



Nozawa Hospitality Discovery & Planning Engagement

Prepared for

Hannah Wilke, Peter Douglas, Nozawa Hospitality

April 14, 2026



Contents

At a glance	3
Why this engagement	3
What we already know	4
Email, domain configuration, and the Ricoh MFP	4
Website security and form spam	4
Website content and asset hygiene	5
Data and customer information handling	5
Opera migration	5
General IT infrastructure	6
What Discovery will produce	6
Discovery scope	7
Engagement timeline	8
Discovery-paired immediate remediation	9
Total range for remediation labor	10
Pricing summary	10
How we'll work together	11
What we'll need from you to begin	11
Next steps	12
Contact Us	13

At a glance

Engagement	Discovery & Planning
Duration	Two to three weeks from kickoff to delivery
Discovery fee	¥500,000 (fixed, exclusive of consumption tax)
Discovery-paired immediate remediation	¥252,000 – ¥432,000 depending on confirmed scope
Operating Baseline ongoing subscription	¥420,000/year (required if remediation item 3 is authorized)
Lead consultant	Rick Cogley, eSolia Inc.
Deliverable	Written assessment, architecture and integration recommendations, prioritized roadmap, and a 60–90 minute walkthrough with your decision-makers
Discovery credit	¥50,000 of the Discovery fee is credited against any Build engagement started within 90 days

Why this engagement

In our March Teams meeting with Peter Douglas and Hannah Wilke, your team described several significant things happening at once: a major migration from RoomBoss to Oracle OPERA Cloud planned for completion by end of October — motivated partly by a perception that Opera offers better security than the current setup — a website rebuild conversation where the development team hasn't yet been chosen but you've indicated a preference for someone local, a recent change in ownership with the new Indonesian parent company evaluating how the business will be structured going forward, and a set of operational concerns around email deliverability, the Ricoh multi-function printer's scan-to-email function, persistent form spam that Forage Studio eventually addressed with a CAPTCHA, and questions about whether the current booking URL structure is predictable enough to be a security concern.

In her follow-up email of April 11, Hannah summarized what your team is most interested in exploring with eSolia: securing your business email accounts, reviewing and strengthening the security of your booking systems and websites, general IT infrastructure advice including networks, backups, and access control, and clarity on how eSolia can support the new website project regardless of which developer builds it. She also asked the broader question that defines this proposal: what would we recommend for a business like Nozawa, what would it cost to set up, and what would it cost to operate.

The honest answer to that question is that we want to do a focused, paid assessment first. There's too much happening across too many systems for any responsible advisor to quote a firm number without understanding the specifics of your environment. **Discovery & Planning** is that focused assessment — two to three weeks of structured work led by a Senior Consultant, ending in a written document you can use to make decisions, whether you continue with eSolia afterward or not.

Because some of the things you've already described shouldn't wait for the full assessment to be written, we're also proposing a small **immediate remediation** package that runs in parallel with Discovery. It's a separate scope and a separate fee, so the Discovery investment stays predictable while urgent fixes get done in the same window.

What we already know

This section is a deliberate departure from how a typical agency would write a proposal at this stage. We're naming what we already know because the NDA is in place, because Hannah's email asked us to be specific, and because pretending not to have noticed things would waste the trust your team showed by being open with us in March.

These observations come from two sources: the conversation in the Teams meeting and a structured external review of the live `nozawahospitality.com` site that we conducted before sending this proposal. We haven't looked at any of your underlying systems, the internal domain configuration, your Google Workspace tenant, or your booking-system configuration — those are the things Discovery will examine.

Email, domain configuration, and the Ricoh MFP

You described email delivery problems on Google Workspace — messages going missing or landing in junk folders — and reported that the Ricoh multi-function printer isn't sending scanned documents by email reliably. We've seen this pattern several times with clients whose email environment evolved over years without a single team owning the operational picture. Something upstream changes — a security setting, a domain record, a mail relay — and devices that previously worked quietly stop working. The cause isn't always the same, but once we can see how everything is currently configured, the diagnosis is usually straightforward.

