nexustek

PRIVATE EQUITY PORTFOLIO PROGRAM

THE PRIVATE EQUITY IT PLAYBOOK

Make IT Improve Value from Acquisition to Exit

Private equity firms and their portfolio companies can turn IT into business value across every stage of the investment lifecycle.

INTRODUCTION

Why IT Is a Private Equity Priority

According to the latest data, private equity (PE) portfolio companies are experiencing increased cyber incidents during their hold period that can cost millions of dollars in financial impact.[1]

$2.1M
average financial impact to PE deals due to cybersecurity risks[2]

68%
of PE firms report increasing cyber incidents during the hold period[3]

Only 15%
of portfolio companies claim "very mature" IT capabilities[4]

$40%
of PE investors experience valuation cuts when digital maturity lags[5]

48%
of PE firms report exit challenges fueled by the proliferation of IT tools[6]

PE firms need an easier way to expand their cyber defenses across their entire portfolio while reducing IT complexity for faster acquisition integrations and easier exit readiness. However, the challenge most PE firms face is that the IT across their portfolio companies is fragmented, undocumented, and largely invisible. Instead of helping generate more value across the three phases most PE investments go through, IT acts as a barrier.

THE THREE PHASES THAT DEFINE IT VALUE IN PRIVATE EQUITY

The three phases every PE investment during which business-aligned IT could reduce risks while generating additional value are acquisition and integration, the hold period, and exit.

Acquisition and Integration 01

This is often the highest risk moment because attackers frequently target companies during merger and acquisition transitions because many portfolio companies don't have a comprehensive IT or cybersecurity plan at close.

- Day 1 readiness and security baseline
- 90-day stabilization playbook
- Legacy MSP transition
- Documentation of inherited environment

Hold Period 02

During the hold period, IT should contribute to better EBITDA by reducing costs while providing cybersecurity protections to avoid incidents. This requires leadership to align IT investments and expenses to support business goals.

- **Managed IT + 24/7 cybersecurity**
- **vCIO + vCISO leadership**
- **Cloud cost optimization**
- **NexusOps portfolio visibility**

EXIT 03

IT due diligence is now standard in PE transactions with teams looking for documented security controls, incident response plans, clean cloud architectures, governance policies, and evidence of ongoing monitoring.

- IT Due Diligence Readiness Assessment
- Remediation roadmap
- Governance documentation

CHAPTER ONE

The Acquisition Phase

IT Integration Often Causes Delays and Risks

CHAPTER ONE

The Acquisition Phase

IT Integration Often Causes Delays and Risks

Challenges integrating IT across acquisitions often increase operational costs and cybersecurity risks while complicating compliance. It's a common problem across mergers and acquisitions that stems from the same root cause: there was no pre-defined IT integration plan at time of close. What typically happens is that the operating team was focused on the business and financials while IT was expected to sort itself out.

Unfortunately, attackers know that mid-market businesses acquired by PE firms have lean IT defenses, and that transitional chaos during a merger or acquisition creates exploitable opportunities.

What Good IT Integration Looks Like

01

PRE-CLOSE IT DUE DILIGENCE

Assess the inherited environment before the deal closes so there are no surprises on Day 1. Document infrastructure inventory, security posture, compliance obligations, and MSP relationships.

02

24/7 SECURITY MONITORING FROM DAY 1

There should be no gap period between your close and the start of active threat monitoring. Attackers that prey on mergers actively know your close date and will look to exploit any weaknesses as soon as transitions start to happen.

03

TRANSITION FROM SELLER IT ENVIRONMENTS ON A 90-DAY TIMELINE

Legacy MSP relationships, shared infrastructure with the seller, and inherited systems all create ongoing risk that should be reduced or eliminated as quickly as possible.

04

DOCUMENTATION OF THE INHERITED IT ENVIRONMENT

Detailed documentation can provide a baseline for the hold-period IT roadmap. Without documentation, portfolio companies often end up managing IT environments they don't fully understand because valuable knowledge was lost during transition.

