TorchLight 3-Layer Security Readiness Assessment

A practical framework for modern businesses

Introduction

Managing cybersecurity risk while maintaining operational efficiency is a challenge every business faces in today's threat landscape. Recent breaches at major organizations like Workday and federal systems highlight how traditional security approaches miss critical vulnerabilities, particularly around vendor integrations and system interconnections.

This assessment uses a 3-layer framework designed to help you identify gaps before they become costly security incidents or operational problems. Each section focuses on practical security measures that directly impact your ability to maintain customer trust, protect business continuity, and safeguard your competitive advantage.

Whether you're in professional services, manufacturing, healthcare, finance, or any industry where data protection and operational reliability are critical to success, this framework provides actionable insights to strengthen your security posture and reduce business risk.

Self-Assessment

Layer 1: Prevention Controls

Stopping threats before they reach your systems

□ **Yes** □ **No** | Do you enforce multi-factor authentication on all systems containing sensitive business or client data?

□ **Yes** □ **No** | Are you protected from criminals sending fake emails to your clients using your company name and email domain?

□ **Yes** □ **No** | Can all staff securely access business systems remotely without creating compliance gaps or productivity losses?

□ **Yes** □ **No** | Are integrations between your business systems (practice management, accounting, document storage) secured against third-party breaches?

□ **Yes** □ **No** | Are administrative privileges restricted to specific personnel and regularly audited to prevent unauthorized access to sensitive data?

□ **Yes** □ **No** | Do you enforce strong, unique passwords across all business systems to prevent easy entry points for competitors or bad actors?

□ **Yes** □ **No** | Is your network properly segmented to contain threats and protect sensitive data when unauthorized access occurs? For example, are executive systems isolated from general staff computers to prevent unauthorized access to high-privilege accounts and sensitive information?

□ **Yes** □ **No** | Does your team receive regular, up-to-date security training on threats specifically targeting your industry?

□ **Yes** □ **No** | Do you know you meet all the requirements of your cyber insurance and that you would be covered in an event?

□ **Yes** □ **No** | Do you have protection that stops sophisticated threats traditional antivirus software misses?

□ **Yes** □ **No** | Do you have visibility and control over staff using unauthorized cloud services or software that could expose client data?

□ **Yes** □ **No** | Is your Microsoft 365 configured beyond default settings to prevent common business email attacks and maximize your software investment?

Layer 2: Threat Detection

Identifying problems before they disrupt client service

□ **Yes** □ **No** | Would you be immediately alerted if someone accessed client data outside normal business hours or from unusual locations?

□ **Yes** □ **No** | Are you alerted of unusual staff behavior that could indicate compromised accounts accessing confidential information?

□ **Yes** □ **No** | Would you detect if threats were targeting your backup systems before losing the ability to serve clients?

□ **Yes** □ **No** | Can you quickly identify when staff accounts have been taken over by unauthorized users?

□ **Yes** □ **No** | Are sophisticated attacks targeting your firm detected before they reach staff and potentially compromise client relationships?

□ **Yes** □ **No** | Do you automatically block access attempts from suspicious locations that could indicate international cybercriminal activity?

□ **Yes** □ **No** | Would you be notified if sensitive data was being copied or shared in ways that could violate confidentiality requirements?

□ **Yes** □ **No** | Do you monitor for staff installing risky applications that could create pathways for data breaches?

Layer 3: Incident Response

Protecting business continuity and client relationships when problems occur

□ **Yes** □ **No** | Do you have written procedures for handling security incidents that meet your industry's regulatory notification requirements?

□ **Yes** □ **No** | Have you practiced your incident response to ensure staff can maintain client service during a security crisis?

□ **Yes** □ **No** | Can you continue serving clients if your primary systems are compromised, avoiding revenue loss and client defection?

□ **Yes** □ **No** | Can you restore client access and resume billable work within 24 hours of a system failure?

□ **Yes** □ **No** | Do you conduct independent security testing that satisfies auditors and demonstrates due diligence to clients?

□ **Yes** □ **No** | Does your cyber insurance actually cover the business risks you face, not just generic IT problems?

□ **Yes** □ **No** | Is there clear accountability for security response so client communication isn't delayed during a crisis?

□ **Yes** □ **No** | Do you regularly test that backups actually work, ensuring you won't discover failures when clients need immediate service restoration?

□ **Yes** □ **No** | Do you have pre-written communication plans for notifying clients, partners, and regulators to minimize relationship damage during incidents?

□ **Yes** □ **No** | Can you document security incidents properly to avoid cyber insurance claim denials when you need coverage most?

Your Business Risk Profile

Count your "Yes" responses:

24-27 "Yes" Answers: Strong operational security that supports business growth and client confidence.

18-23 "Yes" Answers: Moderate risk with gaps that could disrupt client service, trigger audit findings, or complicate insurance renewals.

0-17 "Yes" Answers: Significant operational vulnerabilities that could impact client relationships, regulatory standing, and competitive position.

Next Steps

This assessment provides a high-level view of your operational security posture. If you answered "No" to multiple items or want a detailed analysis of your specific business risks, our comprehensive 3-Layer Security Assessment provides:

- Quantified risk scoring that satisfies auditors and insurance carriers
- Industry-specific compliance gap analysis with remediation costs
- Prioritized improvement recommendations focused on protecting client relationships and operational continuity
- Implementation roadmap designed to enhance rather than disrupt daily operations

The comprehensive assessment is designed for organizations that want to turn security into a competitive advantage rather than just meet minimum requirements.

To discuss how your results impact your operations and client relationships, contact us at info@torchlight.io or 833-761-0695.

About Our Approach

TorchLight helps businesses turn cybersecurity challenges into competitive advantages through comprehensive managed IT and security services. Our security-first methodology strengthens client relationships, accelerates business growth, and ensures operational resilience without disrupting productive work.

We design solutions that enhance your business operations while prioritizing protection. Our services recognize that effective cybersecurity should enable growth, not hinder it.

Our services address three critical areas:

- **Trust Protection** - Safeguarding client relationships and reputation that drive revenue
- **Operational Excellence** - Ensuring technology enhances business performance
- **Strategic Growth** - Building security infrastructure that scales with your business

We work with organizations across industries including financial services, healthcare, legal, manufacturing, professional services, and technology companies where data protection, client trust, and operational continuity are essential to success.

What sets us apart:

- **Security-First Design** - Every solution prioritizes protection while supporting business objectives
- **Comprehensive Services** - From assessments to 24/7 managed security operations
- **Scalable Solutions** - Technology that grows with your business

- **Measurable Impact -** Clear metrics showing technology's business value

Whether you need security assessments, managed IT services, or enhanced cybersecurity capabilities, we transform technology from a cost center into a business advantage.