P-BON CONSULTING SERVICES, INC.

Technology. Strategy. Results.

M365 Security & Email Hardening Audit

A Fixed-Scope Tenant Security Review for NY Metro Firms

COMPLIANCE TOOLKITS & MICRO-AUDITS — PRODUCTIZED SERVICE

SERVICE PROPOSAL — $350 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 M365 Security & Email Hardening Audit, a fixed-price ($350), structured review of a client's Microsoft 365 tenant configuration, focused specifically on the handful of settings that precede the overwhelming majority of business email compromise (BEC) and account-takeover incidents.

Most BEC incidents don't start with a novel exploit — they start with a tenant missing MFA enforcement on one account, an old forwarding rule nobody remembers creating, or Conditional Access policies that were configured but never actually turned on. The Audit is delivered as a written, prioritized remediation report within one week, using the same hardening checklist P-Bon applies to its own managed-IT clients.

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 Foundation and Shield™ managed-IT programs already build M365 hardening into every regulated client's baseline — this audit uses that same internal checklist, not a generic third-party template.
- Direct experience administering M365 tenants for law firms, medical practices, and financial services clients operating under NY DFS Part 500, FINRA 4511, and HIPAA.
- Founder-led delivery: the person reviewing the tenant is the same person who configures tenants for the firm's ongoing clients.

3. Statement of Need

The FBI's Internet Crime Complaint Center (IC3) consistently ranks business email compromise among the costliest categories of reported cybercrime, with reported losses in the billions of dollars annually. The entry point is overwhelmingly credential compromise on tenants without enforced MFA or with legacy authentication still enabled — not a novel technical exploit.

Firms outside a managed-IT contract, including many law firms, medical practices, and financial companies handling M365 configuration internally or via a part-time IT contractor, often have no record of when MFA, Conditional Access, or mail-flow rules were last reviewed. Regulatory frameworks that apply to this client

base — NY DFS Part 500, FINRA Rule 4511, HIPAA — increasingly expect documented, periodic security review of core systems; a tenant audit report is direct evidence of that review.

4. Scope of Work & Deliverables

The Audit is scoped to the configuration areas with the highest yield against real-world BEC and account-takeover incidents, not a generic security scorecard:

- Tenant-wide security configuration review — Conditional Access policies, legacy authentication status, guest access settings.
- Multi-factor authentication audit — per-user and per-admin MFA status across the tenant.
- Mail-flow and forwarding-rule review — catching the auto-forward rules attackers commonly use to exfiltrate mail undetected.
- Admin role and privileged-account review — who holds Global Admin, and whether that access is still needed.
- Written remediation report — findings ranked by risk with specific, actionable fix steps, not just flagged issues.

5. Methodology — How This Is Delivered

1. Kickoff & access — client grants scoped, time-boxed admin review access (Security Reader role is generally sufficient; never a permanent standing credential).
2. Automated + manual review — configuration is pulled and manually reviewed against P-Bon's internal hardening checklist.
3. Findings compiled and risk-ranked.
4. Remediation report delivered, with an optional 30-minute walkthrough call to review findings.
5. Access revoked at project close.

6. Objectives & Success Metrics

Objective	Success Metric
Identify MFA/authentication gaps	100% of user and admin accounts checked, gaps listed by account
Surface hidden mail-flow risk	Every active forwarding/mail-flow rule reviewed and flagged if suspicious or unnecessary
Right-size admin privilege	Global/privileged admin role holders identified and flagged if unnecessary

Objective	Success Metric
Deliver an actionable, not just descriptive, report	Every finding paired with a specific remediation step, not a generic recommendation

7. Who This Is For

Law firms, medical practices, financial companies, and small businesses with an existing M365 tenant who want an independent second look at their security configuration — whether they manage M365 internally, use a different IT provider, or simply haven't had it reviewed since setup.

No minimum tenant size; the audit is typically most useful for organizations in the 5–75 user range.

8. Timeline

Stage	What Happens
Day 0–1	Order confirmed, scoped access requested
Day 2–4	Configuration review conducted
Day 5–6	Findings compiled, report drafted
Day 7	Remediation report delivered; optional walkthrough call scheduled

9. Team

Conducted directly by Wlad Pierre-François, Ph.D., using the same hardening checklist applied to P-Bon's own managed-IT clients under the Foundation and Shield™ programs.

10. What You Need to Provide

- Time-boxed or scoped admin access to the M365 tenant (Security Reader role is generally sufficient)
- A named point of contact to receive and act on the report

11. Investment

Line Item	Basis / What's Included	Cost
M365 Security & Email Hardening Audit	Full tenant review + written remediation report	$350 flat
Optional remediation implementation	Fixing flagged issues, scoped separately	Quoted after report delivery

Independent M365 security assessments from larger MSPs and consultancies commonly start at $1,500–$3,000 or more. This audit is scoped tightly to the highest-yield configuration areas to remain accessible as a standalone check rather than a full security program.

12. Compliance & Regulatory Alignment

Directly supports NY DFS Part 500's risk assessment and access-control provisions, FINRA Rule 4511 recordkeeping expectations around system security review, and HIPAA's required periodic technical evaluation under 45 CFR 164.308(a)(8).

13. Why P-Bon Consulting

- Same checklist used on P-Bon's own managed clients — not a generic scan-and-report product.
- Flat price, no upsell pressure: findings are reported honestly even when they point to needing more work.
- Delivered by the firm's founder, not handed off to a junior analyst.

14. Next Steps

Request the audit through the solutions page or contact page. An invoice follows immediately at the listed price; the audit 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.