

SoftwareGlimpse CRM Security Checklist

Updated: 15 Aug 2026

Vendor being evaluated: _____
 Evaluator / Team: _____
 Date of evaluation: _____

Prove CRM access controls on the plan you would actually buy.

HOW TO USE THIS CHECKLIST

- 1 Draft the access map
- 2 Identity
- 3 Roles
- 4 Export controls
- 5 Audit logs
- 6 Access reviews

Key: ☐ Pass ☐ Partial ☐ Fail ☐ Not tested | * = Must-have

Evidence: screenshots, recordings, official docs, written confirmation, or test results.

#	CHECK ITEM	WHY IT MATTERS	REQ	EVIDENCE	RESULT
1. IDENTITY: SSO & MFA ON THE QUOTED PLAN					
1.1	SSO availability confirmed on the quoted plan	Identity features shown in demos are frequently sold on a higher tier than the quote.	*		☐ Pass ☐ Partial ☐ Fail ☐ N/T
1.2	MFA expectation written	"SSO handles it" is not a policy until you name where MFA is enforced.	*		☐ Pass ☐ Partial ☐ Fail ☐ N/T
1.3	Joiner and leaver paths defined	Most stale CRM access starts with a manual joiner-leaver process nobody owns.	*		☐ Pass ☐ Partial ☐ Fail ☐ N/T
1.4	Same-day leaver disablement tested	A leaver keeping access to the customer book is the sharpest risk CRM carries.	*		☐ Pass ☐ Partial ☐ Fail ☐ N/T
1.5	Local and break-glass admin accounts limited	Accounts outside SSO are the ones nobody reviews.	*		☐ Pass ☐ Partial ☐ Fail ☐ N/T
1.6	Session and idle policy recorded	Shared or unattended devices make session length a real control.	-		☐ Pass ☐ Partial ☐ Fail ☐ N/T
1.7	Identity escalation owner named	An SSO failure blocks the entire sales floor at once.	*		☐ Pass ☐ Partial ☐ Fail ☐ N/T
2. ROLES & OBJECT VISIBILITY					
2.1	Access map drafted: roles against objects	Everything else in this checklist is guesswork until visibility is written down.	*		☐ Pass ☐ Partial ☐ Fail ☐ N/T
2.2	Production role list matches the map	Roles that exist only in production drift away from the design immediately.	*		☐ Pass ☐ Partial ☐ Fail ☐ N/T
2.3	Contact visibility tested per persona	Broad contact visibility is the most common oversharing default.	*		☐ Pass ☐ Partial ☐ Fail ☐ N/T
2.4	Deal visibility tested per persona	Pipeline amounts are visible to more people than most teams intend.	*		☐ Pass ☐ Partial ☐ Fail ☐ N/T
2.5	Account sharing model documented	Coverage models — households, pooled accounts, multi-client agencies — are where sharing rules get complicated.	*		☐ Pass ☐ Partial ☐ Fail ☐ N/T
2.6	Field-level restriction confirmed on the plan	Restricting a single sensitive field is often a higher-tier capability.	-		☐ Pass ☐ Partial ☐ Fail ☐ N/T

