trevaun

Salesforce Org Access Assessment

Findings Report

Sample · Fictional data · Illustrative only

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

1. Scope and limitations

This assessment goes deep on one question: who and what can reach which records in the org, and how they got that access. It covers identity and access management and the sharing and visibility model, for human and non-human users, as configured during the assessment period. Identity side: authentication, single sign-on and MFA, login policies, profiles, permission sets and permission set groups, high-risk system permissions, user lifecycle, and the access held by integration users and AI agents. Sharing side: org-wide defaults, sharing rules, roles, groups, object, field and record access, and external and guest user access.

Out of scope: which systems depend on a given integration, credential or certificate, and what breaks when one changes. That is a separate follow-on review. A whole-org review across data, metadata, configuration, automation, code and build-side security is the Architecture Assessment, also 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 identity side: 14 users hold Modify All Data through permission sets nobody reviewed, 11 people who have left the company still have active logins, and the shared integration user can view all data in the org. 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 removes the unneeded Modify All Data grants and deactivates the departed users within one week, and

completes the sharing model change within ten weeks. All twelve findings have owners; findings F5 through F12 continue in the full findings register.

4
High risk findings

5
Medium risk findings

3
Low risk findings

4. High-risk access register

Access	Type	Granted through	Held by	Owner	Last reviewed	Risk	Ref
Modify All Data	System permission	Permission sets Data_Fix_2023, Ops_Admin_Temp, Migration_Support	14 users (5 admins, 9 others)	None recorded	Never	High	F1, EV-03
Active logins after departure	User lifecycle	No deactivation step in offboarding	11 former staff and contractors	HR and IT Ops	n/a	High	F2, EV-05
Account read for all, edit for Ops-All	Sharing configuration	Account OWD Public Read Only; sharing rule SR-14	All users; edit for 78 users incl. 7 contractors	SF admin	Never	High	F3, EV-13
View All Data	System permission (non-human)	Profile of integration_svc	1 integration user, shared by 2 systems	IT Ops	Never	High	F4, EV-09
Manage Users and Assign Permission Sets	System permission	Permission set Team_Lead_Admin	6 team leads	SF admin	2024	Medium	F5, EV-10
Guest user read on Case and Contact	External access	Experience site guest profile	Unauthenticated site visitors	Support lead	Never	Medium	F8, EV-15

5. Findings

F1: 14 users hold Modify All Data through permission sets nobody reviewed

High risk · Small effort · Identity and access management (IAM)

What we observed	Modify All Data lets a user view, edit, transfer and delete every record in the org, regardless of sharing. 14 active users hold it. Five are the Salesforce administrators. The other nine received it through three permission sets created for one-off tasks: Data_Fix_2023 (a data cleanup), Ops_Admin_Temp (cover during an admin's leave) and Migration_Support (a 2024 migration). None of the three has a description, an owner or an end date, and no assignment has been reviewed since it was made. Two of the nine are contractors.

EVIDENCE

Evidence ID	EV-03
Collected	2026-07-23 10:45 ET, Trevaun read-only user
Org / environment	00D8b000000AbCd (Production)
Values observed	PermissionSetAssignment records for every permission set and profile granting PermissionsModifyAllData; permission set names, assignee names and types, and assignment dates (earliest March 2023)
Query / screenshot	SOQL on PermissionSetAssignment and PermissionSet, EV-03-a; Setup screenshots EV-03-b/c
Affected	Every object and record in the org; 9 non-admin users, 2 of them contractors
Population / period	Full org; observed July 21 to August 1, 2026
Redaction class	User names replaced with role labels; no record data
Validation	Confirmed by Salesforce admin, July 29, 2026

Why it matters	Each of the nine accounts can change or delete any record in the org, including records the sharing model hides from them. A mistake, a misused account or a compromised login has the same reach as an administrator's. Field history and the audit trail record changes after the fact, but they do not stop them. This is the first thing an auditor or a customer's security team asks about.
Recommended fix	Remove Modify All Data from the nine non-admin users this week, after a short check that no scheduled job runs as them. Move admin work to a named admin permission set group with an owner. Retire the three one-off permission sets. Review every holder of Modify All Data, View All Data, Manage Users and Customize Application once a quarter (see ADR-01). Effort is Small: no data changes and no user-facing downtime.

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

High risk · Medium effort · 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, Trevaun 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 to 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 (identity and access) 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; MFA is enforced for every user who logs in through the user interface; API Enabled, checked across profiles and permission sets, is limited to users who need it; no user outside the admin group can view setup and configuration. Full list in Appendix A.

7. Architecture Decision Record

ADR	**ADR-01: Grant high-risk system permissions only through owned, reviewed permission set groups**
Status	Proposed, for adoption at readout
Context	Modify All Data, View All Data, Manage Users and Customize Application reach 21 users through two profiles and five permission sets. Most were granted for a one-off task and never removed. No grant has an owner or a review date.
Decision	These four permissions are granted only through named permission set groups, each with an owner and a written purpose. Profiles do not carry them. Temporary needs use a time-bound assignment with an end date. Every holder is reviewed once a quarter, and the review is recorded. Integration users and AI agents get object-specific permissions, never View All Data or Modify All Data.
Alternatives considered	Keep granting by request and clean up once a year (rejected: grants pile up between cleanups); remove the permissions from everyone but one admin (rejected: blocks legitimate admin work and invites shared logins).
Consequences	One place to see who holds the most powerful access; a review trail for auditors; a small, steady admin overhead each quarter.

8. Remediation roadmap

Target date	Action	Owner	Finding
Aug 7, 2026	Modify All Data removed from the nine non-admin users; three one-off permission sets retired	SF admin	F1
Aug 7, 2026	Eleven departed users deactivated; deactivation step added to the offboarding checklist	IT Ops + HR	F2
Aug 21, 2026	View All Data replaced with object-specific permissions on integration_svc; one integration user per system	IT Ops	F4
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	First quarterly review of high-risk permissions completed and recorded; ADR-01 adopted	SF admin	F1, ADR-01

Appendix A: Evidence Pack index

ID	Description	Collected
EV-03	Modify All Data holders, permission sets and assignment dates (F1)	2026-07-23 10:45 ET
EV-05	Active users matched against HR departures (F2)	2026-07-23 16:10 ET
EV-09	Integration user profile, system permissions and login sources (F4)	2026-07-24 15:05 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.

Trevaun · trevaun.com · hello@trevaun.com. Trevaun[SM] is a trade name and service mark of Aetrum LLC, a Virginia limited liability company. Ashburn, Virginia.