

Physical security systems migration considerations and scenarios:

What to expect when refreshing your technologies





Introduction

Migrating physical security systems can take many forms, but there are basic throughlines that, when you observe them, can guide you to success. One is understanding the common migration components and how they interdepend. Being planful and proactive, particularly around procurement strategies, sequencing your migration, and cutting over carefully as the new system comes online, helps alleviate disruption and mitigate risks. ZBeta has helped clients in many industries tackle nearly every kind of systems migration and navigate a wide range of variables. Here, we share our insights on systems migration, including three real-world scenarios where organizations we worked with overcame obstacles and made their migrations a success.

Let's get tactical

The requirements around replacing or upgrading physical security systems vary widely from each organization to the next. Migrating to a new solution might be a matter of simply upgrading all cameras across your facility, or it can be as major as a complete overhaul. As with any security project, forethought and planning are key to success, no matter the migration scope.

Migration is the “second act” of designing and implementing your upgraded security solution. Act one was laying out your plans and requirements for the migration—that is, creating your roadmap, as described in our [earlier white paper](#), “Plotting a sustainable technology roadmap: Picturing and achieving the future state of your physical security solution.” Whether you followed that guidance or came up with a roadmap on your own, you’ve won half the battle. You’ve done the formative work to get your solution approved; now you need a detailed structure that will ensure implementation success.

The roadmap exercise helped you figure out where you want to go as a security team with your upgraded solution. Migration is all about getting to that solution. This white paper talks you through the high-level migration activities, discussing risk mitigations and other details for each activity. Along the way, we’ll share three real-world scenarios where ZBeta helped clients with various kinds of migration projects and how we navigated the complexities of each one.

The five primary migration activities, roughly in this order, are:

1. **Data gathering.** Conduct due diligence (e.g. site surveys) to establish your migration baseline.
2. **Design and engineering.** Identify roles and standards, and adapt them to your migration project.
3. **Sequencing and scheduling.** Figure out the steps for your migration and put them in order.
4. **Procurement strategy.** Decide how you’ll choose the vendor to implement your migration.
5. **Cutting over.** Plan exactly how and when to bring each part of the migrated solution online.

In the following sections, we’ll take a closer look at each of these systems migration activities.



1. Gather the necessary data

Let's start by considering the data you should gather and provide to make migration successful.

Effective site documentation is essential for many security operations, even though we're all aware how easy it is to fall behind in maintaining it. Systems migrations provide an excellent opportunity to catch your security team up to date. There's also more at stake with migration: due to system-wide dependencies, gaps and errors in documentation compound to produce outsized negative impact to your project's success.

Bottom line, the more you know and communicate about your existing environment, the greater your accuracy when requesting and reviewing the bid you receive from a value-added reseller (VAR) or security integrator seeking to implement your migrated solution. Gathering this data also gives you confidence that you've warded off project risk by setting the right expectations with your sponsors, users, vendors, and other stakeholders.

At the root of data gathering for migration is a site survey. Conducting this survey prior to migration delivers a baseline assessment to identify current vulnerabilities, evaluate system performance, and guide the design of an improved solution. It ensures that new investments align with risk profiles, operational needs, and compliance requirements. If your migration spans multiple facilities, it's ideal to do a survey for each one, as one facility's information might differ from that of the others in hidden ways, leading to mid-project confusion and rework. To save time, you might conduct multiple site surveys in groups, regionally, or one at a time as part of a rolling process.

The details of a site survey will produce helpful knowledge about:

- + Device locations, types, and quantities.
- + Door hardware types and functions.
- + Equipment center inventories and wall/rack layout.
- + Details about network ports, electrical circuits, cabling and raceway, and wiring and resistors.
- + Additional findings that prove critical to your specific project.

Every site is different, and the documentation for each is usually at least slightly out of date. For best results, collaborate with your security consultant—they know which rocks to turn over, and can ask questions as outsiders based on their experience to ward off expensive gaps and errors in the documentation you might not have otherwise been aware of.

