THIN LINE SOFTWARE
TEXAS RMS EVALUATION GUIDE

# How to evaluate an RMS for a Texas law-enforcement agency.

Originally published: June 2026 · Last reviewed: September 2026

What to ask, what to compare, and what matters when choosing a records management system for a Texas law-enforcement agency.

A practical guide to evaluating records management systems for Texas police departments and law-enforcement agencies.

Choosing an RMS is not simply a matter of finding a system that stores reports. A Texas police department must follow an incident from the initial report through supervisor review, correction, NIBRS validation, investigation, disposition, and later retrieval-while preserving a dependable record of what happened.

The best RMS is not necessarily the one with the longest feature list. It is the one that helps the agency complete the work correctly while maintaining a dependable record underneath it.

## Start with the life of the record

Before looking at dashboards, ask the vendor to demonstrate an entire incident.

> *Call / incident -> report -> review -> correction -> NIBRS validation -> investigation -> supplement -> disposition -> retrieval / reporting*

Real incidents branch. A call might close with a report, become an investigation, produce a warrant, involve evidence, or return months later when a name or plate comes up again. The software has to preserve one coherent record through those changes.

> **DEMO THIS**
> An officer starts a report; adds people, vehicles, property, offenses, narrative, and attachments; submits it; a supervisor rejects it with a reason; the officer corrects and resubmits it; the report is approved. Don't just ask whether the system supports it. Ask the vendor to show what each role does and what history remains.

### Make the report the center of the system

Open a completed incident and ask whether you can understand what happened without opening five other screens. Not everything has to appear simultaneously. The pieces should belong to one record. A field on a form is not the same thing as a completed workflow.

### Evaluate the officer's daily work

Have an officer complete a realistic report while everyone watches. Look at screens, repeated fields, narrative entry, attachments, drafts, and how the system behaves on the equipment officers actually use.

> *Would you want to write reports in this every shift?*

Bad field usability becomes a records problem because the RMS depends on complete, accurate entry.

### Look for one record, not copies

If dispatch already captured a name, address, vehicle, and plate, what happens when the officer starts the report? If they retype it, ask why.

> **DEMO THIS**
> Create a person once and use that person in several records. Then change current contact information and ask what happens to historical incidents.

> **Ask the vendor**
> If a person appears in a call, report, citation, arrest, and investigation, is that one record or disconnected copies?

## Make review and Texas reporting real work

A system can have buttons labeled "Approve" or "NIBRS" without supporting the work behind those actions.

### Evaluate supervisor review as work

Small agencies often skip this in demonstrations. Ask what a supervisor sees that needs review, whether they can return a report with a reason, what happens to the original submission, whether changes are audited, and whether command staff can see stalled work.

> **DEMO THIS**
> Show everything waiting for this supervisor, reject a report with a reason, have the officer correct it, and show the history.

After approval, ask who can change the record, whether the original value is preserved, and whether an amendment requires another review.

### Treat NIBRS as a product of the record

> **Texas requirement**
> Texas DPS states that, effective September 1, 2023, Texas criminal-justice agencies are required to implement a NIBRS-compliant RMS and submit NIBRS data monthly to the Texas DPS UCR Program.

Don't stop at whether the system "supports NIBRS." Ask whether required data is captured during report writing, when validation errors appear, whether officers can correct their own errors, whether supervisors can see what blocks submission, whether records staff can find rejected incidents, and whether a reported value can be traced back to the incident.

> **DEMO THIS**
> Create a report with a reporting problem, show who sees the error, correct it, and show the record ready for submission.

> *NIBRS should be the product of good records-not a second recordkeeping system staff reconstruct afterward.*

Texas-specific support matters. Ask which DPS specification the vendor supports, how Texas changes reach production, which Texas agencies currently submit through the RMS, and what certification or recertification support the vendor provides. DPS maintains a public list of vendors actively working with Texas agencies to submit NIBRS; use it as one due-diligence input, not as a product endorsement or CJIS determination.

Vendors actively working with Texas agencies to submit NIBRS (Texas DPS)

For Texas-specific reporting, certification, errors, and vendor questions, read the Texas NIBRS Reporting Guide.

## Make the record useful later

Information entered once should answer questions later-without rebuilding the case from a PDF.

