AETRUM LLC

Salesforce Org Access Assessment

Findings Report

Customer	Meridian Supply Co. (fictional)
Salesforce org / environment	00D8b000000AbCd (Production)
Assessment period	July 21 - August 1, 2026
Configuration as of	August 1, 2026
Version / status	1.0 / Final
Author	Bergin Panimayam, Aetrum LLC
Reviewer	Independent technical reviewer
Classification	Illustrative sample. Fictional data. Published by Aetrum LLC as an example of the deliverable. Real client reports are confidential and not redistributed.

1. Scope and limitations

This assessment goes deep on one domain, identity and access management and the sharing and visibility model, human and non-human, as configured during the assessment period. IAM side: authentication, SSO, connected apps and External Client Apps, named and external credentials, integration users, and API access. Sharing side: org-wide defaults, sharing rules, roles, groups, permission sets and permission set groups, object, field, and record access, and external and guest user access. A whole-org review across data, metadata, configuration, automation, code, and build-side security is the Architecture Review, a separate engagement.

Limitations: this is a point-in-time review of configuration and observable usage via read-only access. It is not a penetration test, not a code review, and not a compliance certification. Findings reflect the org as of the as-of date; changes made after it are out of scope.

2. Methodology and rating definitions

2.1 Risk rating

Risk is the product of likelihood and impact, assessed against data sensitivity, business criticality, affected population, and existing compensating controls.

	Impact: Low	Impact: Medium	Impact: High
Likelihood: High	Medium	High	High
Likelihood: Medium	Low	Medium	High
Likelihood: Low	Low	Low	Medium

2.2 Effort rating

Small: days. Medium: weeks. Large: a quarter or more. Every effort rating states its assumptions and dependencies inside the finding.

2.3 Evidence standard

Every finding carries an Evidence Pack reference. Each evidence item records: evidence ID, collection timestamp, org and environment, exact configuration values observed, the query or screenshot reference, affected users, objects, fields, and business processes, the population and observation period, redaction classification, and validation status including customer confirmation.

3. Executive summary

The org's access posture is broadly sound, with three areas of concentrated risk across both halves of the assessment. On the IAM side: an orphaned dual-purpose certificate 36 days from expiry, and an over-scoped warehouse integration credential whose refresh tokens never expire. On the sharing side: an Account org-wide default of Public Read Only, with a legacy sharing rule extending edit to a group that now includes contractor logins. None of this requires a rebuild. The roadmap completes the highest-risk item, the certificate, within two weeks, and stands up the warehouse credential fix within thirty days. All twelve findings have owners; findings F5 through F12 continue in the full findings register.

	High risk	Medium risk	Low risk

Findings	4	5	3

4. Dependency register

Item	Type	Used by	Owner / backup	Secret store	Expires / rotation	Last verified	Criticality	Ref
SelfSignedCert_2022	Certificate	SSO request signing; ERP mTLS callout	None recorded; no backup	Salesforce cert store	Sep 6, 2026 / none	Jul 24, 2026	High	F1, EV-07
integration_svc@co	Integration user	Marketing sync; warehouse extract	IT Ops; no backup	n/a	n/a	Jul 24, 2026	High	F4, EV-09
WarehouseSync app	Connected app (2022)	Nightly warehouse extract	Data team / J. Rivera	Middleware vault	Tokens: until revoked	Jul 25, 2026	Medium	F2, EV-11
ERP_NamedCred	Named credential	Outbound ERP callouts (Apex)	IT Ops; no backup	Salesforce	Follows cert above	Jul 24, 2026	High	none
PayrollFile SFTP key	SFTP key (middleware)	Middleware payroll export job	Finance; no backup	Middleware vault	Unknown → gap	Jul 28, 2026	High	F7, EV-14
Account OWD + SR-14	Sharing config	Account edit for Ops-All (78 users incl. 7 contractors)	SF admin; no backup	n/a	n/a	Jul 25, 2026	High	F3, EV-13