We'd fix both issues as part of the immediate remediation package described later in this proposal, and we'd set up continuous monitoring through our own system, eSolia Periodic, so that any future change affecting email delivery or domain configuration is flagged the same day it happens rather than discovered weeks later.

One thing we noticed from the public side: your domain is registered through GoDaddy, which is fine, but it's also the kind of registrar where control and visibility can drift over years as staff and vendors change. Part of the email and domain cleanup work is making sure you have a clean, documented picture of who controls the domain and how.

Website security and form spam

You mentioned in the meeting that form spam was a serious problem until Forage added a CAPTCHA, which addressed it. That's a reasonable fix for an existing site, but it's also an example of a pattern we see a lot: security problems that are handled reactively after they cause pain, rather than designed out from the start. If eSolia is involved in the new website from the beginning — whether we build it or we work alongside the developer you choose — protection against automated abuse, filtering of malicious traffic before it reaches the site, and hiding the site's back-end from direct public exposure are part of the initial design rather than something added later in response to a specific incident.

You also raised a concern about the predictability of the current booking URLs on RoomBoss — the worry being that people outside your team might be able to guess valid addresses and reach things they shouldn't. You mentioned that part of the reason for moving to Oracle OPERA Cloud is a perception that it offers better security than the current setup. This is a reasonable expectation, but it's also the kind of expectation that only gets delivered if the Opera integration is designed carefully from the start: how the addresses are structured, how guests and staff sign in, how their sessions are tracked, and who can see what — these are design decisions, not things that come for free with a new booking system. Part of what the Opera architecture review in Discovery will cover is exactly this: making sure the new booking experience, whichever integration path you choose, delivers the security improvement you're hoping for.

On putting Cloudflare in front of the existing Webflow site. This is a common and well-supported configuration. Cloudflare and Webflow maintain a formal partnership for this specific use case, which lets Cloudflare sit between visitors and your Webflow site — filtering bad traffic, blocking automated abuse, and applying protective rules before anything reaches Webflow at all. The Webflow site still works exactly as it does today; Cloudflare just adds a protective layer on top of it. The setup is straightforward, works on any Cloudflare plan (including the free plan), and is one of the first things we'd put in place during the immediate remediation window.

Website content and asset hygiene

During our pre-meeting review of the live site we noted a number of small but cumulative content and quality issues that suggest the site hasn't been actively maintained as the business has evolved — placeholder text still visible in some property cards, duplicated logos in the footer carousel with at least one typo, inconsistent capacity formats across cards, a typo in the footer address, and image filenames that suggest careless export hygiene. None of these are catastrophic. All of them are the kind of thing that accumulates when nobody owns the operational side of the website and the development team is slow to respond to small requests. We mention them not to criticize the site but because they're the visible surface of a deeper pattern — a website that's no longer being treated as a maintained operational asset. They're part of the context for the conversation about what you should expect from a properly operated site going forward.

Data and customer information handling

The forward-looking picture — how customer data enters, moves through, and leaves your systems once the Opera migration is complete — is one of the things Discovery will examine and produce specific recommendations for. We're not proposing a forensic investigation of any past incident; that's specialist incident response work and it's beyond the scope of Discovery. What we are proposing is a clear-eyed look at where customer data will live, who will have access to it, how it will flow between the website, the booking layer, and any integrated systems, and what the practical security and privacy posture should look like going forward.

Opera migration

You mentioned that you're planning to migrate to Oracle OPERA Cloud by end of October. This is a significant infrastructure change with consequences for the website, the booking experience, the data flow between your properties and your guests, and the security posture of the whole booking layer. We've done our own background research on the Oracle Hospitality ecosystem so we can advise you on this intelligently, and we'll share the relevant findings as part of the Discovery deliverable.

