

Getting to audit-ready security operations

How to strengthen compliance during an acquisition

When companies merge, the headlines celebrate growth, synergies, and market opportunities. Behind the scenes, however, physical security leaders face many quieter but equally high-stakes challenges. Chief among these challenges is maintaining compliance in all areas, and ensuring the combined organization is prepared for audits of its newly integrated operations.

Unlike assessments, which provide general observations, audits are formal examinations of compliance with written standards. They require documented evidence, paper trails that prove policies are in place and working as designed. Audits are unforgiving—every finding in an audit report requires a response.

During acquisitions, audit vulnerabilities can grow even more complex. Two organizations with disparate controls, cultures, and contractual obligations must suddenly function as one. Unless security leaders are proactive, gaps can open quickly—gaps that regulators, customers, or even investors may exploit when an audit inevitably occurs.

Our recent white paper, [Aligning Roadmaps for Acquisitional Growth](#), offers an overview and helpful scenarios for addressing physical security challenges during M&A activities. This article provides our specific guidance on audit readiness during these times.



Navigating compliance risk

The link between acquisitions and audit readiness is straightforward: an acquisition can multiply compliance risks overnight. Consider the following areas of exposure:

- + **Inherited obligations.** The acquired company may have contractual security requirements baked into customer agreements—requirements that can easily get lost in the shuffle if no one captures them during due diligence.
- + **Mismatched controls.** The parent company may have a mature audit program, while the acquired company has little evidence to demonstrate compliance. In such cases, it falls on the acquiring company to close gaps quickly.
- + **Expanded audit landscape.** Acquiring a new business line can introduce industry-specific regulations that the parent company hasn't previously faced—think banking, healthcare, or government contracting.
- + **High cost of failure.** From fines to litigation to loss of major customer contracts, the penalties for non-compliance often dwarf the cost of investing in readiness upfront.

Audit readiness isn't just about passing a test. It's about protecting revenue, reputation, and even executive liability. Work closely with your security consultant to address the unique variables affecting compliance during and after your acquisition.

Following are some high-level steps to help guide this effort.





Step 1: Understand the audit landscape

Before you can prepare for audits, you need clarity on what you're preparing for. That starts with mapping the different types of audits you might face:

- + **Internal audits** conducted by the acquiring company's audit team to measure compliance with internal controls.
- + **External regulatory audits** triggered by industry or standards-body regulators such as SEC, Sarbanes-Oxley, PCI DSS, ISO 27001, and UL.
- + **Customer audits** initiated by enterprise clients to verify that you're meeting the security requirements in their contracts.
- + **Third-party or insurance audits** performed by partners or insurers who tie premiums and terms to your security posture.

Acquisitions often expand exposure across all four categories. For example, a company moving from privately held to publicly traded suddenly faces a higher bar, including SEC compliance and Sarbanes-Oxley reporting.

Step 2: Treat compliance as a pillar of the M&A team

In many successful acquisitions, compliance is treated as a dedicated "pillar" within the acquiring company's M&A working group alongside finance, IT, and HR. This pillar typically compels security, legal, privacy, and internal audit leaders to work in close coordination.

The combined role of this audit readiness committee is to:

- + Identify all applicable controls across the acquiring company.
- + Map the acquired company's program against them.
- + Identify gaps in compliance and propose mitigation strategies.
- + Report findings back to leadership with a cost-benefit analysis.

By institutionalizing compliance as a pillar, companies avoid the common pitfall of overlooking security controls until after the fact.

Step 3: Perform courtesy (pre-) audits

Waiting for regulators or customers to discover gaps is risky. A more proactive strategy is to conduct courtesy audits—internal pre-audits that simulate the scrutiny of an external body.

Courtesy audits help you:

- + Validate that policies are not just documented but evidenced in practice.
- + Identify where interim controls are needed until full remediation is possible.
- + Train teams to respond consistently to audit requests.

For example, if your standard requires “90-day video retention,” can the acquired company produce logs that prove compliance? If not, interim controls—such as extending storage policies or documenting compensating measures—can be put in place. Work with your security consultant and leverage their expertise to brainstorm the most impactful proactive audits to perform.



