

TECH & AI CASE STUDY - PAYMENTS PLATFORM - 2026

PCI-DSS 4.0 Readiness That Cut a Payments Platform's Audit Scope by 60%

Based on a delivery engagement with Ledgerline Payments

310 to 124

SYSTEMS IN AUDIT SCOPE

**6 weeks to 11
days**

EVIDENCE COLLECTION

100%

4.0 FUTURE-DATED REQUIREMENTS

zero

CRITICAL ASSESSMENT GAPS

A fillable practice edition: the full story, 8 actions,
6 reflections and a 90-day plan - work it with your team.

Free - no email required
emersontechnology.com

MAKE THIS PRACTICE BOOK YOURS

Work it, do not just read it

This practice book turns the Ledgerline Payments case study into a working session for your team. Read the full story first - what happened, what was built and what it changed. Then tick the 8 actions you can commit to, write short answers to the 6 reflections, and finish with a 90-day plan. Every field in this PDF is fillable: open it in Adobe Acrobat Reader, Chrome, Edge or macOS Preview, type directly into the boxes and save.

YOUR NAME	ROLE
COMPANY	TEAM / DEPARTMENT
DATE	EMAIL (OPTIONAL)

MY GOAL FOR THIS PRACTICE SESSION

- 01 The story** - What happened at Ledgerline Payments - before, during and after the project.
- 02 The results** - The numbers that changed, plus industry benchmarks from public research.
- 03 The 8-action checklist** - Tick boxes as your organization completes each step. Owner and date fields included.
- 04 The 6 reflections** - Fillable questions that pressure-test your own roadmap.
- 05 My 90-day plan** - Three fillable phase cards that turn this case study into your roadmap.

RUN IT AS A 90-MINUTE TEAM SESSION

25 min READ Read the story together. Ask everyone to note the one number that surprised them most.	40 min PRACTICE Work the 8-action checklist and the 6 reflections. Assign an owner and a date to every action you commit to.	25 min COMMIT Fill in the 90-day plan. One goal per phase, one number that tells you it worked. Book a review date before you leave the room.
--	--	---

THE STORY

What happened, and why it worked

01 The Company

Ledgerline Payments processes card payments for 2,300 mid-market merchants, providing the acquiring plumbing behind everything from regional restaurant groups to subscription e-commerce brands. The company's product is trust in two directions: merchants trust Ledgerline to move their money accurately, and the acquiring bank trusts Ledgerline to handle cardholder data to the letter of the Payment Card Industry Data Security Standard. That second relationship underpins the entire business — without a validating acquiring bank, Ledgerline has nothing to sell.

The engineering organization is card-first by necessity. Payment APIs, merchant onboarding flows, settlement pipelines, reconciliation tooling and a growing set of value-added services all live close to cardholder data, and the company's architecture had grown organically around that reality. Over several years, nearly every new service that touched payments in any way had been placed on the same network segment as the systems that store, process and transmit cardholder data. Convenience compounded: if a service could see the payment network, integration was easy, and nobody had ever priced what that ease cost at assessment time.

02 Where Things Stood

The cardholder data environment had grown to 310 systems on a largely flat network — every one of them in audit scope, every one needing quarterly evidence. Assessments consumed engineering for six weeks each cycle, and the work was almost entirely manual: screenshots of firewall rules, spreadsheets of system inventories, and patch reports assembled at the last minute by engineers pulled off roadmap work. The evidence binder, once complete, described a snapshot that began aging the day it was finished, and any drift between the snapshot and production was a finding waiting to be sampled.

Assessment season had also become an organizational event nobody planned for honestly. Requirements would arrive from the assessor, engineering would drop other work, and the six-week scramble would repeat with a new binder at the end of it — a cycle that taught the organization to treat compliance as an annual tax rather than an operating condition. The assessor's pre-read added a deadline to the discomfort. PCI-DSS 4.0's future-dated requirements — the heavy lifts the standards council had deferred to give organizations time — were coming due, including multi-factor authentication everywhere in the cardholder environment, script-integrity controls for payment pages, and documented targeted risk analyses wherever customized approaches replaced defined ones. The PCI Security Standards Council set March 31, 2025 as the effective date, with more than 50 new controls taking effect at once. Ledgerline's roadmap had no realistic capacity to absorb a compliance crunch in the same quarter as its product launches.

Leadership understood the stakes in existential terms. A failed or late validation threatened the acquiring-bank relationship, and without the bank there is no payments platform. Verizon's payment security research has reportedly found that only a minority of organizations remain fully compliant between formal validation cycles — compliance decays by default — and Ponemon Institute research reportedly puts the cost of non-compliance at 2.71 times the cost of maintaining it. Ledgerline was about to discover how expensive an oversized cardholder data environment makes both sides of that equation.

