

PRIVATE EQUITY AND INVESTMENT

IT Controls for Investment Firms

Protect the deal team, the fund, and every company you acquire.

Investment firms are targeted for wire fraud, deal intelligence, and investor data. Each acquisition adds a new IT environment with its own risks. These controls protect the firm itself and give you a repeatable baseline for portfolio companies.

How to use it: tick what you have in place today. Anything left unticked is a conversation worth having.

01 Firm-level controls

- ☐ **Multi-factor authentication everywhere, with phishing-resistant methods for partners**
Deal teams are the top phishing target.
- ☐ **Wire and capital call instructions verified by phone at a known number**
Business email compromise is the costliest attack in finance.
- ☐ **Secure data room and file sharing with expiring, tracked links**
Know exactly who downloaded what.
- ☐ **Encrypted laptops and managed phones with remote wipe**
Deal materials travel.
- ☐ **24/7 monitored endpoint protection and email security**
Attacks land after hours and on weekends.

02 Portfolio due diligence

- ☐ **IT and security assessment before close**
Find the unsupported servers and missing backups before they become your problem.
- ☐ **Review of cyber insurance, prior incidents, and open vulnerabilities**
Ask for the last claim and the last pen test.
- ☐ **Inventory of critical systems, vendors, and contracts**
Know what you are buying.
- ☐ **Estimate of remediation cost and timeline**
Price IT risk into the deal.
- ☐ **Key-person risk check on IT knowledge**
One person holding every password is a finding.

03 Post-close standardization

- ☐ **Day-one access controls and admin account review**
Remove former owners and stale vendor access.
- ☐ **Common security baseline across all portfolio companies**
Same MFA, endpoint, backup, and email standards.
- ☐ **Consolidated reporting on security posture by company**
One view for the operating partner.
- ☐ **Backup and recovery tested at each company**
Recovery time is a value-protection metric.
- ☐ **Integration plan for email, identity, and licensing**
Save money by consolidating tools.

Red flags we see most

- Each portfolio company has a different IT vendor and no reporting.
- Capital call instructions arrive by unverified email.
- Due diligence skips IT entirely.
- Former owners still have admin access.

Where to start

Build an IT diligence checklist into every deal. A two-week assessment before close can change the price and saves months after it.

Want a second set of eyes?

Book a free 30-minute technical assessment. A senior engineer walks through this checklist with you and tells you what to fix first. No sales script, no obligation.

Book a technical assessment

(617) 322-5155

bostonmit.com/it-assessment