The short version, for the purposes of this proposal: there are three realistic ways to connect a new website to OPERA Cloud — Oracle’s own built-in booking engine running on a separate web address, a specialist third-party booking engine that already connects to Opera (several vendors offer this), or a fully custom booking experience we’d build from scratch. Each has a different cost, complexity, and control profile. **eSolia doesn’t need to be your Opera implementation partner to add significant value here.** What we can do, and what nobody else in your current vendor ecosystem will do without prompting, is make sure all the pieces fit together cleanly — the website, the booking experience, the Opera system, the domains and web addresses, the email environment, and your day-to-day IT — so that whoever you choose for Opera implementation and whoever you choose for the website rebuild can do their parts without stepping on each other.

Discovery will produce a written architecture review of the Opera integration choices specifically, with a recommendation that explains the trade-offs of each path so you can make this decision with your eyes open before committing to any vendor for that part of the work.

General IT infrastructure

Hannah’s email asked specifically about networks, backups, and access control. We haven’t yet looked at your internal IT environment, your network configuration, your backup posture, or how administrative access is granted across your various systems. This is Discovery work. What we can say up front is that the pattern of issues you’ve described is consistent with an environment where IT decisions have been made reactively over several years, by different vendors, without a single team responsible for the operational picture. This is normal for businesses your size, and it’s also exactly the kind of situation where a focused assessment produces a quickly actionable plan.

What Discovery will produce

The Discovery deliverable is a single written document, delivered as a PDF, with a Markdown source available if you want it for your own records. It covers everything in the scope section below. You’ll receive it within two to three weeks of engagement kickoff.

Beyond the document itself, Discovery includes a 60 to 90 minute walkthrough meeting with you and any decision-makers or other stakeholders you want to include, where Rick walks through the findings, answers questions in real time, and discusses the recommended next steps. Two weeks of follow-up email Q&A are included after delivery, so you and your team can ask clarifying questions as you absorb the document.

The deliverable is written for two audiences at once: the operational decision-makers on your team who need to act on it, and any parent company or other stakeholders who may need to review it without the same context. It includes both an executive summary and the technical detail that supports each finding.

The document is yours to keep regardless of what you decide next. If at the end of Discovery the right answer is “stay on Webflow with your current developer and just have eSolia handle email and security,” we’ll say so, in writing. If the right answer is a multi-year program of work with eSolia as your operational partner, we’ll say that too, and explain why.

Discovery scope

Discovery is structured as seven workstreams, each of which produces a section in the final document.

1. Email and domain hygiene. We'll inventory the current domain configuration for `nozawahospitality.com` and any related domains, confirm that email authentication is set up correctly, identify the causes of the Google Workspace delivery problems and the Ricoh scan-to-email issue, and produce a corrected configuration with a recommended monitoring approach. This workstream feeds directly into the immediate remediation package.

2. Website security review. We'll do a structured external review of the live website's security posture — confirming that site encryption is properly configured, that the right protective rules are in place, that no parts of the site are unintentionally exposed, and that the site behaves sensibly under automated traffic — and identify the specific gaps that matter most for the months between now and the Opera go-live. This is an external review only; we won't test the booking flow with live traffic or do anything that could affect production operations.

3. Booking and data flow review (forward-looking). Because you're moving away from RoomBoss later this year, we won't spend Discovery time on a deep review of the current booking system. Instead we'll focus on the data flows that matter going forward: how customer data will enter and leave the new Opera environment, where the security boundaries sit, and what the integration layer between Opera and the new website needs to look like to be secure and maintainable.

4. Opera migration architecture review. We'll produce a written architecture review of the Opera integration choices for your specific situation, covering the three realistic paths (Oracle's built-in booking engine, a specialist third-party booking engine, or a fully custom build), the trade-offs of each, and a recommendation for the path that fits your timeline, budget, and operational capacity. This section will also include a list of specific questions for your Oracle implementation partner if you have one, or a discussion of what to look for in choosing one if you don't. The goal is that you have a defensible position on Opera architecture before committing to any vendor for that part of the work.

