

Vendor invoice approval, Infrastructure Department

This report documents how vendor invoices were received, approved, and paid during the review period, assesses the controls around each step, and sets out recommendations with plans for adoption, ownership, and security.

Client	Stoneridge First Nation
Scope	Vendor invoices, from the email arriving to the vendor being paid
Invoices traced	30, received April to June 2026
People	Infrastructure reviewer, accounts payable clerk, senior administrator
Standards	BPMN 2.0 process maps · COSO 2013 control areas · RACI roles

Confidential

Prepared for Stoneridge First Nation, 14 August 2026. Not for distribution outside the Nation without its consent.

In this report

Part 1	Audit findings	2
Part 2	Change management	8
Part 3	Scope, ownership, and training	13
Part 4	Security and data governance	17
Part 5	Prototype	19
Part 6	Implementation proposal	23

PART 1

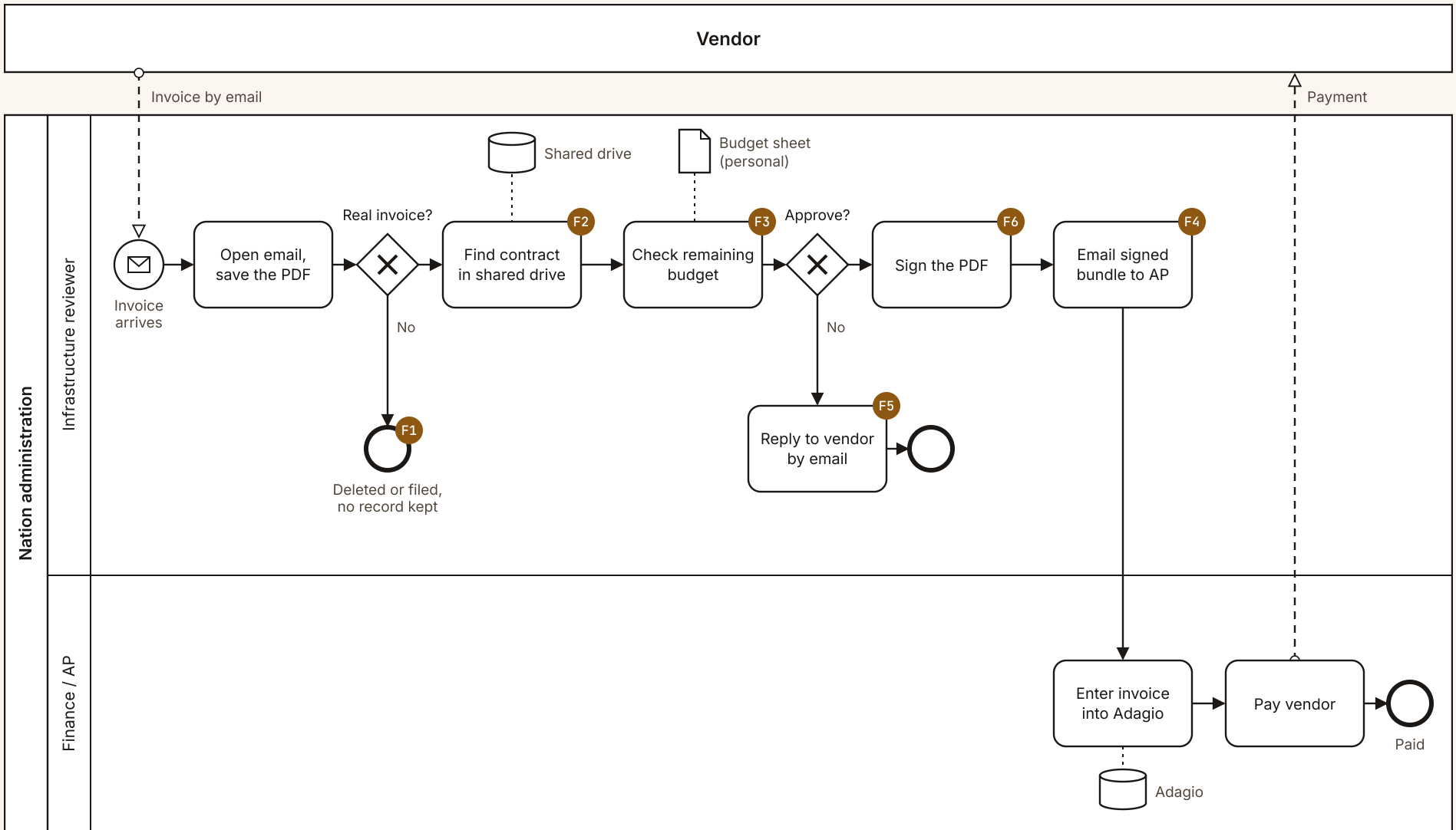
Audit findings

How vendor invoices are handled today, what the review found, and what should change.

1.1	Current process	3
1.2	Findings	4
1.3	Recommendations	5
1.4	Proposed process	6
1.5	Roles, method, and limitations	7

How an invoice gets paid today

BPMN 2.0. Each amber marker points to a finding on the next page.



Findings

Each finding is tagged with the COSO 2013 internal control area it falls under, the framework most auditors use. Ratings weigh likelihood against impact and were agreed with the senior administrator. None of the findings reflect on individual staff. Each is a gap in how the process is designed.

ID	FINDING	WHERE ON THE MAP	CONTROL AREA	RATING
F1	Screened-out emails leave no record. Quotes, statements, and duplicates are deleted or filed by whoever opens them. Nothing shows what was dismissed, or why.	"Real invoice?"	Control activities	Medium
F2	The contract match relies on memory. The reviewer searches the shared drive for the right contract. Nothing checks that the invoice lines actually match it.	Find contract	Control activities	High
F3	Remaining budget isn't visible at the moment of approval. It's checked against a personal spreadsheet updated monthly. An overspend on a funding agreement can first show up at year-end.	Check remaining budget	Information and communication	High
F4	The approval record is an email thread. Proof of who approved what, and when, is a signed PDF in someone's sent folder. Answering an auditor means searching inboxes.	Email signed bundle to AP	Monitoring activities	High
F5	Rejections and corrections aren't tracked. The reasons live in replies to vendors, so a vendor who keeps making the same mistake isn't visible to anyone.	Reply to vendor	Information and communication	Medium
F6	Only one person can approve. There's no named delegate and no written approval limit. When the reviewer is away, invoices wait.	Sign the PDF	Control environment	Medium

