

Big picture: Building a technology roadmap

Unpacking your end-to-end physical security strategy in 4 key phases

Getting to systems migration, step by step

As we discussed in our [recent white paper](#), technology roadmaps are a critical tool for defining the future of physical security at any company. Whether straightforward or multi-layered, your security team's roadmap is your strategic plan for matching short- and long-term security goals with qualified technology solutions that use systems, processes, and training to protect your organization from intentional harm.

It's never one-size-fits-all, but there's a general cadence companies can follow with the help of a trusted security partner to make sure they've asked the right questions and covered all their bases in the right order. The ZBeta presentation on this topic at last year's GSX Conference received overwhelming positive response, so we decided to update and expand on that discussion here.

Follow the guidance and pointers in these four phases to ensure your roadmap success.



1. Assess your current state

Before you decide where you're going, you need to figure out where you are. At ZBeta, we spend as much focused time as needed with clients to produce a current state assessment because it shows you a clear picture of what's functioning smoothly and where gaps lie.

+ Understand current functions and capabilities.

Start by brainstorming a full list of how your security program currently functions, both digitally and operationally, including all current state data requests. With your security partner, interview stakeholders, evaluate program data and documentation, and as needed conduct onsite observations of your business and security operations. Look closely at program/team structure and operational models, risk and regulatory compliance drivers, real estate and facility growth plans, and the existing state of your physical security systems and architectures.

It might feel like overkill, but capturing these factors is an important step toward assessing the maturity of your existing security program overall. It also helps uncover potential weaknesses, highlight strengths, and offer additional insights into areas ripe for improvement. Is your team trained to get the most out of present and future technology investments? Are there existing technologies that you aren't using to its full potential? Are you inefficient in ways that expose your organization to risk?

+ Summarize and report on critical findings.

As you account for the systems and capabilities in your existing security program, look for common themes. What circumstances make your specific needs for a new or updated system stand out? What's working, what doesn't work—again, both operationally and at the system level—and where are the key opportunities for improvement? Early consensus by your project team on key findings helps immensely later on in your project for managing risk, conflict, and change throughout the roadmap process.

Work with your security partner to document all findings from this phase. At ZBeta, this report includes sections on your current security program governance, solution operation and management, technical security environment, and program and solution capabilities. Together with the key findings, these details all become essential inputs to forming your technology roadmap's "true north" direction.

When done thoroughly and professionally, this report also helps answer some fundamental questions like: Who are we as a security organization? What value do we bring to our company's core business? Are our people equipped, trained, and aligned appropriately to best deliver this value? And for the roadmap specifically: How do our people use technology to deliver this value today, and what opportunities can we find to do it better? Knowing these answers at this early phase helps your roadmap team move forward as a unified front.



2. Envision the future state

Once you've assessed your current state, it's time to shift your focus to how you want your security environment to look, feel, and operate in the future. Examine your needs from various angles with the help of your security consultant and the rest of your team so you can build a solid list of requirements for any new or updated system and perform the due diligence needed to select the platform and provider. By the end of this phase, your roadmap options will truly come into view.



+ Confirm business objectives.

Successful roadmapping depends on having the visibility into your company's business that comes from collaborating with other business units throughout your roadmap project. Objectives precede requirements—they form the "why" so you can determine the "how." Ask: What do you hope to achieve with your new technologies? Are you looking to improve incident response times, reduce theft, or streamline access control processes? Clearly defining these items beforehand ensures that the technologies you select align with your overall goals and those of your executive team.

+ Identify functional and technical requirements.

Gathering requirements for your security roadmap entails asking two kinds of questions: What functional capabilities do you need for the new system, and what technologies are required in order to meet your goals? Again, build requirements based on these answers.

Depth of requirements will vary by project, but in general, the more detailed you can be at this point, the better. For example, instead of simply stating that you need a video surveillance system, you can fully define what you need it to accomplish—real-time alerts, integration with access control, or high-resolution imagery to be used in investigations.

+ Prioritize all requirements and identify differentiating criteria.

Before you take your list of requirements into a research phase and start examining potential products for your new security solution, it's important to identify which priorities matter the most, and which ones are less important or just "nice to have." Conduct the technical research necessary for figuring out these "must-have" criteria that will differentiate your solution. And don't think in terms of brands or providers just yet—push yourself to focus on the requirements themselves, and which ones are essential for the solution you ultimately select.

Remember, every manufacturer's product you research will have merit—just not necessarily merit for you. To avoid getting drawn in by impressive capabilities that don't necessarily map to the use cases for your solution, work with your team and security partner to categorize each requirement as low, medium, or high priority so you can refer back to this list later. Reminding the team you've achieved consensus on these priorities will help keep future research and evaluation discussions more focused.

3. Evaluate solution options

Now you're ready to start looking at solutions. Think of this critical step as your chance to build the short list of options for your roadmap's execution. Work with an experienced partner to target likely candidates, and then put each option to the test for your environment and your needs.

