



EXTERNAL VULNERABILITY ASSESSMENT · FTC SAFEGUARDS RULE PROGRAMS

External Vulnerability Assessment Report

Assessment 1 of 2 for this plan year, with a Safeguards Rule mapping and assessment letter.

CLIENT

Lone Oak Tax & Bookkeeping

WEBSITE

www.loneoaktax.example

REVIEW WINDOW

October 5-9, 2026

REPORT ID

NYX-SAMPLE-SG-001

Confidential — prepared for the named client only. This sample uses a fictional business and the reserved .example domain; all findings are illustrative.

01 — EXECUTIVE SUMMARY

Where the firm stands

Assessment 1 of 2 in the current plan year. Written for the owner and the firm’s Qualified Individual. Technical details start in section 04.

OVERALL RISK

HIGH

Driven by a client spreadsheet indexed by Google (F-01). Expected to drop to **Medium** once the “fix this week” list is done, and to **Low** once all findings are fixed.

What we looked at. The firm’s website, its forms and login pages, subdomains in public certificate logs, the client portal’s public settings, email domain records and the email address provided at checkout. Everything was reviewed from the outside.

What we found. Client documents go through a secure third-party portal, which is good. The weak points are around it: an old spreadsheet with client names sits in a public folder and shows up in Google, an intake plugin has a published vulnerability, and nothing stops criminals from sending tax-season emails in the firm’s name.



What this means for the firm

BUSINESS RISK	WHY IT APPLIES HERE	FINDINGS
Exposed client data	A spreadsheet listing clients and engagement details can be found through Google. Under the Safeguards Rule, an incident involving 500 or more consumers must be reported to the FTC within 30 days of discovery.	F-01
Tax-season phishing	Without DMARC, fake emails “from the firm” asking clients for documents or payment can land in their inboxes.	F-02
Website compromise	A known vulnerability in the intake plugin gives attackers a ready-made way to read submitted forms.	F-03

Safeguards Rule context

This report is the external, internet-facing part of the vulnerability assessments described in 16 CFR 314.4(d)(2). Appendix A shows which elements of the Rule it covers, partly covers or does not cover. Appendix B is the dated assessment letter for the firm’s security records.

02 — ACTION LIST

What to fix this week

One page for whoever manages the website and email. Tick each box when done. We will check these items again in the second assessment.

- ☐ **Remove the client spreadsheet and close the folder** **CRITICAL**
Delete the file, turn off directory listing, and ask Google to remove the result. Then decide with your Qualified Individual whether this is a notification event. **F-01**
- ☐ **Publish a DMARC record** **HIGH**
Start in monitoring mode before tax season, then move to enforcement. **F-02**
- ☐ **Update the intake form plugin** **HIGH**
Update QuickIntake Forms to the current version and turn on automatic plugin updates. **F-03**
- ☐ **Turn on two-factor login for WordPress** **MEDIUM**
The Rule requires multi-factor authentication for anyone accessing an information system (314.4(c)(5)). **F-05**
- ☐ **Change reused passwords for the admin mailbox** **MEDIUM**
The address appears in a breach that exposed passwords. **F-06**

All findings

ID	FINDING	SEVERITY	WHERE IT'S FIXED
F-01	Client spreadsheet in a public folder, indexed by Google	CRITICAL	Website files
F-02	No DMARC record — email can be spoofed in the firm's name	HIGH	DNS settings
F-03	Intake form plugin with a published vulnerability	HIGH	WordPress dashboard
F-04	Key security headers missing on the main website	MEDIUM	Website files (.htaccess)
F-05	Username exposed and login page without two-factor	MEDIUM	WordPress dashboard
F-06	Checkout email in 2 breaches, one with passwords	MEDIUM	Your own accounts
F-07	Outdated TLS 1.0 and 1.1 still accepted	MEDIUM	Hosting / CDN settings
F-08	Directory listing enabled on the uploads folder	LOW	Website files (.htaccess)
F-09	No security.txt file for reporting problems	LOW	Website files

03 — SCOPE AND METHOD

What we checked, and how

An external, non-intrusive assessment of everything connected to the firm's domain that is visible from the internet.