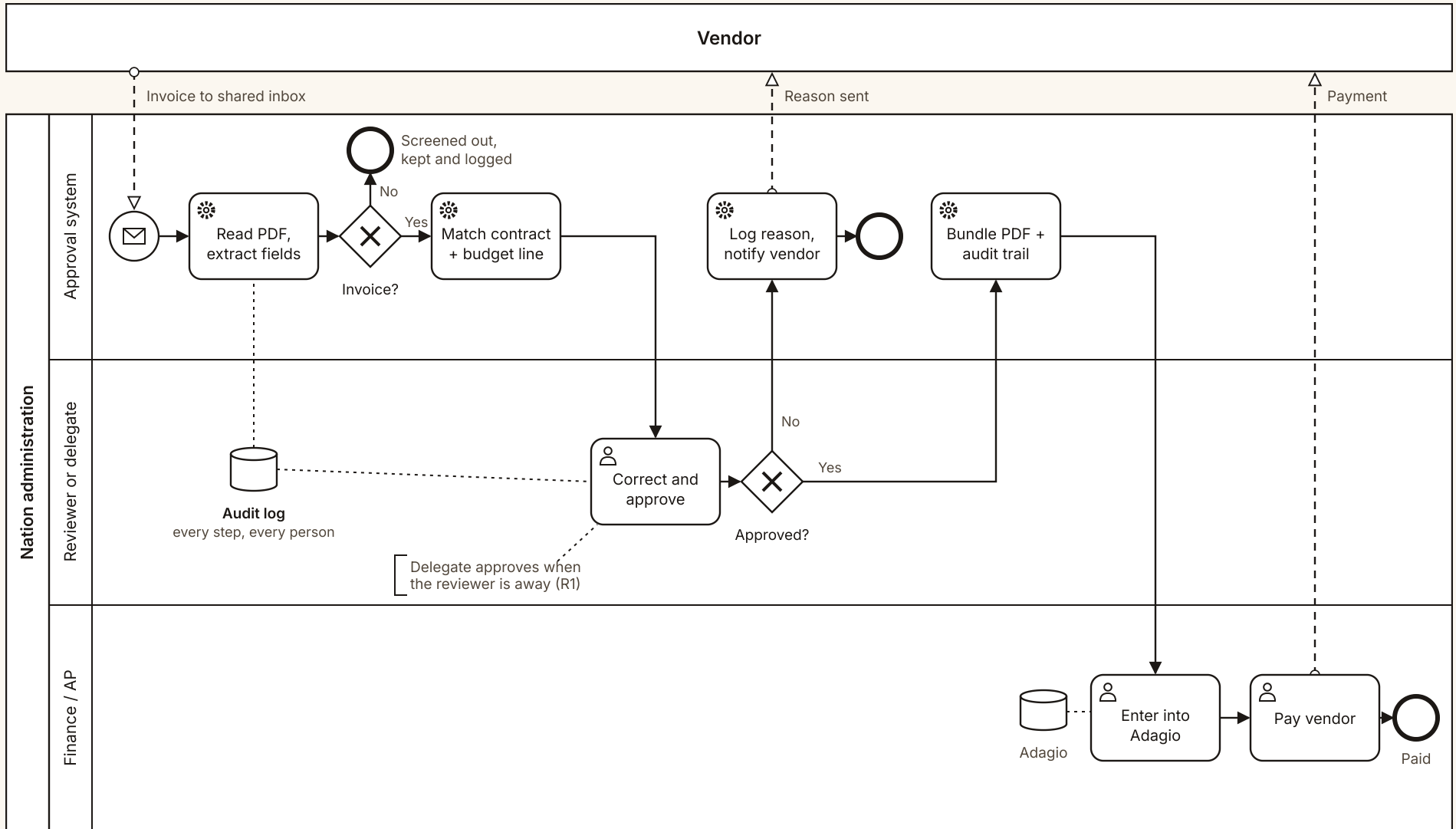
Recommendations

Listed in recommended order. R1 to R3 need no spending and can be implemented immediately. R3 is an interim control until R4 is in place. R5 records a part of the process that should not change.

ID	RECOMMENDATION	TYPE	FIXES	EFFORT	PRIORITY
R1	Name a delegate and write down approval limits. One page, signed by the senior administrator: who approves what, up to how much, and who covers when they're away.	Process change	F6	One meeting	Immediate
R2	Move vendors to one shared invoices inbox. More than one person can see it. Anything that isn't an invoice gets moved to a folder, not deleted, and rejections are replied to from the same inbox.	Process change	F1, F5	An afternoon	Immediate
R3	Add three lines to every invoice before it's signed. Contract number, budget line, and the balance left after this invoice. It makes both checks visible on paper until R4 is live.	Checklist	F2, F3	This week	Immediate (interim)
R4	Implement an approval system that records each step. It reads each PDF, screens out non-invoices, proposes the contract and budget line, and shows remaining budget beside each row. Every step is logged. AP receives one bundle with the trail attached. Adagio remains the accounting system of record.	Build	F1-F5	Two to four weeks	Short term
R5	Leave Adagio entry and payment as they are. It's quick, controlled, and done by one trained person. Automating it would add cost and risk for very little gain.	Leave as is	—	—	—

The same process with R1 to R4 in place

BPMN 2.0. The person still approves. The system does the looking up and the record-keeping. Screens are in Part 5.



Who does what, once it's in place

RACI: **R**esponsible, **A**ccountable, **C**onsulted, **I**nformed. One A per row.