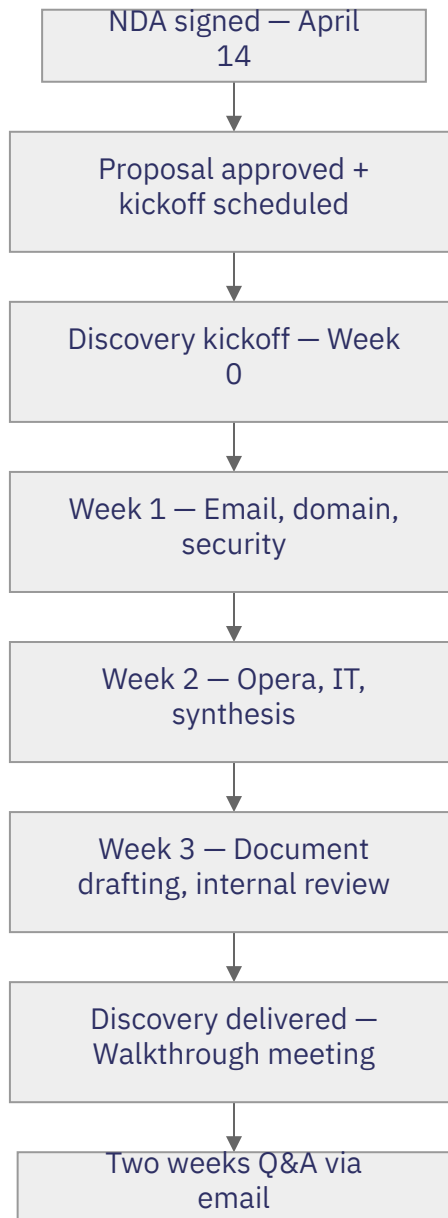
5. Website rebuild — architectural options. We'll document the current state of the website and the realistic options for the rebuild itself. We won't recommend a specific developer or design studio unless you specifically ask us to — that's your team's decision and it depends on factors (budget, brand sensibility, working relationship, local presence) that you're better positioned to weigh than we are. What we'll recommend is the architectural shape of the engagement: which technical decisions should be made by the website developer, which should be made by eSolia as the operational partner, and how the two roles should fit together.

6. General IT infrastructure assessment. We'll conduct a high-level review of the IT environment supporting the business: endpoints, operating systems, backup posture, and how administrative access is granted across your various systems (Google Workspace, the website CMS, the booking system, the domain registrar, and so on). The goal is to identify the most important gaps and produce a prioritized list of recommendations. This isn't a full IT audit — that would be a separate engagement if you wanted one — but it's enough to give you and your team a clear picture of what to do next.

7. Recommended ongoing services and roadmap. The final Discovery section ties everything together: which eSolia services we recommend you adopt on an ongoing basis, in what order, at what monthly cost, and with what expected outcomes. eSolia's web services are structured as a flexible monthly

subscription — clients pick the services that fit their situation rather than buying a fixed package — and Discovery is where we recommend the specific configuration that fits yours. The recommendation is fully itemized so you can see what each service contributes and adjust the mix if needed.

Engagement timeline



Diagram

The Discovery-paired immediate remediation work runs in parallel with weeks 1 and 2, on a separate track but coordinated with the same lead consultant.

Discovery-paired immediate remediation

The following items are scoped as a separate work package that runs alongside Discovery. They're quoted separately so the Discovery fee stays a fixed, predictable amount and so the immediate fixes can begin as soon as you approve the proposal, without waiting for the full assessment to be written.

1. Email and domain configuration cleanup. Audit and correct the current email authentication and domain configuration for `nozawahospitality.com`, coordinate with your Google Workspace admin to verify the fix end-to-end, and set up continuous monitoring through eSolia Periodic so future drift is caught the same day it happens. Includes working with GoDaddy as the current registrar or, if appropriate, moving domain management to a more operationally friendly setup. Estimated effort: 6 to 10 hours of engineering time, **¥108,000 – ¥180,000**.