ITEM	DETAILS
Client	Lone Oak Tax & Bookkeeping (fictional), Round Rock, Texas
In scope	loneoaktax.example, www. and all subdomains found in public certificate logs
Third-party portal	portal. (client document portal run by a vendor): public settings, TLS and headers only
Checkout email	admin@loneoaktax.example (breach lookup only)
Review window	October 5–9, 2026 · next assessment due April 2027
Report ID	NYX-SAMPLE-SG-001

What we did

- Checked HTTP security headers, redirects, TLS protocols, ciphers and certificates on every host found
- Identified visible CMS, plugin and server versions and compared them with public vulnerability advisories
- Reviewed public forms, upload fields and login pages, and checked common locations of exposed files and panels
- Searched certificate transparency logs and search engines for subdomains and indexed files
- Read SPF, DKIM and DMARC, looked up the checkout email in Have I Been Pwned, and listed third-party scripts and cookies

What we did not do

- No login attempts and no password guessing
- No exploitation of any vulnerability
- No opening or downloading of client files we found
- No form submissions and no file uploads
- No testing of internal networks, workstations or servers
- No testing of the portal vendor's application

How we rate severity

SEVERITY	MEANING	SUGGESTED TIMING
CRITICAL	Directly exposes sensitive data or gives an attacker an easy way in.	Same day
HIGH	A known, realistic path to compromise or fraud that needs little skill to use.	Within 7 days
MEDIUM	Weakens defenses or makes other attacks easier.	Within 30 days
LOW	Good-practice improvements that reduce what attackers can learn.	Before the next assessment

What we found online

ADDRESS	WHAT IT IS	FOUND VIA	STATUS
www / apex	WordPress website on shared hosting, intake and contact forms	DNS	F-01, F-03 – F-05
portal.	Client document portal (third-party vendor)	DNS (CNAME)	OK
webmail.	Hosting provider's webmail login page	Certificate logs	Login page only
MX	Email hosted with Google Workspace	DNS	F-02

04 – TECHNICAL FINDINGS

Detailed findings

Each finding explains what we saw, why it matters for the firm, and what the person who manages the website should do.

F-01 Client spreadsheet in a public folder, indexed by Google

CRITICAL

Location: `/wp-content/uploads/2025/01/` Category: Data exposure

WHAT WE SAW

A Google search for files on the firm's domain returns a spreadsheet uploaded in January 2025. Its title and the preview text in the search result show client names and engagement types. The folder it sits in lists its contents to anyone.

```
search: site:loneoaktax.example filetype:xlsx
→ "engagement-letters-2025.xlsx" /wp-content/uploads/2025/01/engagement-letters-2025.xlsx
  preview: "Client name · Return type · Fee · Signed ..."
```

we read only the search result; the file was not opened or downloaded

WHY IT MATTERS

The file contains customer information as defined in the Safeguards Rule, and it is public. Anyone can download it, and search engines have already copied its contents into their index.

HOW TO FIX

- Delete the file from the server today and add `Options -Indexes` to the main `.htaccess` file (see F-08).
- Request removal through Google's "Remove outdated content" tool once the file is gone.
- Check the server access logs (cPanel → "Raw Access") for downloads of the file. Your Qualified Individual should decide whether this is a notification event; under 314.4(j), events involving 500 or more consumers must be reported to the FTC within 30 days of discovery.
- Store working files in your document management system, not in the website's media library.

