, the same scoring, the same audit reports, for any supported IDP.

Standard and custom frameworks, one baseline

SOC 2, ISO 27001, DORA, NIS2, NIST SP 800-53, APRA, FISMA. One compliance baseline across all frameworks. One set of audit reports.

NHI & AI agent coverage

Non-human identities tracked with the same compliance rigor as human identities. Full audit trails for service principals, API tokens, and agent bindings.

Automated remediation

Common compliance drift patterns are remediated automatically. Reduces the manual intervention burden and closes compliance gaps faster.

Ready to be always audit-ready?

See Acsense Compliance & Assurance in action on your IAM tenant.

Request a demo

Built for the compliance team, and everyone who depends on identity

Compliance & Assurance is the audit-readiness guarantee. The platform serves the people who keep IAM compliant every day, and the leaders who carry the regulatory risk.

IAM Administrators

Your job is to keep IAM compliant and auditable. Compliance drift detected automatically. Remediation for common patterns runs without intervention. Focus on operations, not evidence assembly.

IT & Operations Leaders

Quantified compliance scores per framework. Recoverability Health scoring. One dashboard for compliance posture across all tenants and IDPs.

Security & CISO

Audit-ready evidence on demand. Every IAM change mapped to regulatory controls with a full evidence chain. The compliance proof regulators and the board ask for, produced automatically.

AI & ML Leaders

Non-human identities tracked with the same compliance rigor as human identities. Full NHI audit trails as your AI agent surface expands.

CERTIFIED & AUDITED

- **FedRAMP High** Authorized
- **SOC 2 Type II** Audited by EY
- **ISO 27001** Information Security
- **ISO 27017** Cloud Security
- **ISO 27018** Cloud Privacy

ABOUT ACSENSE

Acsense is the IAM Resilience Platform that protects, recovers, and continuously validates enterprise identity infrastructure at scale. The platform delivers Backup & Recovery, Configuration Management, Disaster Recovery, and Compliance & Assurance across Okta and Microsoft Entra ID, from a single purpose-built product. Acsense serves security-first enterprises and federal agencies across financial services, healthcare, critical infrastructure, public sector, and technology globally. Learn more at acsense.com.