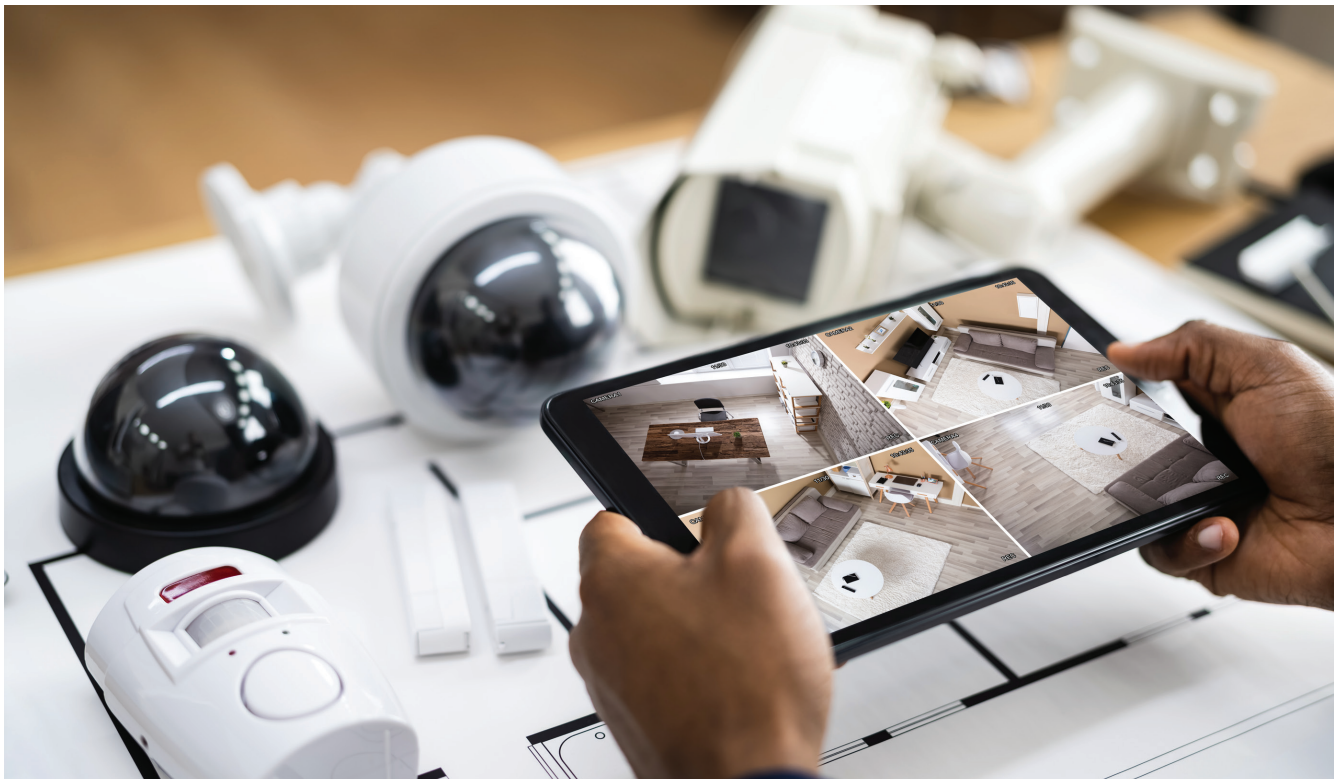


6 pro tips for a successful systems migration

Keep these in mind when overhauling your physical security environment

Is your organization likely to overhaul its physical security technologies in the next eighteen months? Our recent white paper, [Physical security systems migration considerations and scenarios](#), provides in-depth guidance for the five primary migration activities: data gathering, design and engineering, sequencing and scheduling, procurement strategy, and cutting over.

But beyond tactical considerations, there's also the overall mindset you and your security team inhabit as migration planning proceeds. This article provides a round-up of six pro tips to keep in mind. You can also join us at [GSX 2025](#) where one of our principal migration consultants, Mike Lavway, will present his insights on these topics in greater detail. This session is scheduled for **Tuesday, September 30th from 1:30 – 2:30 CT.**



1. Don't start until you're sure you're ready.

For starters, make sure you know what you're getting into. Migrations are a significant commitment, and once you start into migrating your systems, there's really no turning back. Every proposed project needs a "go/no-go" decision point, so don't rush to yours too quickly. How urgent is the need to modernize? If you're stuck constantly restarting servers, or you lack IT support for systems and replacement parts, or users can't easily get to the areas where they need access—you're probably due for a migration. If your issues are less mission-critical, think about other alternatives.

Ask yourself the following:

- + **Is your migration fully planned out**, with reasonable end-to-end certainty on your path to success? Have you thought through the entire budget—capital expenses, operating expenses, future annual fees, labor, and other ancillary costs? Have you compiled the true cost of not migrating by quantifying current lost productivity due to failing systems, excessive maintenance costs, or operational costs for alternate measures during frequent outages?

Once you start a migration, there's no turning back; the budget and expectations have already been excruciatingly hashed out. The fix-as-you-go approach only yields situational relief; your best rollback and contingency options along the way won't solve fundamental problems with the overall plan.