Activity	Reviewer	Delegate	Finance / AP	Senior admin
Check screened-out items weekly	A/R	–	I	–
Correct and approve invoices	A/R	R	I	–
Set approval limits	C	C	C	A/R
Enter into Adagio	–	–	A/R	–
Pay vendor	I	–	R	A
Answer auditor requests	C	–	R	A

Method

We traced 30 invoices from one quarter, start to finish, over screen-share with the people who handled them. We interviewed the reviewer, the AP clerk, and the senior administrator, and walked through the shared drive, the budget sheet, and Adagio with them. No data was copied out of the Nation's systems.

The maps use BPMN 2.0, the international standard for process diagrams, so any analyst, auditor, or other vendor can read them.

 Start: message arrives

 Task done by hand

 Service task, automatic

 Next step

 Data store

 End

 User task, in the system

 Decision, one path

 Message between parties

 Finding marker

Limitations

The review covers 30 invoices from one quarter in one department. Other departments may work differently. The security review covers the invoice process only, with no penetration testing. Ratings are professional judgement, agreed with the senior administrator.

Sign-off

Prepared by	Xerad
Reviewed with	Marcus Hale, Senior Administrator · Dana Whitford, Infrastructure Reviewer
Date	14 August 2026

PART 2

Change management

How staff, Council, and vendors move to the new process, and how it stays in place.

2.1	Change management plan	9
2.2	Communications	10
2.3	Role guides	11
2.4	30-day review	12

Change management plan

The change is planned using ADKAR, a standard change-management model. Staff need awareness, desire, knowledge, ability, and reinforcement, in that order. If a stage is skipped, the old process tends to return. The materials are in sections 2.2 to 2.4.

STAGE	WHAT IT MEANS HERE	PLANNED ACTION	TIMING
Awareness	Staff understand why the process is changing: the findings in this report, not a new tool for its own sake.	A 30-minute briefing on this report for all staff who handle invoices. Vendors get 30 days' notice (2.2).	Before build
Desire	The reviewer and AP clerk see the benefit to them, mainly no more searching inboxes at year-end.	Both review the design before build and can remove any step that doesn't fit their work.	Build, week 1
Knowledge	Everyone knows the new steps for their role.	A one-page guide per role (2.3) and a recorded walkthrough.	Go-live
Ability	Staff can run the process in a busy week, not just in training.	Old and new processes run in parallel for two weeks, with implementation support on call.	Weeks 1–2 live
Reinforcement	The new process stays the default after implementation ends.	Check-ins at 30 and 90 days (2.4). Workarounds are treated as design problems and fixed in the system.	Day 30 and 90

Project partners

Senior administrator: sponsor. Signs off R1 and the go-live date. **Reviewer and AP clerk:** design input, then daily users. **Chief and Council:** short briefing on what changes and why. **Vendors:** 30 days' notice of the new invoice address.

Adoption risks and mitigations

Approvals continue by email. R2 routes every invoice to one inbox, so there's nothing to approve outside the system. **Staff turnover.** Role guides (2.3) let a new hire take over without the person who left.

What people hear before anything changes

Communications for the Awareness stage. Both are issued before the build starts.

AWARENESS • LETTER TO VENDORS

Stoneridge First Nation • Infrastructure Department • 1 September 2026

To our vendors,

Starting 1 October 2026, please send every invoice to **invoices@stoneridgefn.ca**. This replaces sending invoices to individual staff.

What we ask: one invoice per email, as a PDF, with the contract or PO number on it.

What doesn't change: your payment terms, and your contact in the Infrastructure Department.

Banking details: we will never ask you to change them by email. If you change them, we'll confirm by phone, using the number we already have on file, before any payment goes out.

Invoices sent to the old addresses will be forwarded for 30 days, then returned to you.

Questions: Dana Whitford, Infrastructure Reviewer, 250-555-0142

Marcus Hale
Senior Administrator

AWARENESS • 30-MINUTE STAFF BRIEFING

Agenda

- 1 Why we're changing: what the audit found (5 min)
- 2 What changes for you, role by role (10 min)
- 3 What doesn't change (5 min)
- 4 Your questions and concerns (10 min)

Questions people usually ask

Is this replacing my job?