> **Try these searches**
> - Show me everything involving John Smith.
> - Show me reports involving a white Ford pickup with a partial plate.
> - Find incidents at this address during the last two years.
> - Show me records involving this phone number.
> - Find reports involving this person and this vehicle.

Then ask an investigator to take over an approved incident, add a supplement, associate another person or vehicle, and update status. The investigator should inherit what patrol already knows. That is a more useful test than asking whether the system has an "Investigations module."

## Connect the RMS to the rest of the agency

Incidents start in CAD, continue on mobile devices, and may involve evidence, citations, or court. Those connections only help if they enter the same operational record.

Don't accept "we integrate with CAD" as an answer. Ask to see one call become an incident-what arrived, and what the officer still typed.

For mobile, ask whether officers can do the work they actually need from the field. For evidence, ask whether a user can move between a case and associated property while keeping appropriate controls. For citations and crashes, ask whether the activity joins the agency record or creates another isolated database.

Prefer one demonstrated handoff over a list of advertised integrations. For each connection that matters at go-live, require the vendor to say whether it is available today, needs configuration, needs custom work, is planned, or is unsupported.

## Treat security and history as mandatory

Security is a mandatory part of the evaluation. Do not end the conversation at "CJIS compliant" or "CJIS certified."

Ask the vendor to explain how the proposed environment satisfies the agency's applicable requirements and who is responsible for authentication, permissions, audit logging, access control, hosting, encryption, backups and recovery, and CJIS-related documentation.

CJIS security involves responsibilities shared among agencies, vendors, and other participants; buying an RMS does not eliminate the agency's responsibilities.

For the questions an agency should be able to answer before an audit, read the Texas CJIS Audit Readiness Checklist.

For what changed in CJIS Security Policy 6.1, read the Texas CJIS 6.1 Guide.

### Test permissions the agency actually needs

"Role-based permissions" can mean almost anything. Give the vendor actual scenarios:

> **Test these permissions**
> - Can patrol officers see an active internal investigation?
> - Can a dispatcher see information necessary for the call without receiving unnecessary access to investigative records?
> - Can an investigator access restricted case material?
> - Can records personnel correct data without silently changing an approved officer report?
> - Can an administrator manage users without having unrestricted operational access?
> - Can we restrict a particularly sensitive case?

### Make the vendor demonstrate audit history

Pick a record. Change something important. Then ask:

> *Show me who changed it.*

Ask who created, submitted, reviewed, rejected, and approved the record, and what changed. For public-safety records, the history can be almost as important as the current state.

## Protect the agency through the transition and after go-live

A good product can still fail through a conversion that leaves relationships unexplained, training that only shows the Reports menu, or a vendor that cannot say how Texas or NIBRS changes become software changes.

If you're replacing an existing RMS, historical records are part of the project. Ask what will not be converted. That question is often more revealing than asking what will.

> **Ask the vendor**
> - What exactly will be converted?
> - What will not?
> - Are people, vehicles, property, incidents, attachments, relationships, and historical identifiers preserved?
> - How will converted data be validated, and how are exceptions handled?

For exports, mapping, attachments, validation, and go-live or backfill, read the data conversion guide.

Ask who implements, configures, converts, and trains each role; what evidence shows readiness; and what go-live and hypercare look like.

Go-live is a milestone, not a definition of done. Read the Public Safety Software Implementation Readiness Guide.

Ask vendors to train by role and workflow-officer writes report -> supervisor reviews -> records resolves a reporting issue -> investigator continues the case-not merely by screen.

> **Ask references**
> - When you have a real operational problem, can you reach someone who understands Texas and NIBRS work?
> - How long does it normally take to get an answer?
> - What happens when the problem affects the shift that is working now?
> - How did a recent Texas or NIBRS change reach production?

> *What does our agency do if the system is unavailable at 2:00 a.m.?*

Ask what happens to the agency's records if the relationship ends, including format, attachments, relationships, historical identifiers, cost, timing, and vendor assistance.

Compare five-year total cost, including licensing, implementation, conversion, training, interfaces, hosting, support, optional modules, and likely increases.

Ask references at Texas agencies of similar size. Then ask:

> *What is annoying about the software?*

## Make every finalist demonstrate the same incidents

Create your own script. Don't let each vendor choose what to show.