Step 4: Focus on evidence, not just policies

Auditors don't take your word for it—they want proof. That means your program must produce key artifacts to prove compliance, including:

- + Logs of access control transactions
- + Video retention reports
- + Training records
- + Documentation of interim controls and remediation plans

You can't claim compliance unless you can show the evidence. In many acquisitions, the hardest work isn't aligning controls but building evidence where none exists.

Step 5: Write policies that set you up for success

A common audit readiness mistake security teams make during an acquisition is drafting overly prescriptive policies that become impossible to uphold across diverse environments. The key to avoiding this pitfall in many cases is to try crafting policy that captures the spirit of how to comply without stipulating the precise **facts** by which compliance will be assessed. Smart policy writing ensures that when auditors ask, you can show compliance with the essence of the requirement—even if technical implementations differ between legacy environments.

For example, instead of mandating “All IDFs must have floor-to-ceiling walls,” consider framing the intent: “IDFs must be protected against unauthorized entry.” That way, alternative controls such as motion detectors, and alarms can demonstrate compliance without incurring multi-million-dollar retrofits.





Step 6: Prioritize gaps based on risk

Not all compliance gaps are equal. Some require immediate action; others can be closed over time. To allocate resources wisely, weigh:

- + **Severity of penalties.** Is the fine \$10,000—or \$100 million?
- + **Impact on revenue.** Will failure jeopardize a flagship customer contract?
- + **Legal exposure.** Could gaps in compliance expose executives to personal liability?

By tying remediation priorities to risk and cost, security leaders can argue for budget with far more credibility.

Step 7: Leverage external expertise

Many companies underestimate the value of third-party consultants during M&A transitions. As an independent assessor, your security consultant can provide:

- + A history of and familiarity with a wide range of acquisition-related physical security stories.
- + A clear-eyed view of gaps without internal politics.
- + Benchmarks from similar acquisitions and regulatory environments.
- + Cost models for closing compliance gaps.

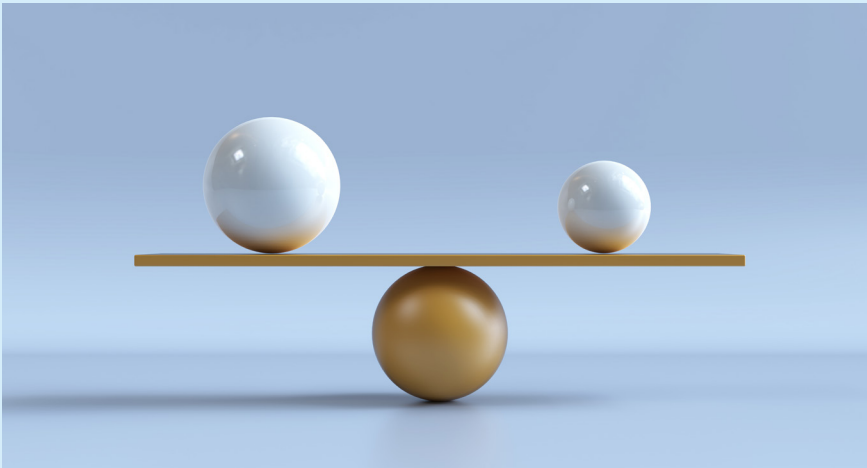
Hiring a consultant for \$50–100K is a small investment compared to the financial, legal, and reputational damage of failing an audit.

Focus on the upside as well as the risk

While much of the conversation around audits focuses on risk, there can also be tangible rewards. Insurance carriers, for example, may lower premiums for companies that demonstrate strong controls. Conversely, poor practices can raise costs. In either case, being audit-ready has bottom-line impact.

Acquisitions are stressful enough without the added pressure of audit failures. By treating compliance as a core pillar of integration, performing courtesy audits, focusing on evidence, writing smart policies, and prioritizing gaps based on risk, physical security leaders can protect their organizations from costly surprises.

Audit readiness during M&A isn't just about checking boxes. It's about showing regulators, customers, investors, and employees that security remains strong, even in times of change. And in the world of physical security, that credibility is worth every bit as much as the deal itself.



When a company evolves through acquisitional growth, its physical security team needs a thoughtful approach to managing the changes. Read our white paper, [Aligning Roadmaps for Acquisitional Growth](#), to find insights and guidance to help your team when growth happens.

Our office:

700 Larkspur Landing Circle, Suite 150
Larkspur, CA 94939

Email and web:

info@zbeta.com
www.zbeta.com

Phone:

(855) 559 2382