(For detailed expert guidance on planning a migration, see our white paper from earlier this year, [Plotting a sustainable technology roadmap: Picturing and achieving the future state of your physical security solution.](#))

- + **Is everyone on board and ready to go?** Migrations are a chance to get your house in order. Take a look at any weak points in your current security operations and tune them up as needed to be ready to take on the migration scope. Ditto your stakeholder teams and their readiness—don't get started until you know what you'll need from everybody and you have a clear path to getting it.
- + **Is the juice worth the squeeze?** Whatever you're planning to put into the migration, both in dollars and in human toil, should be very likely to yield the outcomes you're looking for. If it seems like those results are in peril, you're not ready to call "go."



2. Seize the opportunity to recalibrate and improve.

As our [white paper](#) outlines, migration planning is a holistic activity, generally touching all areas of your physical security operations. One way to maximize the value of the time you spend on it is to work with your security consultant to make note of any deviations from standards that you discover (or knew about already) and make a pre-deployment plan for their improvement.

System upgrades are a timely chance to examine and optimize various processes and activities that you know you can do better. Not all of these can realistically be acted on in the time frame of the migration project schedule, so prioritize the ones whose resolution will actually help the migration be more impactful.

For example, you might:

- + **Refresh policies to confirm relevance.** How long has it been since you looked at corporate policies? Will they need to change once you change or update your systems?
- + **Update basis of design, design guidelines, and procedures.** What are your highest-priority challenges, and where can you make compromises to make the migration successful?
- + **Check on other updates.** What additional systems components can you or must you update in conjunction with a migration? What cable do you have installed? What readers are you using at the edge? What credentials do you use?
- + **Remain open to change.** Migrating will lift the hood and shine a light on blemishes that have been ignored for a long time. Are you ready for the spotlight? Are you ready to break old habits and fix old compromises made long before your time?

Pay special attention to policies you enacted once that don't quite make as much sense anymore. Persisting these policies into the updated environment creates the nuisance and expense of having to remediate aspects of the new system as soon as it's deployed.

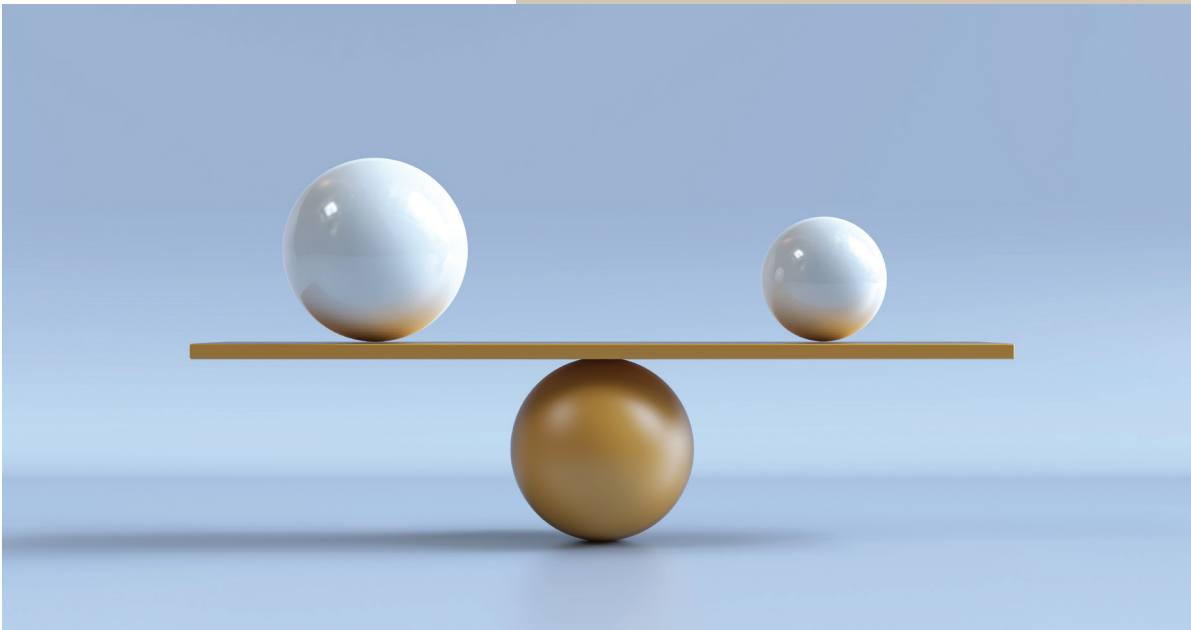


3. Don't rush into procurement.

Your selection of an integrator to do the migration work is of paramount importance, particularly if you're migrating multiple sites across more than one geography. Work with a seasoned security consultant that has experience with centrally managing projects nation-wide to navigate these waters and steer your procurement strategy toward the best choice of vendor who will meet your needs. Seek a "coalition of the willing" that forms a quadrant of productivity across your security team, procurement team, security consultant, and the business groups your new system will support. Consult with this coalition to make the right choice.