For example:

> **Scenarios A-D**
> - A - Incident report. An officer creates an incident involving multiple people, a vehicle, property, and an offense; completes the narrative and required reporting data.
> - B - Supervisor correction. A supervisor reviews the report, identifies a problem, returns it, the officer corrects it, and the system preserves the history.
> - C - NIBRS problem. Create a report with a reporting issue, identify the error, correct it, and show how it becomes ready for submission.
> - D - Investigation. An investigator receives the case, adds supplemental information, associates another person or vehicle, and updates status.

**Scenarios E-H**

- E - Search. Find everything the agency knows about a person, vehicle, location, or property item across multiple incidents.
- F - CAD/RMS handoff. Start with a dispatched call and show what reaches the RMS and what must still be entered manually.
- G - Historical correction/audit. Change significant information on an existing record and show who changed what and when.
- H - Converted record. Open a historical converted case and demonstrate relationships, attachments, identifiers, search, and history.

Now you're comparing systems rather than sales demonstrations.

## A practical RMS evaluation scorecard

Weight the evaluation toward the work the agency actually has to do:

| Category | Suggested weight |
|---|---|
| Core RMS & records workflow | 15% |
| Officer usability | 10% |
| Supervisor workflow | 10% |
| Texas/NIBRS reporting | 15% |
| Search & investigations | 10% |
| CAD/mobile/integration | 10% |
| Security & auditability | 10% |
| Data conversion | 5% |
| Implementation & training | 5% |
| Support/vendor relationship | 5% |
| Cost & contract | 5% |
| Total | 100% |

Change the weights to fit your operation. Also establish a few mandatory requirements that must be satisfied regardless of the overall score. For example:

- Must support Texas NIBRS submission from the operational record.
- Must preserve audit history of material changes.
- Must convert the historical records the agency requires.
- Must provide acceptable data ownership/export terms.

A vendor shouldn't overcome a mandatory deficiency by having a prettier dashboard.

## 30 questions to bring to every RMS demonstration

Print this section and keep it open during vendor demos.

1. Show us an incident from creation through final approval.
2. Show us a rejected report being corrected and resubmitted.
3. Show us what carries from a CAD call into the RMS.
4. Show us a patrol case being assigned to an investigator.
5. Show us multiple investigators working one case.
6. Show us everything associated with one person.
7. Show us a search using incomplete information.
8. Show us how duplicate people are detected.
9. Show us what happens when a person's current address changes.
10. Show us what a patrol officer sees when logging in.
11. Show us what a supervisor sees that needs review.
12. Show us what records personnel see.
13. Show us how each role knows what still needs attention.
14. Show us the NIBRS workflow on a real incident.
15. Show us how a NIBRS error is identified and corrected.
16. Show us how Texas-specific UCR requirements are handled in the system.
17. Which Texas agencies currently submit NIBRS through this system?
18. Show us how a recent Texas or NIBRS specification change reached production.
19. Show us the audit history for a changed record.
20. Show us how permissions differ for patrol, records, and a restricted case.
21. Where is agency data hosted, and who is responsible for each security control?
22. Show us how authentication and MFA work.
23. What is your incident-response process?
24. What exactly will you convert from our existing RMS?
25. What will not be converted?
26. How do we retrieve our data if we leave?
27. Who will implement and train our agency?
28. Who handles our support after go-live?
29. Which requested integrations exist in production today?
30. What will our total cost be over five years?

## Watch for these warning signs

- The demo is mostly dashboards. Ask them to process an incident.
- The vendor says yes without demonstrating the workflow.

- NIBRS is treated as a cleanup task or an export button. Reporting quality begins with the data captured during the work.
- Supervisor workflow is vague.
- Integrations require substantial re-entry.
- Historical conversion is described as "we'll bring everything over." Ask exactly what "everything" means.
- Audit history cannot explain important changes.
- Security is reduced to "we're CJIS compliant." Ask for specifics and documentation.
- Roadmap functionality is presented as available today. Ask: Can our agency use this in production right now?
- The vendor cannot explain how Texas or NIBRS changes reach production.
- Data export and exit terms are vague.

## The final question

After comparing workflows, reporting, search, security, conversion, implementation, support, and price, ask:

> *Does this system help our agency complete the work and keep a dependable record-or does it require staff to reconstruct that record afterward?*

Generated from the Thin Line Software resource library. Read this guide online: https://thinline.software/resources/texas-police-rms-evaluation-guide