Real-world scenario: Campus migration

A ZBeta client, the academic medical campus for a major U.S. higher education institution, sought to bring together its disparate video management and access control systems under a single, unified security management platform. The scope of the project spanned multiple facilities but was contained to a single campus, supporting roughly 2,000 users including faculty, students, providers, and staff, along with patients and visitors at the clinic and other hospital buildings.

Risks:

- + Cost and schedule overruns from unknown or unanticipated conditions in the current systems.
- + System downtime leading to disruptions in security and user experience.
- + Under-optimized feature sets and missed optimization opportunities.

Mitigations:

- + Validated relevant setting, configurations, and performance of the selected platform in our lab.
- + Used structured output from a detailed site survey to fill in gaps from the as-built documentation.
- + Created a pre-cutover plan and used it to actively manage downtime throughout implementation.

Real-world scenario: Enterprise migration

A Fortune 50 multinational financial services institution was planning a migration in their U.S. facilities in three phases: First, upgrading their current card readers; then, replacing the remainder of their access control hardware; and last, migrating to a centralized access control platform, replacing a multi-platform configuration that had resulted from various mergers and acquisitions over the years.

The firm employed nearly 200,000 people, spanned many industry verticals, and operated various sites including datacenters, retail locations, satellite office buildings, and corporate headquarters. Among many other high-impact considerations, this client was beholden to strict requirements for business and operational uptime, not only to meet revenue projections but also to comply with rigorous U.S. governmental regulations.

Risks:

- + Costly business disruption across hundreds of facilities and many lines of business.
- + Complexity of unifying operations and standards across dissimilar facility types.
- + Reliance on new-to-market technology to address outstanding audit findings.

Mitigations:

- + Divided up the various site types, put them in tiers, and phased migration in a logical sequence.
- + Tailored cutover plans to each business unit to minimize disruption of business activities.
- + Coordinated project schedules with equipment release and availability dates to establish dependencies and reduce delays.

2. Flesh out your design and engineering approach

Given the data you assemble and the requirements for your migration project overall, it's important to think early on about how you'll address your migration's design and engineering requirements. For our purposes in this white paper, "design and engineering" refers to the end-to-end security design for your migrated environment and the work it will take by you, the integrator, and/or your security consulting partner to develop the technical solutions, calculations, and specifications for your migration design.

Much of this consideration comes down to how you will sequence your migration activities, which we'll say more about shortly. Some migration projects resemble new construction in that all design and engineering activities happen at the start of the engagement. In most migrations, however, this isn't the case—design and engineering activities are staged throughout the project, as survey and discovery happen at each site, building, or area. To face this challenge with maximum agility, identify which technical decisions are crucial to make up front and which decisions can be deferred until more information is available.

Your migration might also differ from new construction in that design and engineering will be more distributed across multiple parties. In these cases, you'll probably need more input as you go along from the various people involved, including:

- + The manufacturers of your servers and systems.
- + The solution owner, who will guide the device naming and configuration.
- + The integrator, who will specify the wall field layouts.
- + The consultant, who will track details such as technical installation requirements.

For best results, take time to spell out each of these roles up front and the design and engineering impacts of each party's involvement.

3. Determine sequencing and scheduling

With your procurement, data, and engineering and design strategy in hand, you can start plotting out the sequence of phases your migration will follow. Later this will evolve into a more granular project plan, but for now, focus on any known interdependencies and start putting the major activities in a logical order.

One of the most challenging parts of planning a migration is knowing where to start. Because every migration is different, with varying parameters, expectations, and risks, your most logical starting point often isn't apparent.

When phasing and sequencing your migration, ask the following questions to help determine the best place to focus first:

+ **Where are you most vulnerable?**

Do any facilities or technology types present particularly high vulnerabilities? These can include cybersecurity risks, system unreliability, or lack of regulatory compliance. In many cases, these vulnerabilities are the key reason you're migrating in the first place, so consider making them your opening target.