5. Findings

F1: Certificate serving SSO and an ERP callout expires September 6 with no owner

Risk / effort	High risk, Small effort
Access domain	Identity and access management (IAM)
What we observed	One self-signed certificate (SelfSignedCert_2022, 2048-bit RSA, expires 2026-09-06) does two jobs. Salesforce acts as the SAML service provider here, and this certificate signs the outbound authentication requests it sends to the external identity provider (Single Sign-On Settings, Request Signing Certificate). The same certificate also authenticates the mutual TLS callout to the ERP via ERP_NamedCred. No owner is recorded; Salesforce has no native ownership field for certificates. Salesforce does email admins before a certificate expires, but the alert names only the certificate: nothing in the org maps that name to the two systems that depend on it or to a responsible owner.

Evidence

Evidence ID	EV-07
Collected	2026-07-24 14:12 ET, Aetrum read-only user
Org / environment	00D8b000000AbCd (Production)
Values observed	Certificate and Key Management: expiry 2026-09-06; referenced by Single Sign-On

	Settings as the SP Request Signing Certificate, and by ERP_NamedCred as the mutual-TLS client certificate
Query / screenshot	Metadata API retrieve, EV-07-a; Setup screenshots EV-07-b/c
Affected	All SSO-initiated logins; ERP callouts from 3 Apex classes; order-to-invoice process
Population / period	Full org; observed July 21-August 1, 2026
Redaction class	Internal identifiers only; no customer data
Validation	Confirmed by IT Ops lead, July 29, 2026

Why it matters	The expiry alert reaches admins, but without a dependency map no one can see that this one certificate carries both the SAML request signing and the ERP callout. If it lapses, both are expected to fail the same day (validation confirmed the external IdP is configured to require signed authentication requests, and the ERP's TLS layer rejects an expired client certificate), and the two failures would present as unrelated incidents. One certificate serving two unrelated systems is a shared single point of failure.
Recommended fix	Assign an owner in this register. Decouple into two certificates: SSO request signing remains self-signed (standard SAML practice; trust is via metadata exchange), the ERP mTLS leg moves to a CA-signed certificate per the vendor's trust requirements. Open the vendor ticket immediately; complete both swaps within two weeks of the readout, well ahead of the September 6 expiry. Dependencies: ERP vendor trust-store update lead time.

F3: Account org-wide default is Public Read Only, and a legacy sharing rule extends Edit to contractors

Risk / effort	High risk, Medium effort
Access domain	Sharing and visibility
What we observed	The Account object org-wide default is Public Read Only, so every user can already see every Account. On top of that, an owner-based sharing rule (SR-14, created 2021) shares all Accounts owned by users in the Sales roles, which is effectively the entire Account base, with the public group "Ops-All" at Read/Write. Ops-All membership now includes seven external contractor users added over time. Net effect: every user can read every Account, and everyone in Ops-All, contractors included, can edit nearly all of them, including the 1,240 Accounts marked Confidential by a business classification field, a label that carries no access enforcement on its own.

Evidence

Evidence ID	EV-13
Collected	2026-07-25 11:20 ET, Aetrum read-only user
Org / environment	00D8b000000AbCd (Production)
Values observed	Sharing Settings: Account OWD = Public Read Only; owner-based sharing rule SR-14 shares Accounts owned by the Sales roles with group Ops-All at Read/Write; Ops-All membership = 78 users incl. 7 contractor logins
Query / screenshot	Metadata API retrieve (sharingRules), EV-13-a; Setup screenshots EV-13-b
Affected	Account object, all records; 78 users incl. 7 contractors; 1,240 Accounts marked Confidential (classification field)
Population / period	Full org; observed July 21-August 1, 2026
Redaction class	Record counts only; no Account data reproduced

