P-BON CONSULTING SERVICES, INC.

Technology. Strategy. Results.

Express Vulnerability & AI Risk Assessment

A Combined External Exposure and AI/Third-Party Tool Risk Review

COMPLIANCE TOOLKITS & MICRO-AUDITS — PAID ASSESSMENT

SERVICE PROPOSAL — $499 FLAT

Prepared by

Wlad Pierre-François, Ph.D.

Founder & President, P-Bon Consulting Services, Inc.

info@pbonconsulting.com · (516) 734-1515 · pbonconsulting.com

August 2026

Table of Contents

1. Executive Summary

P-Bon Consulting Services, Inc. proposes the Express Vulnerability & AI Risk Assessment, a fixed-price ($499) assessment combining an external vulnerability scan of the client's internet-facing footprint with a review of the third-party and AI tools in active use — including the shadow-IT tools nobody formally approved.

Two risk categories have converged for small and mid-size regulated businesses: what's exposed to the internet, and what unapproved AI/SaaS tools staff have quietly adopted. Both are delivered as one written findings report with prioritized remediation.

2. About P-Bon Consulting Services, Inc.

P-Bon Consulting Services, Inc. is an IT managed services and cybersecurity advisory firm founded and led by Wlad Pierre-François, Ph.D., serving law firms, medical practices, financial services companies, and small-to-midsize businesses across the NY Metro area. The firm's approach is compliance-native: every engagement — from a single toolkit to an ongoing managed IT program — is built with the regulatory realities of HIPAA, the NY SHIELD Act, NY DFS Part 500, SEC Reg S-P, and FINRA Rule 4511 already accounted for, not bolted on afterward.

Relevant qualifications for this offering:

- The firm's compliance-native approach to regulated clients extends to AI governance work with medical and financial clients — see the firm's Medical AI Vault offering for the deeper version of this work in healthcare settings.
- Direct experience running external attack-surface reviews and OAuth/connected-app discovery for M365 and Google Workspace tenants.
- Founder-led delivery, so findings are interpreted by the same person who understands the client's broader regulatory context, not a generic scan output.

3. Statement of Need

External attack-surface scanning remains a baseline security control that regulators and cyber-insurers increasingly expect evidence of. At the same time, generative AI tool adoption inside firms has outpaced any policy governing it — staff pasting client data into consumer ChatGPT accounts, using unapproved AI note-takers on client calls, or connecting AI browser extensions with broad data access are now common findings, not edge cases.

This represents a compliance exposure most firms haven't inventoried, let alone assessed. Cyber-insurance applications increasingly ask about both attack surface and AI tool governance; a firm that can't answer either question is exposed at renewal, not just to attackers.

4. Scope of Work & Deliverables

The Assessment is deliberately scoped to two risk categories reviewed together, since they are increasingly evaluated together by insurers and regulators:

- External vulnerability scan — public-facing IP ranges, domains, and exposed services.
- Identification of unpatched or outdated software, exposed ports, and misconfigured public services.
- Inventory and risk review of third-party SaaS and AI tools in active use across the organization — survey-based intake plus technical discovery where feasible.
- Written findings report — separating "external attack surface" and "AI/third-party tool" risk, each item risk-ranked with a specific remediation recommendation.

5. Methodology — How This Is Delivered

1. Scoping call — confirm domains/IP ranges in scope and distribute a short AI/tool-usage intake to relevant staff or department leads.
2. External scan — run against confirmed scope.
3. Tool/AI inventory — compiled from intake plus, where accessible, technical discovery (e.g., OAuth connected-app review in M365/Google Workspace).
4. Findings consolidated, risk-ranked, and written up.
5. Report delivered with prioritized remediation; optional follow-up call to walk through findings.

6. Objectives & Success Metrics

Objective	Success Metric
Establish a current external attack-surface baseline	All confirmed domains/IP ranges scanned; findings documented even if zero critical issues found
Inventory AI/third-party tool usage	At least one round of intake completed across key departments; connected OAuth apps reviewed where technically accessible
Prioritize remediation realistically	Every finding tagged Critical/High/Medium/Low with a specific next step, not a raw scan dump
Create a reusable governance starting point	Client leaves with a documented AI/tool inventory to build a formal approval policy on top of

7. Who This Is For

Regulated small and mid-size businesses (law, medical, financial services) and general small businesses that want an independent, point-in-time read on external exposure and AI/tool sprawl.

Particularly useful ahead of a cyber-insurance renewal, before drafting an AI usage policy, or as a periodic check outside an ongoing managed-IT contract.

8. Timeline

Stage	What Happens
Day 0–1	Scoping call; AI/tool-usage intake distributed
Day 2–3	External scan conducted
Day 3–5	Intake responses and OAuth/app discovery reviewed
Day 6–8	Findings compiled and risk-ranked
Day 8–10	Report delivered; optional walkthrough call

9. Team

Led by Wlad Pierre-François, Ph.D., drawing on the firm's compliance-native approach to regulated clients and its own AI-governance work with medical and financial clients.

10. What You Need to Provide

- Confirmed list of public domains/IP ranges in scope
- A named contact to distribute the AI/tool-usage intake internally
- Optional but recommended: temporary read access to the M365/Google Workspace admin console for OAuth app discovery

11. Investment

Line Item	Basis / What's Included	Cost
Express Vulnerability & AI Risk Assessment	External scan + AI/tool inventory + written report	$499 flat
Follow-up remediation engagement	Scoped separately based on findings	Quoted after report delivery

Standalone external vulnerability scans alone commonly run $500–$1,500 from security vendors, before any AI/tool governance review is added. Bundling both into one flat-price assessment is intentional — the two risks are increasingly reviewed together by insurers and regulators.

12. Compliance & Regulatory Alignment

Supports NY DFS Part 500 risk assessment requirements and cyber-insurance application/renewal documentation needs, and gives firms a documented starting point for an AI usage policy ahead of emerging state AI-transparency guidance and client/vendor due-diligence questionnaires.

13. Why P-Bon Consulting

- One of the few assessments in this price range that treats AI tool sprawl as a first-class risk category rather than an afterthought.
- Flat price regardless of findings volume.
- Delivered by the same person who will, if engaged further, help fix what's found.

14. Next Steps

Request the assessment through the solutions page or contact page. An invoice follows immediately at the listed price; the assessment is scheduled once payment clears.

Not sure this is the right fit? A short conversation is cheaper than the wrong toolkit — reach out at info@pbonconsulting.com or (516) 734-1515 before requesting this item.