03 The Challenge

The challenge was structural before it was procedural. With 310 systems in scope, every requirement multiplied: 310 inventories to maintain, 310 sets of quarterly evidence, 310 systems to upgrade when MFA-everywhere arrived. Shrinking the environment was not one initiative among many; it was the initiative, because scope drives the cost of everything else. A program that hardened all 310 systems would spend a year of engineering and still leave the assessment treadmill running at full speed for the next cycle.

The second challenge was evidentiary. Auditors assess against evidence, and Ledgerline's evidence was hand-manufactured after the fact — a process that cannot survive continuous validation expectations and cannot scale even in theory. The third challenge was sequencing the 4.0 wave: with more than 50 future-dated controls landing simultaneously in March 2025, compressing them into deadline season would guarantee both quality problems and engineering burnout. The program needed to attack scope first, then build the 4.0 controls into the smaller environment, then make evidence collection a background process rather than an annual scramble — in that order, because each step makes the next one cheaper.

04 Discovery and Diagnosis

Emerson Technology opened with a three-week discovery that mapped every path cardholder data took through Ledgerline's platform, from merchant onboarding through authorization, settlement, chargebacks and reconciliation. The data-flow analysis produced the program's central insight: only a narrow set of systems genuinely needed to handle raw primary account numbers, yet the flat network meant 310 systems sat within the assessor's definition of the cardholder data environment. The gap between "touches card data" and "could touch card data" was the entire scope problem.

The diagnosis also inventoried the 4.0 future-dated requirements against current state, producing a gap list with real engineering estimates attached: MFA coverage across the CDE, script-integrity monitoring for the merchant-facing payment pages, targeted risk analysis documentation for the handful of customized controls the platform already operated, and the continuous-compliance expectations that turn annual evidence into an always-on obligation. Finally, the discovery examined the evidence process itself and found six weeks of annual engineer time spent manufacturing screenshots — a cost with no security benefit, pure assessment overhead. The remediation plan was sequenced accordingly: tokenize and isolate first, segment in code second, build 4.0 controls into the smaller environment third, and automate evidence collection throughout.

05 The Solution

The program attacked scope before controls, on the principle that every system removed from the cardholder data environment eliminates a full year of obligations — and then rebuilt the remaining environment around continuous, codified compliance.

Shrinking the cardholder data environment

A tokenization vault now holds cardholder data in an isolated enclave, and application servers receive tokens instead of raw card numbers. The effect on scope was immediate and permanent: systems that once handled PANs now handle surrogate values, and the assessed environment dropped from 310 systems to 124. Cloud-native segmentation, defined in Terraform, enforces the enclave boundary with continuous configuration checks rather than annual firewall screenshots — segmentation that lives in code survives audits in a way that screenshots never do, and drift between declared and actual configuration surfaces within a day instead of at the next assessment. Merchants gained a side benefit the roadmap had never promised: new services no longer enter the cardholder environment by default, which sped up onboarding architecture reviews.

The 4.0 controls, built early

The future-dated requirements were implemented a full quarter ahead of the March 2025 deadline, in the smaller post-tokenization environment where each control cost a fraction of its original estimate. Phishing-resistant MFA now covers every access path into the CDE. Script-integrity monitoring watches the payment pages — third-party scripts inventoried, every change validated through a controlled release process — satisfying the 4.0 integrity requirements that most processors were still scrambling to meet. Wherever Ledgerline customizes a control instead of following the standard's defined approach, a targeted risk analysis documents the risk, the compensating logic and the review cycle, because undocumented customization is a finding waiting to happen. Quarterly internal scans keep the vulnerability posture continuous rather than episodic.

Evidence as a pipeline

Evidence collection moved into a GRC platform that pulls configuration, scan and access data through APIs nightly. What was once six weeks of screenshot assembly became a background process: the evidence for "is the firewall configuration correct" is the live configuration, versioned and timestamped, rather than a picture of it. A QSA pre-assessment one quarter before the formal window converted the remaining unknowns into a remediation list while there was still time to work it calmly. The security team's assessment role shifted from manufacturer to reviewer — checking the evidence pipeline's output rather than producing it.