No. It does the looking-up. You still decide, and your name is on every approval.

What if the system gets it wrong?

You correct it before approving. Every correction is logged, so we can see what it gets wrong and fix it.

Can I still approve by email?

Not after go-live. If you're away, your delegate approves in the system instead.

Who do I ask when I'm stuck?

For the first two weeks, the implementation team. After that, the reviewer.

One page per role, written for a busy week

Each person gets only their own steps. New staff start here, so the process doesn't depend on one person.

KNOWLEDGE • ROLE GUIDE: REVIEWER

Every day

- 1 Open the approval page. New invoices are at the top.
- 2 Check the proposed contract and budget line on each row.
- 3 Correct anything that's wrong. The system records what you changed.
- 4 Approve, or reject with a reason. The vendor is told automatically.
- 5 Once a week, scan the screened-out list for anything real.

When something's wrong

- | | |
|------------------------|---|
| No contract found | Pick it from the list, or flag it to the senior administrator. |
| Over budget | You'll see a warning. Approve only within your limit. Above it, send it up. |
| Looks like a duplicate | Reject as duplicate. Don't delete it. |

When you're away

Set your delegate and the dates before you leave. Your queue moves to them and comes back when you return.

KNOWLEDGE • ROLE GUIDE: FINANCE / AP

Every day

- 1 Open today's bundle. It has every approved invoice and its trail.
- 2 Enter each invoice into Adagio, as you do now.
- 3 Mark the bundle as entered.
- 4 Pay on your usual schedule.

When something's wrong

- | | |
|----------------------|--|
| Page missing | Reply inside the system, not by email, so it's on the record. |
| Bank details changed | Stop. Phone the vendor on the number already on file before anything else. |
| Totals don't match | Send it back to the reviewer with a note. |

When the auditor asks

Search the log by vendor, invoice number, or date, then export it as a PDF. Send the PDF, not an email thread.

The 30-day check-in: is it sticking?

Reinforcement stage. Results are compared with the week-one baseline, then reviewed for workarounds. A workaround means the system doesn't fit the work yet, so the system is adjusted, not the person.

MEASURE	BASELINE	DAY 30	NOTE
Invoices through the system	0%	94%	Two vendors still email the reviewer directly.
Days from arrival to AP	6.5	2.0	Measured from email timestamp to bundle sent.
Approved with no corrections	n/a	21%	About one in five. Most corrections are the budget line.
Approvals made by email	ALL	3	All three during the first week.

Workarounds found and actions taken

Two vendors still emailing the reviewer	Reminder letter sent. The reviewer forwards to the inbox instead of replying.
Reviewer printing bundles to check totals	A total row was added to the approval page. Printing stopped.
Delegate hasn't signed in yet	15-minute session booked before the reviewer's next leave.

Next check: day 90

Target: every invoice through the system and no approvals by email. If the no-corrections share hasn't moved, the budget lines it gets wrong are reviewed and the matching rules adjusted.

PART 3

Scope, ownership, and training

What Xerad delivers and when, who owns the system on the Nation’s side, and how staff are trained.

3.1	Scope and delivery	14
3.2	Product owner and change control	15
3.3	Training	16

Scope and delivery

What Xerad builds, what it doesn't, and how it is delivered. Scope is fixed at the start. Anything added goes through change control in 3.2.

