

Testing is the new due diligence

Treating solution test plans as a core design activity, not a procedural afterthought



When you're fully committed to a successful deployment, adopting a testing mindset up front is invaluable. Many physical security teams, if they do solution testing at all, approach it as a narrow technical exercise. In practice, its value is broader and more strategic. Done right, testing at all stages of security design unlocks valuable, timesaving, security-strengthening insights that deliver superior outcomes.

As we explore in our [recent white paper](#), embracing this mindset means examining security solutions through multiple lenses at once: technical, operational, architectural, and human. The best test plans find a structured way to integrate those perspectives rather than privileging one at the expense of the others.

At ZBeta, we use a holistic testing protocol—tailored to the client, their facilities, their project scope, and their solution goals—that goes beyond technical examination to embrace important adjacent principles. These include:

+ **Impartiality and objectivity.**

Effective testing requires the testers to be as neutral as possible about predetermined technology brands or preconceived system constructions. ZBeta has always taken this to heart, and it's the main reason we don't sell products or represent manufacturers. Our tests are designed to answer client questions, not just validate vendor narratives. That objectivity matters most when decisions involve trade-offs rather than obvious winners.

+ **Cross-audience impact that meets all requirements.**

Executives need clarity and confidence. Technical teams need detail and specificity. Users need ways to comply effortlessly with security so they can do their best work. The right testing produces all of these outcomes, fostering design conversations that can move between strategic, implementation-level, and hands-on use cases without confusion or distortion.

+ **Avoidance of the most expensive failure mode.**

The most damaging outcome is rarely "The solution doesn't work." It's: "The solution works, but only if we can justify more budget, time, customization, and disruption than anyone expected." Most security solutions can be made to work eventually. The real risk is discovering late in the project (or after implementation) that achieving the desired outcome requires far more resources than anticipated. Good testing shifts those discoveries forward, when the impact of change is still manageable.

- + **Knowledge that compounds rather than disappears.**
When organizations test in isolation, they relearn the same lessons repeatedly. In contrast, you can partner with a security consultant who brings a wide array of experiences to every engagement. At ZBeta, this approach allows insight from one design experience to inform the next without compromising any amount of client confidentiality. Over time, patterns emerge that would otherwise remain invisible.

The best-laid deployment plans only go as far as what you can see coming. The right testing—at the right level, in the right environment, with the right priorities—can mean the difference between high-value, cost-efficient outcomes and unmitigated project chaos. Work with a consultant with extensive experience, compounded by the bench strength of their team. These consultants will be tuned into the latest wisdom and best practices for testing your solution in the unique ways it requires for success.



For more details on testing philosophy and best practices for physical security systems, read our white paper, [Making test plans worth your investment: How innovations in security solution testing pave the way to on-budget results.](#)



ZBeta provides lab space for testing just about any solution under conditions that will closely resemble your built environment. For more information, visit zbeta.com/labz.

Our office:

700 Larkspur Landing Circle, Suite 150
Larkspur, CA 94939

Email and web:

info@zbeta.com
www.zbeta.com

Phone:

(855) 559 2382