For example, if you're compelled to migrate because a security survey found that your legacy card readers are outdated and easy to exploit, you might start by upgrading these first—then back up and perform the necessary control hardware upgrades for cutting over to the new head end.

+ **What's falling apart?**

Are any systems or equipment at or near end of life, in danger of not being supported, significantly disrupting user experience, and/or costing too much money and time to administer and maintain? If so, prioritize accordingly. When legacy platforms fail often and no longer have manufacturer support, your support staff is burdened with maintaining them when their time can be better spent elsewhere.

+ **What are your pilot opportunities?**

Is there a suitable and/or representative portion of the migration, like a specific facility or area within a facility, that makes sense as a place to test cutting over to the new or updated solution? Look especially for pilot projects that will test your key migration assumptions and approaches, including the ones you've identified in your other migration activities. Pilot projects are a great way to "fail fast" and learn as you go without causing much detriment to the overall migration.



+ What are your business continuity drivers?

Are there facilities or areas with particularly complex or sensitive business functions or mission critical operations? Are there areas with blackout dates for work execution? Depending on the urgency of these business factors and which migration activities directly affect them, you can choose these activities as a starting point or sequence them later at specific times.

Be intentional and realistic with all sequenced steps. The time duration estimates you put in your schedule should address time spent on all aspects of the migration project. For example, don't forget to leave time for project management activities, such as work breakdown structures, meetings and meeting minutes, status reporting and aggregation, issue management, quality/cost control, and project data visualization.



Real-world scenario: Tactical migration

In lieu of assisting with an end-to-end systems migration, ZBeta often engages with clients for select activities at specific stages of a migration effort. These partial projects vary based on the client's budget, most critical needs, and readiness to implement their roadmap.

In one recent example, we helped a prominent cancer research center migrate off of an end-of-life access control system and onto a unified platform that was already serving as a campus video management solution. The incremental construction and modification of the institute's buildings, over many decades and by many contractors, had introduced multiple risk factors. But by far the most impactful current state conditions were the legacy system's unreliability and lack of support. Gaining a thorough understanding of these factors helped us work with the client to prioritize a critical path through a larger migration effort as budget and resources allowed.

Risks:

- + Fixed budgetary allowances left very little room for unexpected conditions and changes.
- + Business operations spelled out minimal tolerances for downtime, a factor that was complicated by existing equipment centers with limited space for new components.
- + A wide variety and vintages of current state conditions added complexity for commissioning certainty and work acceptance.

Mitigations:

- + Developed a thorough and tightly defined scope that clarified migration processes, communication, and priorities, helping to ensure that onsite integrator resources were utilized effectively.
- + Used cutover strategies that allowed legacy head-end equipment to continue operation simultaneously while new equipment was installed and brought online.
- + Established pre-testing for each area, with both client operators and the integrator, ensuring same-page understanding of all pre-migration conditions.

4. Procurement strategy

One key migration decision is the method by which you will choose the integrator to implement your migrated security solution. This vendor might end up being someone you've worked with before, they might be someone you or your security consultant knows of by reputation, or they might be someone you find through a request for proposal (RFP) process. If you go with an RFP—at least for private organizations not beholden to public sector procurement guidelines—now is the time to start a list of qualifications you'll require in order for them to be invited into the RFP process.

Don't try to make the incumbent vs. RFP decision too fast—if you have leeway in your procurement strategy, it's wise to leave your options open at first while you consider all the angles. You might assume, for example, that you'll work with the same integrator who's done all your work before, but there could be good reasons for looking beyond that. Beating their price is an obvious motivation, but also some integrators might also bring advantages even if their cost is somewhat higher.

Keep an open mind, and be frank with yourself and your incumbent integrator about how well they match up to your migration needs. Many integrators specialize in repair, maintenance, and related services, but lack the breadth of experience to tackle a whole migration. Realistically, can your incumbent integrator mobilize in the ways that you need for this project, in all of your markets? Objectivity is also crucial. Is your usual integrator willing and able to gather more data from site surveys versus proceeding with their current (possibly incomplete) understanding of your environment?