Validation	Confirmed by Salesforce admin, July 30, 2026

Why it matters	Read access is company-wide by default, and SR-14 turns that into Edit for everyone in Ops-All, contractors included. People outside the business can edit Accounts it treats as Confidential, which is the first thing an auditor or a customer security review will flag. The rule is a real, active grant today, so tightening the model means changing both the OWD and the rule together, in the right order, or access breaks for the teams that legitimately depend on SR-14.
Recommended fix	Sequence matters. In a full sandbox, reduce the Account OWD to Private and confirm what access the business actually needs. The broad read comes from the OWD and the broad edit from SR-14; replace SR-14 with targeted sharing: role hierarchy for management visibility, plus criteria-based rules scoped to the specific teams that need cross-Account edit. Remove contractor logins from Ops-All and grant contractors only the records they need. Validate with a permissions comparison (record visibility per user before and after) so no legitimate access breaks. Effort is Medium because it touches every Account and needs UAT with the Ops teams; no data is migrated, so there is no user-facing downtime.

F1 (IAM) and F3 (Sharing and Visibility) are shown here in full to demonstrate both halves of the assessment. Findings F2 and F4 through F12 follow the same structure in the full report, ordered by risk.

6. Inspected and found clean

Checked against Salesforce Security Health Check plus the customer's password and session policy: password policies and session settings meet baseline; no inactive users hold active integration credentials; API Enabled access, checked across profiles and permission sets, is limited to users who need it. Full list in Appendix A.

7. Architecture Decision Record

ADR	ADR-01: Standardize new integrations on External Client Apps
Status	Proposed, for adoption at readout
Context	Six integrations authenticate five different ways. Salesforce now recommends External Client Apps and, as of Spring '26, no longer allows new connected apps to be created unless Salesforce Support grants an exception; existing and packaged connected apps continue to function, and migration tooling is provided.
Decision	All new integrations use External Client Apps. OAuth flow chosen by interaction model: client credentials only for trusted, non-interactive server-to-server integrations; authorization code with PKCE where a user delegates access; JWT bearer where certificate-based trust fits. Each server-to-server integration runs as a dedicated integration user on an API-only Integration User license with a purpose-specific permission set. The legacy username-password flow is not used.
Alternatives considered	Continue per-team choices (rejected: ungovernable); mandate one flow for everything (rejected: wrong for user-delegated apps).
Consequences	One framework to govern and audit; per-system blast radius; migration absorbed into planned work; short-term effort to document flow choice per integration.

8. Remediation roadmap

Target date	Action	Owner	Finding

Aug 8, 2026	Certificate owner assigned; ERP vendor ticket opened; CA-signed cert requested; new SSO signing cert generated	IT Ops	F1
Aug 14, 2026	Both certificate swaps completed in maintenance window (23 days before expiry)	IT Ops + ERP vendor	F1
Sep 2, 2026	External Client App for warehouse extract live in sandbox; warehouse auth change scheduled	Data team	F2
Sep 2, 2026	Account OWD-to-Private change staged in full sandbox; SR-14 replacement and contractor removal drafted; permissions comparison run	SF admin	F3
Oct 6, 2026	Sharing model change deployed to production after UAT with Ops teams	SF admin	F3
Nov 2, 2026	Warehouse cutover (held for the warehouse team's change window); old app tokens revoked, app disabled and removed; ADR-01 adopted for remaining integrations at next planned change	Data team / per system	F2, ADR-01

Appendix A: Evidence Pack index

ID	Description	Collected
EV-07	Certificate expiry and references (F1)	2026-07-24 14:12 ET
EV-09	Shared integration user, systems and login sources (F4)	2026-07-24 15:05 ET
EV-11	WarehouseSync OAuth policies, scope, login sources (F2)	2026-07-25 09:40 ET
EV-13	Account OWD (Public Read Only) and SR-14 owner-based Edit grant path (F3)	2026-07-25 11:20 ET

This index is abridged for the sample. The full report lists one evidence entry per finding across all twelve.