2. Ricoh multi-function printer scan-to-email fix. Diagnose the specific cause of the Ricoh problem (most commonly, the printer was configured to send mail through a path that worked under older settings and needs to be updated for how Google Workspace handles mail today, though the exact cause isn't knowable until we can see the device and how it's currently set up), implement the fix, and test from multiple device functions. Estimated effort: 4 to 8 hours of engineering time, **¥72,000 – ¥144,000**. The range reflects real uncertainty in this kind of fix — simple cases resolve in half a day, harder cases involve firmware quirks or vendor coordination and take a full day.

3. Cloudflare protective layer in front of the existing website. Set up Cloudflare in front of the current Webflow site using the documented Webflow partnership pattern, configure protective rules to block automated abuse before it reaches the site, enable filtering of bot traffic, harden the browser-facing security settings, and put basic uptime monitoring in place. This directly addresses the ongoing need for automated-abuse protection that a CAPTCHA alone doesn't cover. Estimated effort: 4 to 6 hours of engineering time, **¥72,000 – ¥108,000**.

Important note on the Cloudflare item and the Operating Baseline. When eSolia sets up Cloudflare for a client, the resulting configuration needs ongoing, if light, stewardship — protective rules occasionally need tuning, monitoring alerts need eyes, configuration drift needs to be caught before it causes problems. None of this is intensive work, but all of it requires a person who knows the setup and is available when something comes up. For this reason, authorizing remediation item 3 commits Nozawa Hospitality to eSolia's **Operating Baseline** ongoing subscription, starting from the first of the month after the Cloudflare setup goes live. The Operating Baseline is ¥420,000/year, billed annually in advance, and is prorated for the first year based on when the Cloudflare setup goes live. It includes ongoing maintenance of the Cloudflare configuration, continuous domain and email monitoring through eSolia Periodic, uptime monitoring, weekly backups with monthly verification, the automated security dashboard, bilingual support during Japan business hours, and a monthly work report. Full details are in the Web Services Investment Overview attached with this proposal.

We are being explicit about this upfront rather than letting it surprise you at Discovery delivery, because we have seen other firms deploy Cloudflare setups without a maintenance relationship and leave clients with what effectively becomes operational orphan infrastructure — something that works on day one, slowly drifts out of alignment with the client's evolving needs, and eventually breaks without anyone noticing. That is not a situation we are willing to create for Nozawa Hospitality.

Total range for remediation labor

¥252,000 to ¥432,000 depending on which items you authorize and actual effort within the estimated ranges. We bill these as time-and-materials within the agreed range, with a written status update at the midpoint and final actuals captured in a Monthly Work Report at the end of the month.

You can authorize all three remediation items, a subset, or none. Discovery proceeds either way — the remediation package is parallel work, not a precondition. One thing to note about item 3 specifically: if you authorize it, you are also committing to the Operating Baseline ongoing subscription as described above. Items 1 and 2 (email/domain cleanup and the Ricoh fix) can be authorized on their own without triggering any ongoing commitment.

Pricing summary

Item	Fee	Billing
Discovery & Planning	¥500,000	Fixed, invoiced at engagement start
Immediate remediation — email and domain cleanup	¥108,000 – ¥180,000	T&M within range, invoiced at start of work
Immediate remediation — Ricoh MFP	¥72,000 – ¥144,000	T&M within range, invoiced at start of work
Immediate remediation — Cloudflare protective layer	¥72,000 – ¥108,000	T&M within range, invoiced at start of work
Operating Baseline (required if Cloudflare item authorized)	¥420,000/year	Billed annually in advance, first invoice prorated from the first of the month after Cloudflare go-live
One-time engagement cost — Discovery + all remediation	¥752,000 – ¥932,000	
First-year ongoing (prorated) — Operating Baseline from Cloudflare go-live through year end	typically ¥210,000 – ¥280,000	depending on when in the year Cloudflare goes live
Year 2 and after	¥420,000/year	plus any additional services added after Discovery

First-year total if you authorize Discovery and all three remediation items: approximately **¥962,000 – ¥1,212,000** in eSolia fees, depending on actual remediation effort and Operating Baseline proration. The Cloudflare subscription (~¥530,000/year, approximately ¥265,000–¥353,000 prorated for the first year) is additional and is paid either directly to Cloudflare or passed through on our invoice — see the note below.