06 The First 90 Days

The first month was discovery plus the tokenization pilot: the data-flow map was completed in weeks one and two, the vault architecture was designed in week three, and the highest-volume payment path was migrated to tokens in week four as a live proof. The pilot mattered politically as much as technically — once engineering leadership saw a production flow running on tokens with zero customer-visible change, the remaining migrations became scheduling rather than debate. Weeks five through nine executed the migration wave by wave, with each retirement of raw card data access shrinking the scope inventory in real time and the Terraform segmentation landing in parallel.

Weeks ten through thirteen delivered the first 4.0 controls into the shrinking environment: MFA coverage was audited path by path and closed to full coverage, and script-integrity monitoring deployed against the payment page inventory built during discovery. The GRC platform's first API integrations went live in the same window — cloud configuration, the scanner and the identity provider — producing the first nightly evidence run before the quarter closed. The internal scan cadence moved from pre-assessment panic to standing schedule. By day 90 the scope count had fallen past the halfway mark, the evidence pipeline was collecting nightly, and the QSA pre-assessment was booked for the following quarter with an agreed remediation window behind it rather than an open-ended risk in front of it.

07 The Results

Assessment scope fell 60% — from 310 systems to 124 — and the next audit took eleven engineering days instead of six weeks. Every future-dated 4.0 requirement was implemented a quarter before the March 2025 deadline, and the QSA pre-assessment closed with zero critical gaps. Evidence collection now runs nightly through APIs, freeing the security team to fix risks rather than assemble screenshots, and merchants onboard faster because new services no longer enter the cardholder environment by default.

METRIC	BEFORE	AFTER
Systems in audit scope	310	124
Evidence collection	6 weeks	11 days

METRIC	BEFORE	AFTER
4.0 future-dated requirements	-	100%
Critical assessment gaps	-	zero

The compounding benefits are structural. The smaller cardholder data environment is cheaper to harden, faster to scan and simpler to explain to the acquiring bank, and the codified segmentation means scope cannot quietly regrow — a new system either fits the enclave patterns or it does not. Assessment season, once a six-week engineering tax, is now an exercise in reviewing evidence the platform already collects. The targeted risk analysis framework gave engineering a legitimate channel for the customizations a real platform requires, replacing informal exceptions with documented, reviewable rationale.

08 What Your Business Should Do

Ledgerline's experience compresses into a sequence any card-accepting organization can follow. Shrink scope before hardening systems: tokenize cardholder data and isolate it in the smallest possible enclave first, because every system removed from scope eliminates a full year of controls, scans and evidence obligations. Define segmentation in code — express network zones and firewall intent in Terraform or an equivalent, then check drift continuously, since segmentation that lives in configuration survives audits far better than screenshots. Automate evidence through APIs nightly by pointing a GRC platform at your cloud, scanner and identity systems; nightly collection makes every future assessment an exercise in review rather than manufacture.

Start the 4.0 future-dated requirements early — MFA everywhere, script-integrity monitoring and targeted risk analyses are the heavy lifts, so inventory them now and sequence them across quarters instead of compressing into deadline season. Document targeted risk analyses properly wherever you customize controls, writing down the risk, the compensating logic and the review cycle, because undocumented customization is a finding waiting to happen. Monitor payment-page script integrity by inventorying third-party scripts on checkout flows and validating every change through a controlled release process. Book a QSA pre-assessment one quarter before your validation window; it converts surprises into a remediation list while there is still time to fix findings calmly. And tie the compliance work to risk reduction — report scope reduction, vulnerability trends and incident readiness alongside requirement status, because framing PCI work as risk engineering keeps engineering teams engaged instead of treating it as tax. Move through these eight steps ahead of your next validation cycle using the action checklist in this practice book, and revisit the reflection questions when the assessor's pre-read arrives: how many systems sit inside your cardholder data environment and how many genuinely need to, what did your last assessment cost in engineer time, and if your acquiring bank called tomorrow about validation timing, would your evidence be ready within a week?

REAL-WORLD PROOF & BENCHMARKS

The PCI Security Standards Council set March 31, 2025 as the effective date for PCI-DSS 4.0's future-dated requirements — more than 50 new controls taking effect at once. - PCI Security Standards Council

Verizon's payment security research has reportedly found that only a minority of organizations remain fully PCI-DSS compliant between formal validation cycles. - Verizon Payment Security Report

Ponemon Institute research on compliance economics reportedly finds the average cost of non-compliance runs 2.71 times the cost of maintaining compliance. - Ponemon Institute

THE PRACTICE PAGES

The 8-action checklist

Work through the list with your team. Tick each box as your organization completes the step, and fill in an owner and a target date so every action has a name and a deadline.

