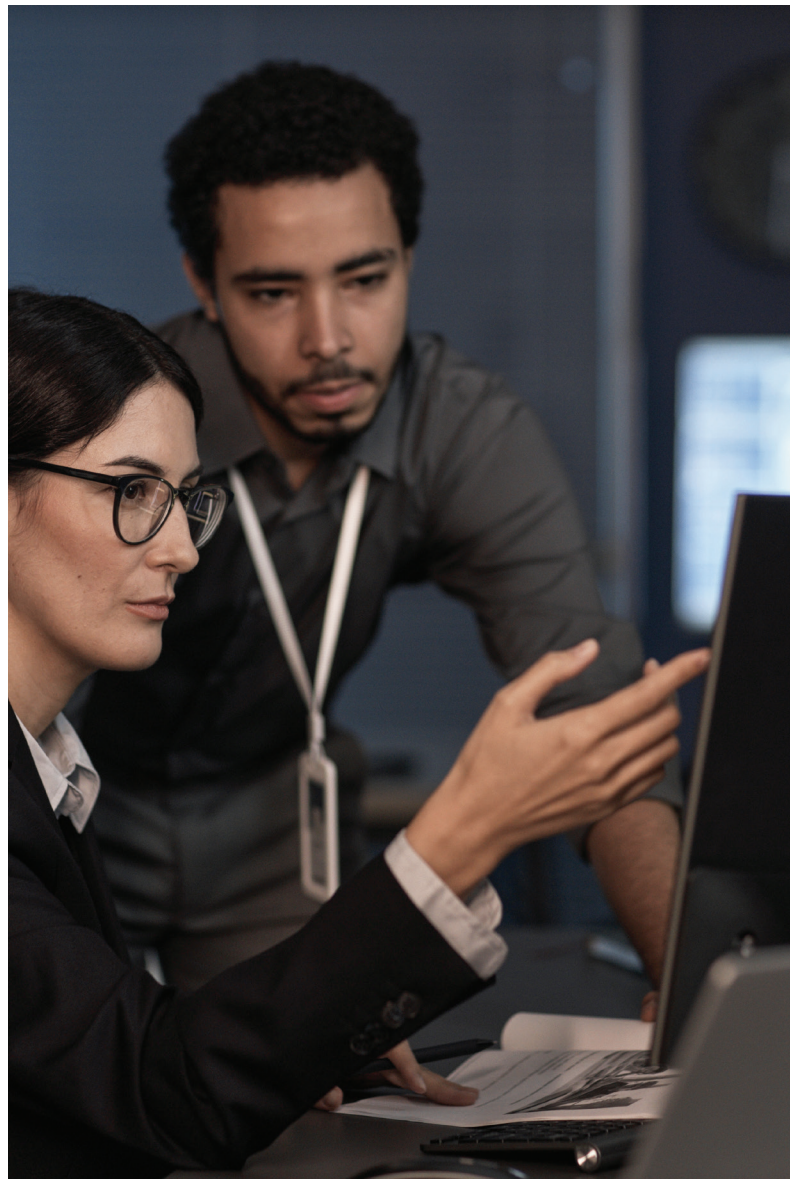


The art of cutting over

5 tips for seamless transition to your newly migrated security system

Risk mitigation is central to physical security systems migrations. You face risks throughout your migration of delivering on time, on budget, and with minimal disruption, and cutting over is where these risks all culminate in your project's conclusion. For best results, always leverage the experience and perspective of your security consultant relationship to gain the risk mitigation insights you'll need to be successful on your particular migration. Meanwhile, here's a high-level list of the most important dos and don'ts.



1. Don't persist unwanted issues

The worst outcome of any systems migration is replicating past issues in the new solution. But it happens. Malfunctioning hardware gets re-incorporated, faulty (and often disabled) alarm circuits get cut over as is, and terminated credential holders who improperly have access retain it. Gather these risk areas using a combined data-driven and human-driven approach. First, run as many targeted database reports as you can. It can even be cost-beneficial to invest in customized queries and reports to yield detailed insights your systems can't provide on their own. Then supplement and prioritize these findings with anecdotal data by asking your team: What “temporary” work-arounds did we devise in recent years in lieu of diagnosing and addressing actual system faults? What things did we turn off in the past year rather than simply fix?

Your best defense against persisting critical issues is by referencing the current state assessment you performed as part of your roadmap (see our earlier white paper, [Plotting a sustainable technology roadmap](#)) and using that information to mitigate risks.

What you can do:

- + **Test, test, test.** Establish well defined pre-testing procedures as a central tenet of your migration cutover. Use the data from your targeted and customized database reports mentioned above to guide your test planning, including pinpointing the nature of the results you want to see in the tested outcomes.
- + **Triage.** Sort any issues that arise into two lists: existing issues carried over from the old system, and issues caused by the migration itself. Among other clarifying benefits, keeping these lists reduces the risk of potential finger pointing and accountability gaps.
- + **Lean into process.** Be ready with operational work-arounds. In the likely event you don't have scope or budget in the migration project to resolve all cutover issues, planning ahead with a formalized processes for identifying the issues ensures you can readily address them in the future.