In scope		Out of scope	
Vendor invoices, Infrastructure Department	From arrival in the shared inbox to the bundle reaching AP	Other departments' invoices	Roadmap item, assessed at day 90
Contract and budget-line matching	Against the contracts in the shared drive and the budget lines in Adagio	Purchase orders	Roadmap item
Approval, delegation, and audit log	As mapped in 1.4, with the limits set in R1	Changes to Adagio	Adagio is not modified or replaced
AP bundle	One PDF per day with the trail attached; Adagio entry stays manual	Payments	Payment stays with Finance as it is today
WHEN		DELIVERY	
Week 1	Design confirmed with the reviewer and AP clerk. Inbox set up. Vendor letter issued.	ACCEPTANCE	
Week 2	Build. Twenty real invoices from Q2 run through it as a test.	Signed design summary, one page	
Weeks 3-4	Parallel run. Old and new side by side. Role guides in use.	Test results, reviewed with the reviewer	
Day 30	Review against baselines (2.4).	Go-live sign-off by the product owner	
Day 90	Review. Roadmap decision on other departments.	30-day review	
		90-day review and recommendation	

Each stage is accepted by the product owner before the next begins. Acceptance means the delivery matches this report, not that the product owner is satisfied in general.

Product owner and change control

The Nation names one product owner before the build begins. Marcus Hale, Senior Administrator, has agreed to take the role.

The product owner

Decides	Priorities, changes, and the go-live date. Signs each acceptance in 3.1.
Owns	The success measures, the roadmap, and the relationship with Xerad or any later vendor.
Doesn't do	Approve invoices or operate the system day to day. That stays with the reviewer.
Time	About two hours a week during build, one hour a month after.

Success measures

Share of invoices processed through the system
Days from arrival to AP
Share approved with no corrections
Auditor questions answered from the log alone

Day-to-day contact

Dana Whitford, Infrastructure Reviewer. Raises issues, tests fixes, and keeps the role guides current. Backup: the AP clerk.

Change control

1. Request	Anyone on staff, through one form: what, why, and what happens if it isn't done.
2. Assess	Xerad estimates effort and flags any effect on the controls in 1.2 or the security requirements in 4.1.
3. Decide	The product owner approves, defers, or declines. Nothing is built without this.
4. Record	Who asked, who decided, when, and why, kept with the audit log.

Roadmap

Now: R4 as scoped. **Next:** other departments' invoices, decided at day 90 against the measures. **Later:** purchase orders. Options, not commitments.

Training

Delivered by Xerad during weeks 2 to 4. Every session is recorded and kept with the role guides (2.3), so it can be rerun for new staff without Xerad.

SESSION	WHO	LENGTH	COVERS
Product owner briefing	Marcus Hale	90 min	How the system works, what the log shows, how to read the success measures, how to run change control. Before go-live.
Reviewer and delegate	Dana Whitford, delegate	2 × 60 min	Approval page, corrections, delegation, the screened-out list. Second session on real invoices during parallel run.
Finance / AP	AP clerk	60 min	The daily bundle, Adagio entry, sending items back, answering an auditor from the log.
Council briefing	Chief and Council	20 min	What changed, why, and what the log now shows. Delivered by the product owner with Xerad present.

Ready for go-live when

The product owner has signed the design summary. The reviewer and delegate have each approved 20 real invoices in the system during parallel run. The AP clerk has entered one full bundle into Adagio. The auditor question in 2.3 has been answered from the log in a test.

Handover

At day 90, Xerad hands the product owner the documentation, admin access, the recordings, and a full data export. From then on the Nation can operate, change, or move the system without Xerad.

PART 4

Security and data governance

How the Nation’s data is owned and protected, assessed against OCAP® and NIST CSF 2.0.

4.1	Security and data governance	18
-----	------------------------------	----

Security and data governance

Data handling is assessed against the First Nations principles of OCAP®. Security is assessed against the six functions of the NIST Cybersecurity Framework 2.0. Scope is limited to the invoice process. This is not a network assessment or a penetration test.

OCAP®: requirements for R4

Ownership	The invoice records and the audit log belong to the Nation. This is stated in any implementation contract.
Control	The Nation decides who has access, including any vendor, and can revoke it at any time.
Access	Staff can export all records at any time, in standard formats.
Possession	Data is stored in Canada, in an account held by the Nation.