Before deciding on a procurement approach, consider a range of factors:

- + Are you migrating across multiple sites? If so, should you choose a national integrator with teams in all locations, or should you engage a separate regional integrator for each facility?
- + Based on the systems you've selected to implement in your roadmap, does your security consultant know an integrator who's familiar with those manufacturers' products?
- + If you're inclined to hire a particular integrator without shopping around, do you have the legacy documentation needed for them to produce a realistic bid? Does their institutional knowledge trump the price advantages of competitive bidding?

This last point is especially important, and it's the main reason you're examining this choice before launching into additional planning. Migration projects can go downhill fast when an integrator submits a bid based on incomplete information. In fact, it's often safest to choose the RFP route because based on the data you gather, you can be as precise and rigorous as needed in the RFP questions you submit.

Any bids you receive for your migration, whether from a single integrator or many integrators via RFP, will be most reliable when they take a maximum of project data into account, including as-built drawings of your environment, markup on the as-builts for subsequent changes, and a site survey of each facility that covers the gaps between the marked-up drawings and reality.



Beware of “bidding the holes”

Sanity-check all migration bids, especially if they seem too good to be true. Often when a bid you receive from an integrator or other vendor seems tantalizingly low, the reason is that it's based on an overly optimistic set of assumptions.

In the best cases, this leads to a handful of change orders as the integrator ends up doing extra (unscoped) work based on discovering partway into the project that their assumptions were incorrect. In the worst cases, these change orders pile up to the extent that the integrator can't complete the project due to understaffing or a similar lack of readiness, and you're stuck starting over and going back to collect more bids.

This risk can come about when the integrator sees the lack of detailed data and knowingly “bids the holes”—that is, bids a threadbare amount based on the scant documentation you've provided, knowing they can rack up the change orders later and make more money off the deal. But integrators can also bid the holes innocently enough by wrongly assuming the information you provided was complete.

Either way, data is your best friend for getting to accurate bids, and diligence wins the day. Work with your security consultant to confirm the full scope of work needed, and push to document your existing security environment in all the ways needed for integrators to understand the challenges your project might face.

5. Cutting over

“Cutting over” refers to the migration phase when the new, integrated security solution gradually goes live and takes over operational control from the legacy systems. Once cutover is complete, your organization stops relying on the old systems and begins using the new one for day-to-day security operations.

It’s much more than just flipping a switch; cutting over actually comprises dozens or hundreds of cutover instances—this camera, that door, the first operations console and then the next one, and so on. The cutover process typically includes not only reconfiguring hardware and software but also migrating data, testing functionality in the new or updated system, and retraining personnel.

When you cut over to your migrated solution, whether in phases or all at once, you face a number of important risks:

- + Unplanned system downtime if things go wrong.
- + Loss of access control or credentials data.
- + Incomplete integration due to dissimilar device configurations.
- + Gaps in compliance and real-time monitoring.

To mitigate these risks, work with your security consultant to produce a cutover plan that contains:

- + Clear procedural steps to follow.
- + Timelines for all cutover activities.
- + Fallback protocols including decision authority and pre-defined fallback conditions.
- + Names and contact data for responsible parties.
- + Checklists for pre- and post-cutover tasks to be completed.

Cutover requires you to monitor all systems, old and new, throughout the transition, while maintaining user credentials and communicating the cutover to users when the migrated systems fully come online. As you create your cutover plan with the help of your security consultant, keep in mind any opportunities for data hygiene as well—establishing uniformity and consistency of your configuration settings on card readers, cameras, and other devices to meet the standards of the new solution.





ZBeta is a world class physical security design and managed services firm that provides services to some of the most dynamic, high-profile organizations and individuals in the world. We leverage a data-driven, technology-led, human-centered approach in order to help our clients architect and engineer superior physical security solutions, implement them seamlessly, and operate them at peak efficiency. Whether designing a new corporate campus, a futureproof technology roadmap or augmenting a client's internal team, we operate at scale, move at the speed of today's projects, represent your program as you would, and assure delivery where others cannot.

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