☐

1. Shrink scope before hardening systems

Tokenize cardholder data and isolate it in the smallest possible enclave first. Every system removed from scope eliminates a full year of controls, scans and evidence obligations.

OWNER

TARGET DATE

STATUS

--	--	--

☐

2. Define segmentation in code

Express network zones and firewall intent in Terraform or an equivalent tool, then continuously check drift. Segmentation that lives in configuration survives audits far better than screenshots.

OWNER

TARGET DATE

STATUS

--	--	--

☐

3. Automate evidence through APIs nightly

Point a GRC platform at your cloud, scanner and identity systems so evidence refreshes without engineers. Nightly collection makes every future assessment an exercise in review.

OWNER

TARGET DATE

STATUS

--	--	--

☐

4. Start 4.0 future-dated requirements early

MFA everywhere, script-integrity monitoring and targeted risk analyses are the heavy lifts. Inventory them now and sequence them across quarters instead of compressing into deadline season.

OWNER

TARGET DATE

STATUS

--	--	--

☐

5. Document targeted risk analyses properly

Where you customize controls instead of following defined approaches, write down the risk, the compensating logic and the review cycle. Undocumented customization is a finding waiting to happen.

OWNER

TARGET DATE

STATUS

--	--	--



6. Monitor payment-page script integrity

PCI-DSS 4.0 requires integrity controls for payment-page scripts and headers. Inventory third-party scripts on checkout flows and validate every change through a controlled release process.

OWNER

TARGET DATE

STATUS

--	--	--



7. Run a QSA pre-assessment

Book a formal pre-assessment one quarter before your validation window. It converts surprises into a remediation list while there is still time to fix findings calmly.

OWNER

TARGET DATE

STATUS

--	--	--



8. Tie compliance work to risk reduction

Report scope reduction, vulnerability trends and incident readiness alongside requirement status. Framing PCI work as risk engineering keeps engineering teams engaged instead of treating it as tax.

OWNER

TARGET DATE

STATUS

--	--	--

AFTER THE CHECKLIST: OUR TOP 3 PRIORITIES

From the eight actions above, write down the three you will start first - and the single number you expect each one to move. Three priorities with owners beat eight without any.

PRIORITY 1 NUMBER IT SHOULD MOVE	PRIORITY 2 NUMBER IT SHOULD MOVE	PRIORITY 3 NUMBER IT SHOULD MOVE
--	--	--

THE PRACTICE PAGES

Reflections for your team

Use these questions in your next planning session and type short answers into the boxes. The gaps you find are usually the fastest wins.

Q1. How many systems sit inside your cardholder data environment today, and how many genuinely need to?

Q2. What did your last assessment cost in engineering time — and how much of that was screenshot assembly?

Q3. Which future-dated PCI-DSS 4.0 requirements are still on your backlog, and who owns each one?

Q4. If your acquiring bank called tomorrow about validation timing, would your evidence be ready within a week?

Q5. Where do you customize controls today without documented rationale a QSA could review?

Q6. Could tokenization remove your application tier from scope entirely — and what has stopped that conversation so far?

THE PRACTICE PAGES

My 90-day plan

Finish the session by committing to a plan. Three phases, one goal each, one number that tells you it worked. Bring this page to your next leadership review - or to a free consultation with Emerson Technology, and we will pressure-test it with you.

Days 1-30 Focus: audit and alignment

PRIMARY GOAL**KEY ACTIONS****HOW WE MEASURE SUCCESS****OWNER**

Days 31-60 Focus: build and prove

PRIMARY GOAL**KEY ACTIONS****HOW WE MEASURE SUCCESS****OWNER**

Days 61-90 Focus: scale and measure

PRIMARY GOAL

KEY ACTIONS

HOW WE MEASURE SUCCESS

OWNER

Tip: save a copy per team so each group keeps its own answers. Revisit the reflections every quarter - the questions stay the same even as the numbers move.

BOOK THE REVIEW BEFORE YOU CLOSE THE BOOK

Plans without a review date drift. Before you close this practice book, agree on when you will come back to these pages, who will run that session, and when you will check the numbers again. If you want an outside pair of eyes, bring this page to a free consultation with Emerson Technology and we will pressure-test the plan with you.

REVIEW DATE	REVIEWED BY	NEXT CHECK-IN
------------------------------------	------------------------------------	--------------------------------------

Ready for a transformation like Ledgerline Payments's?

Emerson Technology designs and builds the data, AI, cloud and automation systems behind results like these. On a free consultation call we will map this exact playbook to your business - your data, your constraints, your numbers.

Book a free consultation

support@emersontechnology.com

or start online: emersontechnology.com/contact