

CLIENT CASE STUDY

Turning Fragmented Controls into a Practical Cybersecurity Roadmap

Cybersecurity risk assessment for a growing professional services firm

INDUSTRY	ORGANIZATION	WORKING MODEL	ENGAGEMENT
Professional services	50-100 employees	Hybrid workforce	Cybersecurity risk assessment

Client Context

A growing professional services firm had introduced security measures over time, but they had not developed into a coordinated cybersecurity program. Greater reliance on cloud services, remote work and sensitive client information led leadership to seek a clearer view of risk and a practical basis for deciding what to address first.

The Challenge

The challenge was not a complete absence of security; it was inconsistency. Policies and procedures had evolved unevenly, responsibilities were not always clear, and management had limited visibility across business operations and technology assets. There was also no documented plan connecting immediate control gaps with longer-term governance priorities.

Assessment coverage: governance and risk management | policies and procedures | access and endpoints | backups and recovery | cloud services | assets | awareness | incident preparedness

How Amnix Approached the Assessment

STAGE	FOCUS	WHAT AMNIX DID
01	Understand the business	Interviewed stakeholders and identified critical processes, information and supporting technology.
02	Review governance	Examined policies, oversight, accountability and the assignment of cybersecurity responsibilities.
03	Assess controls	Reviewed access, endpoints, backups, awareness, cloud services, asset management and incident preparedness.
04	Prioritize action	Evaluated risks in business terms and organized recommendations into a practical, phased roadmap.

WHAT THE ASSESSMENT REVEALED

The most significant issue was not one isolated vulnerability, but the absence of a consistent management structure around cybersecurity.

Priority Themes

Governance and accountability. Formal oversight was limited, and responsibility for monitoring or treating risk was not always clearly assigned.

Access and visibility. Access practices were inconsistent, while asset inventory and risk ownership needed greater definition.

Preparedness and resilience. Incident response, backup validation and recovery testing required a more structured, repeatable approach.

People and policy. Documentation and awareness practices needed strengthening so expectations could be applied consistently.

From Assessment to Action

BEFORE THE ASSESSMENT	AFTER THE ASSESSMENT
Security activities were fragmented, risk visibility was limited and priorities were not connected through a common improvement plan.	Leadership had a shared, prioritized view of risk, clearer accountability recommendations and a phased basis for investment decisions.

What Amnix Delivered

- A risk decision package combining a prioritized cybersecurity risk register with an executive-level summary of the most significant findings.
- A practical roadmap separating immediate priorities from medium- and longer-term initiatives.
- Governance, ownership and policy recommendations to support sustained cybersecurity management.

Business Impact

Leadership gained a shared view of cybersecurity risk and a clearer basis for investment decisions. The organization could now sequence improvements according to business impact, risk exposure and operational readiness, while building stronger ownership, oversight and resilience.

Need a clearer view of your cybersecurity risk?

Amnix Advisory helps organizations identify gaps, strengthen governance and build practical cybersecurity programs that support business objectives.

[Discuss a Cybersecurity Risk Assessment >](#)