05

ALIGNMENT TO A COMMON IT STANDARD

Each acquisition should include a standardized IT and security program shared across all portfolio companies and not remain on its own IT stack and MSP relationship.

When the portfolio company's IT environment is changing, time-sensitive and high-pressure integration windows are the hardest time to make **good IT decisions**. The private equity firms that handle acquisitions best have an IT integration playbook ready before the deal closes, instead of piecing them together afterward.

The 90-Day Integration Playbook

PHASE	TIMELINE	KEY DELIVERABLES
Pre-Close	Before close	IT due diligence assessed, integration playbook prepared, security baseline established, 24/7 monitoring contract ex-ecuted
Day 1	Close date	24/7 monitoring live, emergency contact protocol estab-lished, legacy MSP transition initiated, cybersecurity base-line deployed
Days 1–30	Month 1	Network stabilized, documentation underway, IT standards aligned to fund, critical vulnerabilities remediated
Days 30–90	Months 2–3	Full integration complete, NexusOps reporting active, hold-period IT roadmap delivered to CFO and operating partner

NEXUSTEK INTEGRATION CAPABILITY

NexusTek's IT Integration Playbook has been refined across hundreds of acquisitions. It's a standardized, proven process that puts portfolio companies in a stable, monitored, and documented state within 90 days of close, regardless of what was inherited from the prior owner. For roll-up strategies, the same playbook activates at each acquisition without having to build from scratch.

CHAPTER TWO

The Hold Period

From IT Cost Center to EBITDA Contributor

CHAPTER TWO

The Hold Period

From IT Cost Center to EBITDA Contributor

IT should improve the value of your portfolio, yet 40% of PE firms experience devaluation due to immature IT.[7] Advancing both IT and cybersecurity maturity needs to be driven by solid business and financial reasoning.

How is IT showing up in your EBITDA bridge right now: as a cost problem or a growth driver?

Most portfolio company CFOs and operating partners view IT as a necessary expense and something to minimize, not leverage. There is a better approach. EY identifies technology modernization, AI/analytics adoption, and operational efficiency as three of the top drivers of PE value creation. IT is the foundation that all three require.

The four IT investments with the clearest hold-period ROI are cybersecurity protection, cloud cost optimization, strategic IT leadership, and portfolio visibility. Together, they shift IT from a cost center to an EBITDA contributor.

$2.1M Avoidance

CYBERSECURITY

Protecting the Return

On average, PE firms lose $2.1M on deals due to increased cybersecurity risks, and nearly 70% of PE firms report increasing cyber incidents during their hold period.8 For a portfolio company at 15% EBITDA margins on $50M revenue, $2.1M is nearly a third of a year's earnings. 24/7 MDR and SOC coverage is the most defensible IT investment in the portfolio.

20–35% Savings

CLOUD COST OPTIMIZATION

Freeing EBITDA

Many portfolio companies migrate to cloud without a cost governance strategy, often resulting in overprovisioned environments and cloud spend that eats into EBITDA without any clear benefits. Cloud cost optimization typically returns 20–35% of cloud spend back to the business.

vCIO+ vCISO

Strategic IT Leadership Without Headcount

Most portfolio companies cannot justify a full-time CIO or CISO. The vCIO and vCISO model provides the strategic IT leadership needed at a fraction of the headcount cost while providing continuity that remains when the company is sold.

Real-time IT Health

NEXUSOPS

Portfolio Visibility That Scales

Operating partners cannot manage what they cannot see. NexusOps provides real-time IT health data on endpoint status, security posture, and incident activity across every portfolio company in a single dashboard so you can monitor your IT health just like you do for your financial KPIs.