All fees exclusive of Japan consumption tax (currently 10%).

¥50,000 of the Discovery fee is credited against any Build engagement started within 90 days of Discovery delivery, making the effective Discovery fee ¥450,000 in that case.

The immediate remediation ranges are estimates based on what we already know. Actual effort depends on what we find when we open the systems. We'll give you a written status update before reaching the top of the estimated range on any item, so you have the chance to scope down or stop the work before it goes over.

How we'll work together

Single eSolia lead. Rick Cogley (Senior Consultant, eSolia Inc.) is the consistent point of contact and the author of the Discovery deliverable. Specialist staff are brought in as needed under his coordination.

Single client decision-maker. We work best with one person on your side who has the authority to grant access, make scoping decisions, and review interim findings. Hannah has been the primary contact so far; if she remains in that role for Discovery we'll plan on it. If you'd like a different point of contact, please let us know.

Weekly check-ins. Discovery includes two scheduled check-in conversations during the engagement (around end of week 1 and end of week 2), each 30 to 45 minutes, where Rick walks through what's been found so far and surfaces any blockers. These are working sessions, not status presentations.

Asynchronous communication. Email is fine for most things. We can set up a shared communication channel of your choice (Slack, Teams, or simple email) at kickoff if you'd like one for the longer-running items.

Confidentiality. Everything in the engagement is covered by the executed NDA. Findings about your specific environment stay strictly within the engagement and aren't shared with other parties without your written authorization.

What we'll need from you to begin

To start the engagement effectively, we'll need the following during the first few days after kickoff:

- **GoDaddy registrar access** for `nozawahospitality.com` and any related domains, or a path to making changes when fixes are required
- **Google Workspace admin access** (read-only is fine for assessment; admin access required for the deliverability fix)
- **Webflow admin or editor access** for the current site, ideally read-only for assessment
- **A point of contact at the current website development team** if they're still actively engaged on the site, so we can coordinate any changes without surprising them
- **Whatever you have so far about the Opera migration** — Oracle account team contact, implementation partner if any, modules in scope, target go-live date, and any architecture documents
- **Network access** to the property where the Ricoh MFP is located, either through a remote session with someone on-site or through a brief on-site visit, depending on what the diagnosis requires

- **A short list of people** on your team and in any parent company or other stakeholder group who should be included in the walkthrough meeting at the end of Discovery

Missing items don't block the engagement from starting — they just shape what we can include in the assessment. We'll work with what's available and document the gaps in the deliverable.

Next steps

To proceed:

1. **Review this proposal** with whoever on your side needs to approve it.
2. **Approve the Discovery scope** and confirm which items of the immediate remediation package you want included. A short email reply confirming approval is sufficient; a formal signature is welcomed but not required for engagement start.
3. **Schedule the kickoff meeting** — typically a 60-minute call, ideally within a few business days of approval. We'll use the kickoff to confirm scope, exchange access credentials securely, and agree on the working schedule for the next two to three weeks.
4. **Discovery begins.** From kickoff, the deliverable arrives in two to three weeks, with the immediate remediation work happening in parallel throughout that same window.

We're ready to begin within two business days of your approval.

If you have questions about anything in this proposal — the scope, the pricing, the timeline, or the way we plan to work — please reply directly to Rick at the contact details provided, or schedule a brief call. We're happy to revise the scope based on your feedback before you commit.

Thank you for the trust you've shown in opening this conversation with us. We're looking forward to the work ahead.

Contact Us

eSolia Inc. Shiodome City Center 5F (Workstyling) 1-5-2 Higashi-Shimbashi, Minato-ku Tokyo 105-7105, Japan

Phone	03-4577-3380
Email	hello@esolia.co.jp
Web	https://esolia.co.jp/en
Hours	Monday-Friday, 9:00-18:00 JST