F-02 No DMARC record – email can be spoofed in the firm's name

HIGH

Domain: `loneoaktax.example` Category: Email security

WHAT WE SAW

<code>_dmarc.loneoaktax.example</code>	TXT	(no record)
<code>loneoaktax.example</code>	TXT	<code>"v=spf1 include:_spf.google.com ~all"</code>
<code>google._domainkey</code>	TXT	DKIM key present (2048-bit)

WHY IT MATTERS

SPF and DKIM are in place, but without DMARC receiving servers are not told to reject messages that fail them. During tax season, criminals send emails that look like they come from a client's own preparer, asking for W-2s, bank details or payment.

HOW TO FIX

```
_dmarc    TXT    "v=DMARC1; p=none; rua=mailto:dmarc@loneoaktax.example"
```

- Create the `dmarc@` mailbox first, or point the address to a free DMARC report service.
- After 2–4 weeks with all legitimate senders passing, move to `p=quarantine` and then `p=reject`, ideally before January.

F-03 Intake form plugin with a published vulnerability**HIGH**Component: **QuickIntake Forms 2.1.3** Category: **Outdated software****WHAT WE SAW**

```
<script src="/wp-content/plugins/quickintake-forms/assets/form.js?ver=2.1.3">
GET /wp-content/plugins/quickintake-forms/readme.txt → Stable tag: 2.1.3
```

The vendor published a security advisory for versions below 2.2.0: under certain conditions, visitors who are not logged in can read stored form entries.

WHY IT MATTERS

The "New client intake" form collects names, phone numbers, email addresses and filing status. Attackers scan for sites still running vulnerable versions soon after an advisory is published.

HOW TO FIX

- Update the plugin today and turn on automatic updates for plugins.
- Set the plugin to delete stored entries after they are copied to your practice software, so the website does not keep a growing archive of client data.

We did not attempt to exploit this vulnerability. The rating is based on the version number and the vendor's advisory.

F-04 Key security headers missing on the main website**MEDIUM**Location: **all pages of www.** Category: **Browser protections**

HEADER	STATUS	WHAT IT PROTECTS AGAINST
Strict-Transport-Security	Missing	Downgrade to unencrypted HTTP on public Wi-Fi
Content-Security-Policy	Missing	Injected scripts that copy what clients type into forms
X-Frame-Options	Missing	Your pages being framed by a fake site
X-Content-Type-Options	Present	File-type confusion attacks

HOW TO FIX

```
Header always set Strict-Transport-Security "max-age=31536000"
Header always set X-Frame-Options "SAMEORIGIN"
Header always set Referrer-Policy "strict-origin-when-cross-origin"
```

- Add a Content-Security-Policy in report-only mode first, so it does not break the booking widget, then enforce it.

F-05 Usernames exposed and login page without two-factor**MEDIUM**Location: **/wp-json/wp/v2/users, /wp-login.php** Category: **Login entry points**

```
GET /wp-json/wp/v2/users → 200 OK slugs: "loneoak", "jwalker"
GET /wp-login.php → 200 OK (no CAPTCHA, no visible two-factor prompt)
```

The user slugs normally match the login names. The login page shows no sign of attempt limits or two-factor authentication. We did not attempt to log in.

WHY IT MATTERS

The website stores intake form entries (F-03), so it is an information system that holds customer information. The Safeguards Rule requires multi-factor authentication for anyone accessing such systems, unless your Qualified

Individual approves an equivalent control in writing (314.4(c)(5)).

HOW TO FIX

- Turn on two-factor authentication for both accounts and limit failed login attempts.
- Hide the user list in the REST API (available in most security plugins).

F-06 Checkout email in 2 breaches, one with passwords**MEDIUM**

Address: **admin@loneoaktax.example** Source: **Have I Been Pwned**

BREACH (ILLUSTRATIVE)	YEAR	DATA EXPOSED
Accounting software forum	2021	Email addresses, usernames, hashed passwords
Business directory	2024	Email addresses, business names, phone numbers

If the forum password was reused anywhere, including tax software, the portal or Google Workspace, that account is at risk.

HOW TO FIX

- Change any reused passwords, use a password manager, and make sure two-step verification is on for this mailbox.