Security requirements for R4

- Multi-factor sign-in for every user
- Role-based access, reviewed quarterly
- Audit log that can't be edited
- Encryption in storage and in transit
- Daily backups, with tested restores
- Bank changes held until confirmed by phone

Security findings in the current process

ID	FINDING	NIST	RATING
S1	Bank detail changes arrive by email and aren't confirmed by phone. This is the most common way payments get redirected to fraudsters.	Protect	High
S2	The reviewer's email has no multi-factor sign-in, and it holds both invoices and approvals.	Protect	High
S3	Access to the shared drive isn't reviewed. Former staff may still have access.	Identify	Medium
S4	The budget sheet is kept on one laptop with no backup.	Recover	Medium

S1 and S2 can be fixed immediately, whether or not R4 goes ahead.

PART 5

Prototype

What R4 looks like in use, shown with Q2 invoices. The design is confirmed with the reviewer and AP clerk in week 1, before anything is built.

Open the working prototype →

Approve, reject, and correct real rows. The audit log fills as you go.

5.1	Approval queue	20
5.2	One invoice	21
5.3	Audit log	22

The reviewer's inbox

20 / 24

Correct, then approve

The PDF sits beside what the system read from it. Anything the reviewer changes is marked and logged. Approval limits from R1 are enforced here, not remembered.

approvals.stoneridgefn.ca/inbox/NE-1190

X Approvals

Inbox 7

Approved

Rejected

Screened out

Audit log

Contracts

Budgets

Inbox > Northline Electrical > NE-1190

Northline Electrical · \$9,600.00

Reject...

Send up: over budget

Invoice PDF as received

NE-1190.pdf · 1 page · received 12 Aug 2026 09:14

Over budget. This invoice leaves \$1,400 on C-2026-011. It's within your \$10,000 limit, but the budget line needs the senior administrator.

Vendor	Northline Electrical Ltd.
Invoice no.	NE-1190
Date	8 Aug 2026
Amount	\$9,600.00 incl. GST
Contract	C-2026-011 · Community hall lighting
Budget line	Facilities · Capital · 2026 edited
PO	None on invoice

TRAIL FOR THIS INVOICE

12 Aug 09:14 Received at invoices@stoneridgefn.ca

12 Aug 09:15 System: read PDF, matched C-2026-011 (high confidence)

12 Aug 09:15 System: budget line proposed Facilities · O&M

13 Aug 08:42 D. Whitford changed budget line to Facilities · Capital

Dana Whitford

Reviewer

This replaces the inbox search in F4. Finance filters by vendor, contract, or date and exports one PDF. Screened-out items and rejections are here too (F1, F5).

22 / 24

PART 6

Implementation proposal

What Xerad would deliver, on what terms, and what happens next.

6.1	Implementation package	24
-----	------------------------	----

Everything in this report, implemented and run for a year

One fixed price covers the build and every plan in the report. You don't buy the pieces separately.

\$15,000

FIXED • ALL-IN • FIRST YEAR

Less the \$2,500 audit fee already paid: **\$12,500** due

What's included

The approval system (R4)	Built to the process in 1.4, the screens in Part 5, and the security requirements in 4.1.
Change management	The plan in 2.1, with every material in 2.2 to 2.4 written and delivered.
Product ownership setup	Success measures, week-one baselines, and the change-control process in 3.2.
Security and data	OCAP® requirements built in and tested. Help closing S1 and S2.
First year of running it	Monitoring, fixes, support, and the 30- and 90-day check-ins.

Not included

AI and hosting	Billed at cost, separately.
Changes outside scope	Quoted before any work starts.

What you keep

Documentation, admin access, and a full data export. If you stop working with us, the system keeps running and it's still yours.

Timeline

WEEKS 1-2
Build

WEEKS 3-4
Parallel run

DAY 30
Check-in

DAY 90
Check-in

MONTH 12
Review and renewal

01 • CONFIRM

The product owner confirms scope (3.1) and a start date. Valid for 90 days from 14 August 2026.

02 • SIGN

A one-page agreement: this report is the scope. Half on signing, half at go-live sign-off.

03 • BEGIN

Week 1 starts with the design session with Dana Whitford and the AP clerk, and the vendor letter (2.2).