

Taking the initiative to get it right

4 questions to ask your physical security consultant about solution testing

In physical security, testing is often treated as a luxury—something you do when a project is unusually complex, unusually risky, or unusually well-funded. Many organizations assume that testing is already happening somewhere upstream, handled quietly by manufacturers before products ever reach the field. They also assume they can't afford the time, disruption, or expense of doing their own testing.

The first assumption is both correct and dangerous, because what matters is how the components perform in your environment, not in a quality assurance cycle.

The second assumption is worse yet. As we explore in our [recent white paper](#), testing isn't an indulgence; it's one of the few reliable ways to align expectations with reality before those expectations become operational commitments. The point of testing is to break things early on during design so you don't have to fix them later on when the solution is live. The cost of the first option more than pays off the risk of the second.



Not all tests are helpful for every solution, and no two environments are the same. So if you don't have access to a lab to test in, work with a physical security consultant who does. Before you engage, determine whether they have the test capabilities you need for shoring up the risks facing the solution design and implementation specifics they advise. Ask:

1. What success factors and functional requirements are you testing against?

Before you test—anything—you must understand the requirements you've derived for your solution—starting with the central problem you're trying to solve. Then, conduct testing accordingly so you and the consultant can interpret the results with this in mind. Identifying requirements prior to identifying solutions sounds obvious, but it's common to get it the wrong way around, leaving you testing against conditions that don't exist in your environment and shopping for solutions to problems you don't have. Your consultant should operate from this principle at all times in the testing services they provide.

2. What kinds of testing will the security consultant perform?

Make sure you're working with a security consultant who understands two important things: your business requirements, and what the solution must yield (beyond simply "working" correctly) to meet those requirements. A solution might run perfectly end to end but still miss by a mile when it comes to solving your actual challenges.

3. Where will they do the testing, and how closely can it mirror your site layout and conditions?

To reproduce outcomes you can examine, you should build your tests in an environment that's configured as much like your own facility as possible. This lets you prove all the components will work together in concert by implementing them on actual doors and walls that are built and configured to resemble your architectural layout, fitted with identical hardware in conditions that mirror the lighting, positioning, aesthetics, and other factors of your actual environment.

4. What meaningful value will their test capabilities add to the consulting engagement?

Not all projects require the full gamut of testing. Not all budgets can accommodate it, either. Work with your security consultant early in the planning stages to define the areas of testing that will best suit your purposes—the proverbial "bang for your buck." Identify choke points and other high-risk solution parts, and aim your testing there for starters.



Testing costs money and time, but if you do it right, there's a multifold return on your investment in the form of clarity, credibility, and averted risk. The more you understand your design, the more you can innovate—and intelligently ward off expensive surprises. Understand the scope and value of testing that makes sense for your project, and build the cost into your budget up front to avoid disastrous break-fix problems post-deployment.

Testing makes your plan more durable and your deployments smoother. As a thought exercise, it also compounds your team's shared wisdom and credibility, project over project. Work with a consultant who understands and supports these priorities and can help fit the right test plan into your roadmap for serving your precise business and physical security needs.



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