Breach data provided by Have I Been Pwned (haveibeenpwned.com). Breach names in this sample are illustrative.

F-07 Outdated TLS 1.0 and 1.1 still accepted**MEDIUM**

Host: **www.loneoaktax.example:443** Category: **Encryption in transit**

```
TLS 1.3  accepted  ✓
TLS 1.2  accepted  ✓ (strong ciphers only)
TLS 1.1  accepted  ✗ deprecated (RFC 8996)
TLS 1.0  accepted  ✗ deprecated (RFC 8996)
```

The Rule requires customer information in transit over external networks to be encrypted (314.4(c)(3)). The site is encrypted, but it still accepts protocol versions that are deprecated. Modern browsers do not use them, so switching them off does not affect real visitors.

HOW TO FIX

- Set the minimum TLS version to 1.2 in the CDN dashboard, or ask the hosting provider if there is no CDN.

F-08 Directory listing enabled on the uploads folder**LOW**

Location: **/wp-content/uploads/** Category: **Server configuration**

Folders under `/wp-content/uploads/` show a full list of their files to anyone. This is how the file in F-01 became easy to find. Fix: add `Options -Indexes` to the main `.htaccess` file.

F-09 No security.txt file for reporting problems**LOW**

Location: **/.well-known/security.txt** Category: **Good practice**

Researchers who notice a problem like F-01 look for this file to know whom to tell. Two lines are enough: `Contact: mailto:security@loneoaktax.example` and an `Expires: date`.

05 — WHAT IS ALREADY IN GOOD SHAPE

Checks that passed

CHECK	RESULT	NOTES
HTTPS enforced	Pass	All HTTP requests redirect to HTTPS (301)
TLS certificates	Pass	Valid and auto-renewing on all hosts
Client portal	Pass	Vendor portal enforces HTTPS and HSTS and offers two-factor login
Document collection	Pass	The website sends clients to the portal for tax documents instead of collecting them by form
SPF and DKIM	Pass	Correct for Google Workspace, 2048-bit DKIM key
PHP and WordPress core	Pass	Supported PHP 8.3, current WordPress release
Exposed source code, backups or secrets	Pass	No .git, .env, backups or config copies found
Exposed hosting or database panels	Pass	No phpMyAdmin or similar panels reachable
Contact form spam protection	Pass	CAPTCHA on the contact form

06 — INVENTORY

Third-party scripts and cookies

Outside services that can run code on the firm's pages, relevant to service provider oversight (314.4(f)).

SERVICE	PURPOSE	LOADED ON	NOTE
Google Analytics 4	Visitor statistics	All pages	OK
Online booking widget	Appointment scheduling	/book/	OK
Google reCAPTCHA	Spam protection	/contact/	Add to intake form
Google Fonts	Web fonts	All pages	OK

COOKIE	SET BY	SECURE	HTTPONLY	SAMESITE	ASSESSMENT
wordpress_test_cookie	WordPress login page	Yes	No	Not set	Harmless
_ga, _ga_*	Google Analytics (script)	Yes	n/a	Lax	Expected

APPENDIX A — SAFEGUARDS RULE MAPPING

How this assessment relates to 16 CFR 314.4

An overview for the Qualified Individual. It shows where this assessment provides evidence and where the firm needs other measures. It is not a compliance opinion.