HOLD-PERIOD IT INVESTMENT

The EBITDA Model

IT INVESTMENT	EBITDA IMPACT	NEXUSTEK CAPABILITY
24/7 MDR + SOC	Prevents $2.1 million average financial impact due to cybersecurity risks for direct EBITDA protection; reduces cyber insurance premiums	MDR + 24/7 SOC, EDR, AI Email Security
Cloud Cost Optimization	Returns 20–35% of cloud spend to reduce expenses	Cloud assessment, NexusTek Private Cloud, hybrid strategy, FinOps
vCIO + vCISO	Strategic leadership to align IT to business goals and timelines without headcount costs	vCIO + vCISO services delivered by former industry leaders
NexusOps Visibility	Portfolio IT health visible to GPs without requiring internal IT expertise to build or interpret	NexusOps platform delivers real-time IT health metrics across every portfolio company
Data + AI Platform	Portfolio benchmarking and AI-driven efficiency gains across operations	Data platforms, analytics, Liminal AI Manager
Managed IT	Replaces fragmented per-portfolio company MSP spend with portfolio-scale economics at or below the same cost	Complete Managed IT, Co-Managed IT, IT Operations

CHAPTER THREE

The Exit Moment

What Buy-Side IT Due Diligence Teams Are Looking For

CHAPTER THREE

The Exit Moment

What Buy-Side IT Due Diligence Teams Are Looking For

IT due diligence has become standard in PE exits. Today's buy-side due diligence teams have become more sophisticated and have significantly expanded what they look for when it comes to IT in the past five years.

When a buyer's IT due diligence team arrives, they're looking for documented security controls, incident response plans, clean cloud architectures, governance policies, and evidence of ongoing monitoring. Any gaps they find become escrow holds, purchase price adjustments, or representations and warranty exclusions that cost you on exit. You can discover and remediate those gaps up front.

The portfolio companies that arrive at exit with documentation likely close on time at the desired valuation.

The Six Things Due Diligence Teams Evaluate First

What Diligence Teams Need	NexusTek Status	Evidence Produced
Security Risk Assessment	Built during hold	Mapped to NIST CSF / CIS Controls — defensible framework
Incident Response	Built during hold	Documented, tested, and current with evidence of testing
Evidence of Ongoing Monitoring	24/7 via NexusOps	Logs, alerts, and SOC engagement records on continuous timeline
Current Asset Inventory	Maintained live	Hardware, software, and cloud updated in NexusOps
Governance Policies	Built during hold	Acceptable use, password policy, access control, data handling
Clean Cloud Architecture	Optimized + documented	Cost-governed, auditable, and defensible to acquirers