2. Brace yourself for surprises

The smartest strategists don't rule out the unexpected—they plan for it. Even greenfield, new construction projects throw curveballs that put schedules at risk, which makes the kind of retrofitting you perform in a migration project even riskier in this regard.

The game you're playing is to reduce the pesky change orders that can pile up and derail your project's budget, implementation schedule, credibility, and overall success. Design and procurement strategies for conversions are best calibrated against the availability of accurate information on current state conditions as well as the project's schedule needs and budget constraints.

What you can do:

- + **Document your site.** Similar to avoiding issue persistence, preparing for the unknown means investing in a structured approach to surveying and assessing current state, especially in areas of the migration project where you lack good design and as-built documentation.
- + **Script your cutovers.** No effort is perfect, and questionable and completely unpredictable historical design and installation decisions will still show up unannounced. In tandem with collecting site survey data, create clear and concise cutover scripts for each element of the migration plan.
- + **Make plenty of "Plan Bs."** Your cutover scripts should include concrete go/no-go milestones and decision points, retroactive "back-out" scripts, and alternative work plans for preserving utilization when the migration hits a snag.

3. Treat business continuity as sacred

Even the best planned and risk-managed migration will have system downtime. This inevitability is important to acknowledge and communicate so that the business units you support can set their expectations accordingly. Areas and assets that require monitoring and surveillance will be blind for periods of time, sometimes longer than intended. Ladders block doorways. Effective access control is temporarily stymied when readers and door sensors are inactive.

The risk here is not just losing critical business and security productivity for your company but also losing good will between the business and security organizations. Plan ahead so this doesn't happen and you can carry your migration over the finish line with minimal disruption.

What you can do:

- + **Message your solidarity.** Make it clear to your sponsors and stakeholders that throughout your migration project, maintaining a secure, productive business environment is your #1 goal.
- + **Finish what you can in advance.** Wherever possible, engineer your equipment center upgrades to enable new controller, board, power supply, and network equipment to be fully operational prior to cutover, either in temporary or permanent locations.
- + **Build in decommissioning time.** Prior to cutover, identify any instances where existing equipment must first be taken offline, and reserve those activities for days of the week and hours of the day when this fact will be less impactful.
- + **Actively manage downtime.** Track your progress and surprises throughout the cutover. Stay on top of communication protocols with the business and with security operations center (SOC) operators to help ensure that sensitive areas are not left unprotected without mitigations.
- + **Beef up security.** Higher-risk areas are likely to need temporary security officers during cutover. Estimate this expense up front and incorporate it into budgets and staffing plans.





4. Monitor and manage all systems in concert

The vast majority of systems migrations are not completed in a day, or even a week. Some can take months. In instances where a single system or set of platforms is being replaced wholesale by another, a migrating organization often needs to stand up and operate multiple platforms simultaneously—and usually for the first time, unless your migration happens to entail consolidating from multiple legacy systems down to one.

Managing simultaneous systems effectively can present significant challenges if your security organization hasn't developed the resources, processes, and tools over time to do so. Complicating factors include shifting personnel roles and responsibilities for the duration of the cutover, manual duplication of data entry across systems, and added complexity and inefficiency around monitoring alarms.

What you can do:

- + **Embrace the complexity.** In your migration planning and organization, focus specific consideration on the reality of administrating multiple systems during the project, especially for complexities that touch SOC operations and access management. These considerations are as critical to your success as those for cutting over a specific set of cameras or doors.
- + **Plan ahead.** Have clear migration sequencing and responsibilities clearly defined. Invest in training, and be ready to pull in additional resources or socialize increased workload with existing team members.
- + **Shop for helpful tech.** Continue working with your security consultant throughout cutover, including hearing any recommendations they have about the potential for using automation solutions, such as ones to keep multiple databases synced accurately. These tools add another piece to the tech puzzle of cutting over, but the investment could save you valuable time and effort overall.

5. Don't forget to optimize

While systems migrations themselves are an occasion for improving efficiency and functionality, true operational gains occur on an even higher level. Every migration presents chances to optimize in the form of advanced configuration, process automation, and utilizing unrealized potential in your new investments.

Maximizing solution value is one of the most difficult aspects to achieve in any systems project, migration or otherwise. During a migration, the duration and incremental nature of your efforts typically make optimization challenging, especially since your primary focus is mainly on staying the course of the overall endeavor. Meanwhile, your integrator has their hands full just meeting the minimum specs of the engagement.

What you can do:

- + **Leverage your partner relationship.** Your security consultant can provide valuable perspective around optimization, not only because they have a broad range of systems migration experience, but also because their position outside your company enables them to more readily “see the forest for the trees” and help ensure you don’t leave any time- and money-saving options on the table.
- + **Resource optimization separately.** For under-optimized solutions, we advise clients to fund optimization efforts as a budget line item distinct from migration itself. Create a discrete team with a scope focused on getting the most out of your migration solution, populated with in-house resources, manufacturing professional services from your manufacturer, or your security consultant’s experts.
- + **Mind the (consumption) gap.** Examine your “consumption gap”—the range of unused features in your solution that can be applied to help tune and improve performance. Ask: Are you fully aware of your current system’s range of capabilities? What features did a provider sell to you that you’re not currently using? Then, work with your security consultant to determine the ways you can leverage these existing investments to achieve new levels of productivity with your migrated solution.



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