SECTION	REQUIREMENT (SUMMARY)	COVERAGE	WHAT THIS ASSESSMENT PROVIDES
(a)	Designate a Qualified Individual	Not covered	—
(b)	Written risk assessment of internal and external risks	Partly	Findings and severity ratings for external risks, as input
(c) (1)	Access controls	Partly	Exposed login pages and user lists (F-05)
(c) (2)	Inventory of data, devices and systems	Partly	List of internet-facing hosts and outside services (sections 03, 06)
(c) (3)	Encryption in transit over external networks and at rest	Partly	TLS on public systems (F-07); at-rest encryption not visible from outside
(c) (4)	Secure development; testing of external applications	Partly	Outdated components in the website (F-03)
(c) (5)	Multi-factor authentication	Partly	Whether public login pages offer two-factor (F-05, portal)
(c) (6)	Secure disposal and data retention	Partly	Old customer files still reachable online (F-01)
(c) (7)	Change management	Not covered	—
(c) (8)	Monitoring and logging of user activity	Not covered	—
(d) (1)	Regular testing or monitoring of safeguards	Partly	Independent external testing twice a year
(d) (2)	Vulnerability assessments at least every six months	Covered (external)	This assessment, for internet-facing systems. Internal systems need separate assessment.
(d) (2)	Annual penetration testing	Not covered	Not a penetration test; arrange separately
(e)	Security awareness training and qualified staff	Not covered	F-02 and F-06 are useful training examples
(f)	Oversight of service providers	Partly	Public settings of the portal and third-party scripts (section 06)
(g)	Evaluate and adjust the program	Partly	Testing results as input; fix verification in assessment 2
(h)	Written incident response plan	Not covered	—
(i)	Annual written report to the board or a senior officer	Not covered	This report can be attached as testing results
(j)	Notify the FTC of events involving 500+ consumers within 30 days	Not covered	Relevant to the decision on F-01

Requirement summaries are paraphrased from 16 CFR 314.4 as published in the eCFR. Rely on the official text. Firms that maintain customer information on fewer than 5,000 consumers are exempt from 314.4(b)(1), (d)(2), (h) and (i) under 314.6.

APPENDIX B — ASSESSMENT LETTER

External Vulnerability Assessment Letter

For the firm's security records. A signed copy is sent as a separate PDF.

Date: October 12, 2026

To: Lone Oak Tax & Bookkeeping, Round Rock, Texas — attention of the Qualified Individual

Reference: NYX-SAMPLE-SG-001 · Assessment 1 of 2, plan year October 2026 – October 2027

Nyorsoft s.r.o. carried out an external vulnerability assessment of the internet-facing systems of Lone Oak Tax & Bookkeeping between **October 5 and October 9, 2026**.

Scope. The domain loneoaktax.example and its subdomains identified through DNS and public certificate transparency logs, the public settings of the third-party client portal, and the domain's email authentication records.

Methods. Non-intrusive review from the public internet: checks of TLS, HTTP security headers and certificates; identification of visible software versions and comparison with public vulnerability advisories; review of public forms and login pages; search for exposed files and panels; review of search engine results; and a breach lookup of one email address through Have I Been Pwned.

Results. 9 findings: 1 Critical, 2 High, 4 Medium and 2 Low, described in report NYX-SAMPLE-SG-001 of October 12, 2026.

Limitations. The assessment did not include internal networks, workstations or servers, authenticated testing, or penetration testing, and no vulnerabilities were exploited. It reflects conditions observed during the dates above. This letter confirms that the assessment described here was performed; it is not a certification of compliance with 16 CFR Part 314 or any other law.

Next assessment. Scheduled for April 2027, including verification of the findings listed above.

Nyorsoft s.r.o.
Bratislava, Slovakia · info@nyorsoft.com
[signature]

NEXT STEPS

1. Fix this week's items

Forward section 02 to whoever manages the website and email.

2. File this report

Keep the report, Appendix A and the signed letter with your written information security program.

3. Ask us anything by email

Write to info@nyorsoft.com and quote the finding ID. We reply in writing.

4. Assessment 2 in April 2027

We will remind you 30 days ahead and verify which findings were fixed.

This is a sample report. Lone Oak Tax & Bookkeeping, the domain loneoaktax.example, QuickIntake Forms and all findings are fictional and were created to show the format of a Nyorsoft External Vulnerability Assessment for FTC Safeguards Rule Programs. Any resemblance to a real business is unintended.