The Right Timeline for Exit Readiness Work

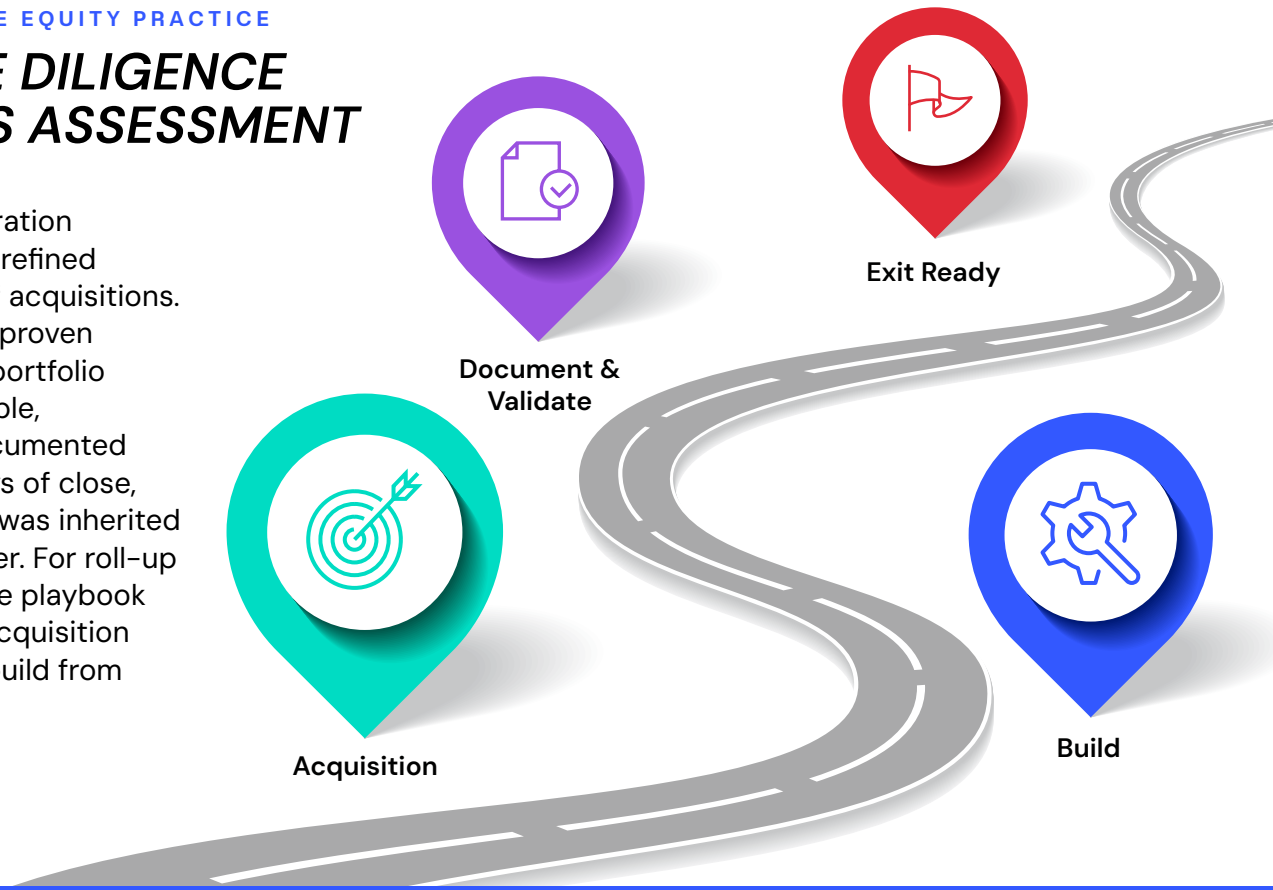
TIME TO EXIT	WHAT'S STILL POSSIBLE	PRIORITY ACTIONS
24+ MONTHS	Full remediation and documentation program; progressive build with no rush	Security baseline assessment, governance policies, monitoring deployment, cloud optimization
12–18 MONTHS	Targeted remediation of highest-impact findings; most documentation buildable	IT Due Diligence Readiness Assessment, top-priority gap remediation, documentation package
6–12 MONTHS	Documentation and presentation optimization; some remediation still feasible	Audit-ready documentation package, due diligence preparation, coaching
<6 MONTHS	Damage control, framing of known issues, acceleration of critical items	Due diligence preparation coaching, known-issue framing, rapid remediation of critical findings

When IT due diligence teams find a problem, it becomes a **negotiating chip**. **NexusTek** makes sure there aren't any to find.

NEXUSTEK PRIVATE EQUITY PRACTICE

THE IT DUE DILIGENCE READINESS ASSESSMENT

NexusTek's IT Integration Playbook has been refined across hundreds of acquisitions. It's a standardized, proven process that puts portfolio companies in a stable, monitored, and documented state within 90 days of close, regardless of what was inherited from the prior owner. For roll-up strategies, the same playbook activates at each acquisition without having to build from scratch.



CHAPTER FOUR

The Portfolio Program Model

Why a Common Approach to IT Beats Per-Portfolio Company MSP Relationships

CHAPTER FOUR

The Portfolio Program Model

Why a Common Approach to IT Beats Per-Portfolio Company MSP Relationships

Five Problems the Per-Portfolio Company MSP Model Creates

The standard model where each portfolio company manages its own MSP relationship creates five problems that a portfolio program eliminates.

