Compliance Gap Assessment

Evaluate vulnerabilities, reduce risks, and strengthen your business' defenses

What Is It and Why Do You Need It?

The Compliance Gap Assessment provides a point-in-time evaluation of your security maturity against selected industry standards. This assessment gives you actionable insights and a prioritized action plan to safeguard your organization while optimizing your security investments and achieving compliance.

Benefits

- **Understand Strengths and Weaknesses:** Clearly identify security gaps and vulnerabilities
- **Focus on What Matters:** Address high-risk vulnerabilities first for maximum impact
- **Remain Compliant:** Align with industry standards, including FTC Safeguards, NIST 800-171, HIPAA, PCI-DSS, or GDPR
- **Leverage Expert Guidance:** Get actionable, tailored recommendations from TPx security experts
- **Custom Fit:** Receive solutions tailored to your organization's unique needs

How It Works

The Gap Assessment consists of two key components:

Security Strategy

- Evaluation of security policies, standards, and procedures.
- Assessment of roles, responsibilities, and security management processes.

Operational Security

- Technical evaluation of security measures implemented in your environment.
- Categorization of cybersecurity risks, including:
  – Access controls and identity management
  – Network segmentation and protection
  – Email and endpoint security

This approach provides a thorough understanding of your organization's vulnerabilities and a clear roadmap to improve compliance and security.

Why TPx?

As a trusted leader in cybersecurity for SMBs and public-sector organizations, TPx combines industry expertise with tailored solutions to strengthen your security posture. TPx consultants leverage proven standards to deliver actionable insights and measurable improvements.

61% of SMBs are targeted by cyberattacks, but only 14% are prepared. Is your business ready?

What To Expect

TPx consultants assess your organization's security maturity through interviews, data collection, and technical reviews. Your information security posture is assessed based on a set of categorizations (e.g. access controls and network protections). The categorizations covered during the gap assessment focus on areas of cybersecurity that have the highest likelihood of incidents and breaches for your organization.

Gap Assessment Activities

The areas of focus can range from information security governance to cybersecurity infrastructure and capabilities.

Information Security Organization Accountability Information security accountability and compliance, including strategic roles and responsibilities and information security policy

Human Resource Security Management Human resource security management, including information security in hiring, awareness, education and training, and change and termination

Identity and Access Management User access management and password policies

Information Security Incident Management Information security incident management preparation, identification and assessment, response and continuity, and testing

Change Management Change management, including planning, building, testing, and implementation

Network Segmentation, Isolation and Protection Network security architecture, including segmentation, isolation, firewalls, and threat management

Security Services Core security services, including onboarding/offboarding, account and access management, and backup services

Server and Workstation Security Endpoint security, including access controls, technical vulnerability management and protections

Email Service Security Email security, including architecture, access controls, technical vulnerability management and protections

Reporting

You'll receive three actionable reports tailored to leadership and practitioners:

- **Heatmap Report:** Visual overview of security maturity
- **Executive Summary:** Strategic insights for decision-makers
- **Comprehensive Gap Assessment Report:** Detailed findings with prioritized recommendations

These reports provide actionable steps based on your organization's specific vulnerabilities and exposure landscape.