#	CHECK ITEM	WHY IT MATTERS	REQ	EVIDENCE	RESULT	
2.7	Full admin roster minimized	Every extra full admin is an unaudited export path.	*		☐ Pass ☐ Fail	☐ Partial ☐ N/T
2.8	Permission-change approver named	Role edits requested in chat are how least privilege erodes.	*		☐ Pass ☐ Fail	☐ Partial ☐ N/T
3. EXPORT CONTROLS FOR CONTACTS & DEALS						
3.1	Roles allowed to export contacts defined	A contact export is your customer list leaving the CRM.	*		☐ Pass ☐ Fail	☐ Partial ☐ N/T
3.2	Roles allowed to export deals defined	Pipeline and forecast extracts are commercially sensitive.	*		☐ Pass ☐ Fail	☐ Partial ☐ N/T
3.3	Export audit availability confirmed on the plan	Without export events you cannot answer who took what.	*		☐ Pass ☐ Fail	☐ Partial ☐ N/T
3.4	Report and dashboard sharing reviewed	A widely shared report is an export with extra steps.	*		☐ Pass ☐ Fail	☐ Partial ☐ N/T
3.5	Connected apps and scopes inventoried	Integrations often hold read access to every contact and deal.	*		☐ Pass ☐ Fail	☐ Partial ☐ N/T
3.6	API tokens owned and rotatable	A token created in a personal account outlives the person.	*		☐ Pass ☐ Fail	☐ Partial ☐ N/T
3.7	Migration and cutover extracts controlled	Legacy export files usually sit in the least protected place in the company.	-		☐ Pass ☐ Fail	☐ Partial ☐ N/T
4. EMAIL & CALENDAR SYNC PRIVACY						
4.1	Sync scope documented	Users assume only metadata syncs; products often capture more.	*		☐ Pass ☐ Fail	☐ Partial ☐ N/T
4.2	Who can read synced email on records defined	Mailbox content on a shared timeline is a privacy decision, not a feature setting.	*		☐ Pass ☐ Fail	☐ Partial ☐ N/T
4.3	Privacy brief delivered before sync enablement	Consent after connection is not consent.	*		☐ Pass ☐ Fail	☐ Partial ☐ N/T
4.4	Disconnect and retention behavior tested	Stopping sync rarely removes what has already synced.	*		☐ Pass ☐ Fail	☐ Partial ☐ N/T
4.5	Attachment visibility reviewed	Attachments carry the sensitive content people forget is syncing.	-		☐ Pass ☐ Fail	☐ Partial ☐ N/T
4.6	Private and personal folders excluded	Syncing everything sweeps in correspondence that was never a business record.	-		☐ Pass ☐ Fail	☐ Partial ☐ N/T
5. AUDIT LOGS & EVIDENCE						
5.1	Required audit events listed	Asking for "audit logs" gets you whatever the vendor happens to log.	*		☐ Pass ☐ Fail	☐ Partial ☐ N/T
5.2	Log retention on the plan recorded	Short retention closes the investigation window before you notice a problem.	*		☐ Pass ☐ Fail	☐ Partial ☐ N/T
5.3	Evidence export path proven	A log you cannot extract is not evidence.	*		☐ Pass ☐ Fail	☐ Partial ☐ N/T
5.4	Anomaly escalation route written	Unusual admin activity or an export spike needs somewhere to go.	*		☐ Pass ☐ Fail	☐ Partial ☐ N/T
5.5	Control gaps accepted in writing	An unacknowledged gap becomes a surprise during an incident.	*		☐ Pass ☐ Fail	☐ Partial ☐ N/T
6. ACCESS REVIEWS AFTER GO-LIVE						

#	CHECK ITEM	WHY IT MATTERS	REQ	EVIDENCE	RESULT	
6.1	Review cadence set with calendar holds	A cadence with no holds becomes an intention nobody honors.	*		☐ Pass ☐ Fail	☐ Partial ☐ N/T
6.2	Review inputs defined	A review without user, role, and export lists is just a conversation.	*		☐ Pass ☐ Fail	☐ Partial ☐ N/T
6.3	Reviewer and signer named	Reviews with no signer produce no decisions.	*		☐ Pass ☐ Fail	☐ Partial ☐ N/T
6.4	Remediation tracked to closure	Findings that are not tracked reappear at the next review.	*		☐ Pass ☐ Fail	☐ Partial ☐ N/T
6.5	Re-run triggered by material change	New integrations and reorganizations change the access picture faster than time does.	*		☐ Pass ☐ Fail	☐ Partial ☐ N/T
6.6	Post-go-live re-run scheduled	The first weeks of production always create access exceptions.	-		☐ Pass ☐ Fail	☐ Partial ☐ N/T

7. NICHE: CLIENT-BOOK REVIEWS (FINANCIAL SERVICES)

7.1	Advisor client-book visibility documented	Cross-book browsing is the visibility question FS teams get asked about most.	-		☐ Pass ☐ Fail	☐ Partial ☐ N/T
7.2	Export-capable roles re-attested on a cadence	Client-list export rights need a periodic, recorded confirmation.	-		☐ Pass ☐ Fail	☐ Partial ☐ N/T
7.3	Leaver client-book reassignment runbook	An advisor departure moves whole books of contacts and deals at once.	-		☐ Pass ☐ Fail	☐ Partial ☐ N/T
7.4	Sample access evidence for client records	You may be asked to show who viewed or exported client data.	-		☐ Pass ☐ Fail	☐ Partial ☐ N/T
7.5	Compliance partner review recorded	This checklist is operational; regulatory interpretation is not its job.	-		☐ Pass ☐ Fail	☐ Partial ☐ N/T

Scoring guidance

Pass = fully meets. Partial = works with limits.
Fail = does not meet. Not tested = no proof yet.

Evidence matters

Only mark a result when proof exists. Otherwise use Not tested — sales slides alone do not count.

One script. Every vendor.

Use the same scenarios and test steps for every product so comparisons stay fair.