

LIYATECH EXECUTIVE READINESS SERIES

FINANCIAL & PROFESSIONAL SERVICES CYBER READINESS CHECKLIST

Banking, Financial Services, Insurance, Legal, Accounting & Advisory Firms

"If sensitive client information was exposed today, would you know — and could you respond fast enough?"

Introduction

Financial and professional services organisations operate on one core principle: **trust**.

Clients expect that their financial data, legal matters, insurance records, and advisory information are always protected — without exception.

But modern business environments are increasingly digital, distributed, and interconnected.

This checklist is designed to help leadership teams assess whether their organisation is truly prepared for the risks that come with handling high-value, sensitive, and regulated information.

Tick what applies to your organisation.

1. Client Financial & Sensitive Data Protection

- ☐ We know exactly where all client financial and confidential data is stored across our systems.
 - ☐ Access to sensitive client information is restricted strictly based on role and responsibility.
 - ☐ We are confident that client data cannot be copied, downloaded, or shared without detection.
 - ☐ We regularly review who has access to financial, legal, or advisory information.
-

2. Email Fraud, Payment & Impersonation Risk

- ☐ We are confident staff can identify fraudulent payment requests, even when they appear to come from trusted clients or executives.
 - ☐ Controls exist to prevent email impersonation of partners, directors, or executives.
 - ☐ We have processes to verify high-value financial transactions before execution.
 - ☐ We are confident we could detect a business email compromise attempt before financial loss occurs.
-

3. Confidential Document Handling & Sharing

- ☐ Client documents are shared through secure systems rather than personal email or messaging apps.
 - ☐ We can track how sensitive documents are accessed and shared internally.
 - ☐ Confidential case files, contracts, or financial records are protected from unauthorised forwarding or copying.
 - ☐ External collaboration with clients is controlled through secure and approved platforms.
-

4. Regulatory Exposure & Accountability

- ☐ We can confidently demonstrate how client information is protected if requested by regulators or clients.
 - ☐ We understand where all regulated or sensitive data resides within the organisation.
 - ☐ Compliance requirements are actively reviewed and updated as regulations change.
 - ☐ Leadership is regularly informed of compliance and cybersecurity risks.
-

5. Identity, Access & Insider Risk

- ☐ Employees only have access to systems and data required for their role.

- ☐ Access is immediately removed or updated when staff change roles or leave the organisation.
 - ☐ Privileged accounts (administrators, finance, partners) have additional monitoring and protection.
 - ☐ We can quickly identify who accessed sensitive client data and when.
-

6. Business Continuity & Client Service Protection

- ☐ We are confident we could continue serving clients if core systems were disrupted.
 - ☐ Critical financial, legal, or operational data is backed up securely and can be restored quickly.
 - ☐ We have tested recovery procedures for system outages or cyber incidents.
 - ☐ We understand the financial and reputational impact of extended downtime.
-

Leadership Reflection

This checklist is designed to surface risk awareness — not to provide a score.

If several answers were **“No” or “Not Sure”**, it may indicate exposure in areas that could affect:

- Client trust and reputation
 - Regulatory compliance
 - Financial integrity
 - Operational continuity
 - Data confidentiality
 - Business resilience
-

Optional Executive Conversation

If this checklist highlighted areas that raised concern or uncertainty, it may be useful to have a structured conversation about your organisation's current cybersecurity and IT environment.

The goal is to provide clarity on where risk may exist and what practical steps can reduce it.

Contact

Nomfundo Makapela

 nomfundo.makapela@liyatech.co.za

 073 582 4195

Terence Moabi

 terence.moabi@liyatech.co.za

 078 710 4180

 www.liyatech.co.za