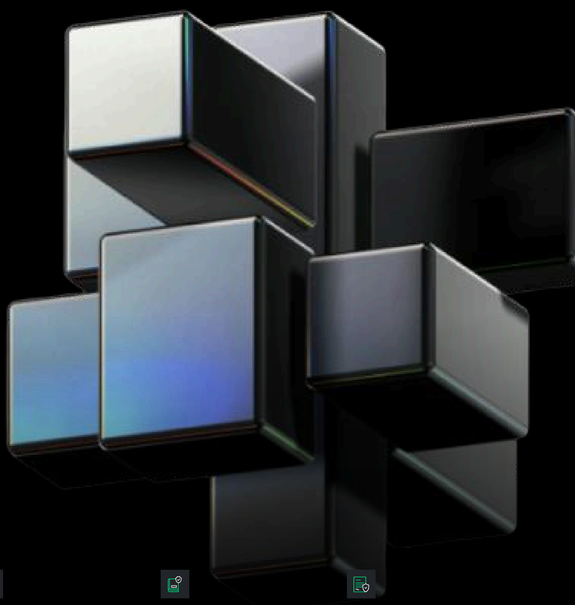
FYNCH CONSULTING

Cybersecurity audit

$4.45 million was the average cost of data breach with 83% of companies experiencing more than one breach - Ponemon Institute



In cybersecurity, you're either proactive or reactive—ideally, you're both

Without a cybersecurity audit, unseen vulnerabilities can go unchecked, exposing your business to data breaches, financial loss, and reputational damage. Failing to assess risks regularly leaves critical assets unprotected, jeopardizing business continuity and customer trust. At Fynch we believe that a business that doesn't invest in cybersecurity is a business planning to fail.

- **Threat & vulnerability assessment**
- **Security policy review & development**
- **Compliance assessment**
- **Penetration testing**
- **Incident response planning & testing**
- **Security awareness training**

Key activities

1 Risk identification and assessment

Identify threats and vulnerabilities: We conduct thorough assessments to identify potential threats and vulnerabilities in the organization's cybersecurity infrastructure.

Evaluate security controls: The effectiveness of existing security controls is analyzed and areas for improvement are identified.

Risk analysis: We assess the potential impact and likelihood of identified risks to prioritize mitigation efforts.

High level outcomes

- Detailed threat landscape
- Improved security posture
- Effective risk prioritization

2 Policy and compliance review

Based on the needs assessment, we develop a strategic plan for your enterprise architecture. This plan outlines the structure and components of the architecture, ensuring alignment with business goals.

Review security policies: We evaluate the organization's cybersecurity policies for comprehensiveness and relevance.

Compliance assessment: Compliance with industry standards and regulatory requirements is ensured.

Recommendations for policy enhancements: We provide guidance on updating and improving security policies.

- Enterprise architecture blueprint
- Defined technology stack
- Integration map
- High-level implementation roadmap

3 Technical security testing

Penetration Testing: We simulate cyberattacks to test the resilience of the organization's systems.

Vulnerability Scanning: Automated scans to identify security weaknesses are conducted.

Incident Response Testing: We assess the effectiveness of the organization's incident response plan.

- Resilience testing insights
- Thorough vulnerability detection
- Enhanced incident response

Ready to move forward with clarity?

Whether you need strategic direction, actionable insights, or market execution, our team is here to support your journey from vision to measurable result.

Book a consultation

Connect with us on

How else can we help?

start@fynchconsulting.com