As you do this, watch out for the most common pitfalls that arise during the integrator selection process. You might have a bias toward ones you've used before, or you might be tempted to favor the lowest bid. You might even forego receiving bids if you've made up your mind who you want. Or you might opt for a project management company who outsources the integrators, but the project managers might not keep their eyes on relevant individual expertise that each integrator brings to the table.

Most of all, push yourself to see the context of every procurement option you consider. Your security consultant will be instrumental in providing this perspective. Every integrator has their own way of bidding a deal, their own policies around work time versus after-hours availability, and their default own methods of tackling unexpected issues they encounter—methods you're likely to revise with the help and insight of your security consultant. Look carefully at all of your options and trust your security consultant's experience to help guide you to the vendor selection that's best for you.



4. Measure effectiveness, not just performance.

It's one thing to know whether your migrated physical security system will perform the way you want it to. It's another thing to understand and quantify the impact migration has on your security operations and your company's larger business mission.

When you measure migration project performance, you're asking: Did our security team deliver on the terms of the project? Did we live up to our scope of work? Was the migration delivered on time and within budget? Did we deliver all of the devices and firmware and infrastructure pieces we said we'd deliver? All important questions—but just as we advise customers during roadmap planning, the questions also require asking “So what?” at the end of each one. To wit: How will the migration help users and stakeholders achieve success with the goals you sought to achieve?

And so it's important to measure effectiveness as well. Think of this as: OK, we understand WHAT we did; now HOW is it going to help us? Migration success requires measuring both of these outcomes, because people remember rewards. Three years out, your stakeholders are likely to recall how much time and effort went into the system migration; help them also to measure whether the effort substantially served their business and operational needs.

To measure effectiveness, work backwards from the short list of “north star” goals you make at the onset of the project: “Our migration should achieve X, Y, and Z objectives above all else.” Then, instrument the project in ways that allow you to check your progress against these effectiveness goals, even as you're working on making it all perform and deliver on the more prosaic details listed in your statements of work.

Our programs are only as successful as we can articulate how they've achieved their purpose. Measuring effectiveness helps tell the story of the “why” to help keep and maintain your executive and stakeholder buy-in.



5. Minimize disruption.

Doctors have a creed: First, do no harm. Extending this mantra from physical wellness to physical safety and security isn't that big of a stretch. In the case of a systems migration, one key harm to watch out for is harm to the business as your migration proceeds.

The responsible way of proceeding through a migration project is to remain vigilant, mindful, and respectful of all teams' needs and expectations, all while executing on a well-made plan. The number one expectation from many stakeholders is that you'll minimize business disruption. Look for ways to do this in the following areas:

- + **Core business.** The business units that do the work of your company and drive revenue are the same ones you're striving to keep secure. Migration is a success when potentially invasive upgrades dovetail as closely as possible with maintaining continuity of business operations.
- + **Culture.** Your users are accustomed to thinking about security at your company in a particular way. Introducing unnecessary changes or inconvenience throughout a migration creates stress, confusion, non-compliance, and other potentially unsafe responses. Always keep in mind how your people will interact with the security systems throughout design, engineering, and cutover activities, and do your best to communicate unavoidable changes and disruptions in a timely, empathic way.
- + **Budget.** Whoever gave you the funding for your migration is invariably watching to make sure they put their money toward a worthwhile cause. Disruptions in budget can be just as harmful to your migration project as disruptions to the business and users themselves. As the project unfolds, work with stakeholders and communicate with sponsors to ensure the inevitable hiccups are promptly and sensibly addressed.



6. Think beyond the finish line.

Let's daydream for a moment. It's eighteen months into the future, and you've just finished the migration. Per our guidance on dual measurement, the project was both a performance and effectiveness success. What's next? What happens once everything starts working?

You'd be mistaken to think the surprises end when the last migration node is cut over. You'll have a learning curve as new features come online, producing alarms and data you didn't previously account for. Have procedures ready for dealing with these Day One consequences. Think ahead as best you can for the system behavior you're able to anticipate—and also have a general plan for dealing with the surprises that happen anyway.

If you lack a way of dealing with unexpected behavior once the new system is active, your response to these surprises will be problematic. In advance of cutting over, create standard operating procedures for addressing the unpredictable changes that you, your team, and your users will encounter. Don't let yourself become victims of your own success.

Here are a few examples to look out for:

- + What happens if there is an influx of alarms that previously went undetected?
- + How do you process service requests during the inevitable first few weeks of adjusting to the new system?
- + How do you train your team on new features or functions?
- + How do you orient business end users on new procedures and technologies?
- + How do you modify processes to perform enduring tasks in a new way?



For more tips and detailed guidance on systems migration strategies, read our white paper [Physical security systems migration considerations and scenarios: What to expect when refreshing your technologies](#). Want to talk in person? Join us at [GSX 2025](#) in Suite 1277!



Our Office:

700 Larkspur Landing Circle, Suite 150
Larkspur, CA 94939

E-mail and Web:

info@zbeta.com
www.zbeta.com

Phone:

(855) 559 2382