+ Research and evaluate likely solutions.

Work with your partner to identify the most likely solution and architecture options that will meet your differentiated, must-have criteria. For each product you consider, ask: Does it deliver the features and functionality we want, and can we prove it can do this in a live environment? Can it deliver at the scale we need, with an acceptable level of demand on our operational resources (people, processes, and budgets)? Do the capabilities we need come as part of the native product, or do they require professional services in order to customize them for our requirements?

As a best practice in more complex use cases, develop multiple roadmap scenarios so you can compare the options you preliminarily deem viable. For example, you might compare two scenarios side-by-side where you rely partly on repurposing some of your current investments versus building out a net-new “rip and replace” solution.

+ Estimate and compare costs.

In the previous step, you rigorously checked the functional viability of your roadmap options. Next, you need to put estimated pricing on each option so you can determine the most cost effective way forward. Work with your security partner, other members of the roadmap team, and the manufacturers you're considering to price out the estimated costs of building each solution.

Here's your chance to spot any hidden costs, including unwelcome operational burdens for solutions that require a lot of hands-on maintenance, or new systems that require an upgrade in your physical or network infrastructure for implementation. Examine costs from every angle, using input from the whole roadmap team, until you're sure you have the best approximate price tag for each proposed solution. This doesn't mean you'll choose the cheapest one—it just means you've done the work to assess and communicate the cost of executing your roadmap long-term.



+ Make your final system selection.

Based on all the information you've gathered, plus guidance and recommendations from your security partner, you're ready to narrow your short list of system options down to a final selection. Keep in mind that the “new solution” you choose might not be completely new—your ultimate choice might be to repurpose and augment your existing security technology assets and investments. Whatever the case, use this step to affirm your best choice among the options you've identified.

If two or more solutions seem equally compelling, conduct further investigation to help understand their comparative advantages, such as submitting a request for qualifications (RFQ, also called a request for information or RFI) to the manufacturer with specific questions about what they can provide. RFQs are the process by which you literally qualify a manufacturer, saying: “Put it in writing; tell us specifically how and to what degree you can meet these requirements.” You can also test whether each manufacturer's features will perform in your environment by running a proof of concept (POC) at the ZBeta Innovation Lab or other lab facility. Investing time in a POC now can save a world of headaches down the road.

4. Get budget and buy-in

And... the rubber meets the road! Well, almost. This roadmapping phase connects all of your hard work, research, consensus building, and investigations to the systems migration effort you'll ultimately undertake. It started with selecting your technology, and now it means planning carefully based on that selection to ensure the path forward proceeds smoothly and your roadmap project ends in success.

To do this, you need to prepare for the questions and challenges you'll face getting budget and buy-in for your migration effort. Work with your security partner—who has probably seen many projects like the one you're proposing—to anticipate these challenges and help line up the necessary support you'll need to feel accurate with your estimates and make a convincing case. A complete reporting by the end of this phase will include a credible range of cost for the solution you've chosen, together with a time frame for implementation, with priorities and dependencies built in.

+ Prioritize sites and systems for migration.

Work backwards through your proposed implementation and identify the areas where crucial work is needed to enable it. Prioritize the work that needs to start first, clear any critical paths for the people you'll assign tasks, and make sure any adjacent technologies or other project factors on which the work depends will be ready to integrate as part of the migration.

+ Build a strategy for scoping, engineering, and gathering data.

The team that implements the migration will rely on accurate as-built, as-configured documentation of your environment. Your current VAR might have this, but often many of the salient details exist only in their memory. It's too soon to decide whether that VAR will be doing the migration work, so plan ahead to get this data via a site survey as needed. Having the data will enable scope and engineering estimates that are known, realistic, and easier to support.

+ Identify project risks and plan how to mitigate them.

Your security partner can also advise you at this stage on unique risks facing your migration, including tricky ones you might not have thought to account for. Risks without mitigation plans beget uncertainty, which in turn threatens forward motion, so having the right details in advance helps make you bulletproof to the scrutiny your migration budget request might arouse. Meanwhile, make the usual plans for mitigating project risk as you'd normally do at your business, and ensure that your team is trained and the migrated technology blends into your daily operations.



You're ready to go

Developing a comprehensive physical security technology roadmap is an exciting challenge, worthy of careful and comprehensive effort. Your company can achieve roadmap success through the four phases outlined here, along with collaboration, thoughtful planning, and a clear-eyed determination to align with your company's core business and physical security needs.

Planning your roadmap with the help of a security consultant and members of your larger roadmap project team puts you in the starting blocks for a highly successful deployment. In our next white paper and its related articles, we'll talk you through system migration deployment steps and considerations in further detail.



Read our white paper [Plotting a sustainable technology roadmap: Picturing and achieving the future state of your physical security solution](#) to learn about our methodology and best practices at ZBeta for developing your company's physical security technology roadmap from strategy to solution.

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