01

UNQUANTIFIED RISK

The fund has no visibility into aggregate IT health or cyber exposure across the portfolio. You find out about portfolio company IT problems when the CEO calls or when the buyer's due diligence team finds it.

02

EXCESS COST

Paying for MSP relationships across different portfolio companies eliminates your group buying power. A single provider program typically costs the same or even less for significantly better coverage.

03

INTEGRATION FRICTION

Every acquisition requires navigating a new MSP relationship on deal timelines. Without a standardized playbook backed by a single provider, integration is created from scratch for each new acquisition.

04

INCONSISTENT SECURITY POSTURE

Some portfolio companies are well-protected, while others are not. The fund doesn't know which is which until a ransomware event makes it obvious.

05

EXIT DOCUMENTATION GAPS

Each portfolio company arrives at exit with its own IT documentation that is often incomplete, leaving firms scrambling to assemble what they should have been building for years.

The PE firms with strong cybersecurity aren't relying on IT delivered by multiple MSPs across their portfolio companies. Instead, they have a portfolio-level program managed by a single IT and cybersecurity partner delivering standardized controls and 24/7 monitoring across every company.

What the NexusTek Portfolio
PROGRAM DELIVERS

IT operations

- Managed IT / Co-Managed IT
- vCIO Services
- NexusOps Platform
- IT Integration Playbook
- Cloud Cost Optimization
- IT Consulting and Strategy

Cybersecurity

- MDR + 24/7 SOC
- vCISO Services
- EDR / IAM / MFA
- AI Email Security
- Cybersecurity Baseline Assessment

Cloud + Data + AI

- NexusTek Private Cloud
- Hybrid Cloud
- DRaaS
- Data + AI Services
- Portfolio Benchmarking
- Liminal AI Manager

NexusTek by the Numbers

1,200+
active clients across every industry PE acquires into

98%
client satisfaction rating proves we deliver on our promises

~6 Years
average client relationship for better hold stability for your portfolio

30
IT services experience provides depth that only comes with time

CRN
MSP 500
recognition for nine consecutive years demonstrates our expertise

GET STARTED

IT Is a Portfolio Investment. Treat It Like One.

NexusTek provides three no-cost, no-commitment starting points to help private equity firms generate more value from their IT.

01

Portfolio IT Assessment

For GPs and operating partners, NexusTek baselines IT and security health across all portfolio companies. Delivers a risk-ranked view of the portfolio and a program recommendation. No cost, no commitment.

02

IT Diligence Readiness Assessment

For portfolio companies that are 12–24 months from exit, it mirrors time-sensitive buy-side due diligence evaluation, identifies findings, and produces a remediation priority list before the buyer does.

03

IT Integration Playbook Session

For operating partners with active pipelines, it offers a 30-minute working session that produces the IT integration checklist for the next acquisition, based on our proven Day 1 to 100-day playbook.

1. Kroll, Cyber Risk at Scale: Safeguarding Portfolio Value in Private Equity, Feb 11, 2026
2. Ibid.
3. Ibid.
4. Boston Consulting Group, Private Equity's Future Is Digital First and AI Powered, Jan 7, 2026
5. Ibid.
6. EY, What Can Private Equity Do Now to Finish Strong? EY Private Equity Exit Readiness Study 2025, Jun 11, 2025
7. Boston Consulting Group. Private Equity's Future Is Digital First and AI Powered, Jan 7, 2026
8. Kroll, Cyber Risk at Scale: Safeguarding Portfolio Value in Private Equity, Feb 11, 20262026

nexustek.com

Protect Portfolio Value. Accelerate Growth.
nexustek.com · (877) 470-0401 · info@nexustek.com

nexustek