BLACKDUCK®

The CISO's First 100 Days

Key considerations for success

Introduction

As a new CISO, you're embarking on a dynamic and challenging role, one that will flood you with demands and responsibilities. As you begin this journey, nothing is more important than how you perform in your first 100 days. You have the opportunity to demonstrate your ability to get the job done. Failure to bring meaningful and impactful results, quickly, can easily be seen as failure or an inability to rise to the occasion. In order to thrive in your first 100 days, it's critical that you formulate a clear and concise plan for your organization, and then communicate and deliver on that plan. In this eBook, we offer key considerations and actionable steps you can take to build a strategic 100-day plan and come away with clearly defined goals and priorities in place.

Starting your journey: Consider three key goals

Before we dive into the specifics of your 100-day plan, you should consider your journey through the lens of these three key goals.

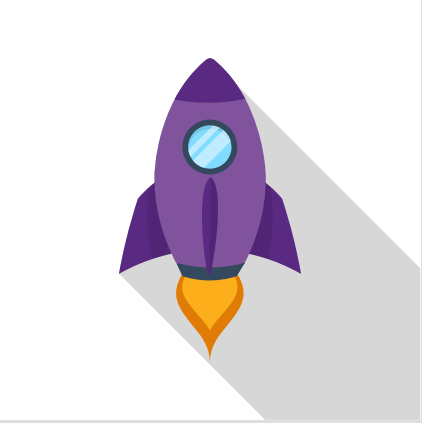
THREE KEY GOALS

Establish relationships with key stakeholders

It's critically important for the CISO to become acquainted with everyone on the team, understand their pain points and concerns, and develop a working knowledge of team dynamics and responsibilities. Even more important is developing relationships with the board of directors in order to facilitate top-down support. Fostering this relationship early on will be a key enabler for your 100-day plan's success.

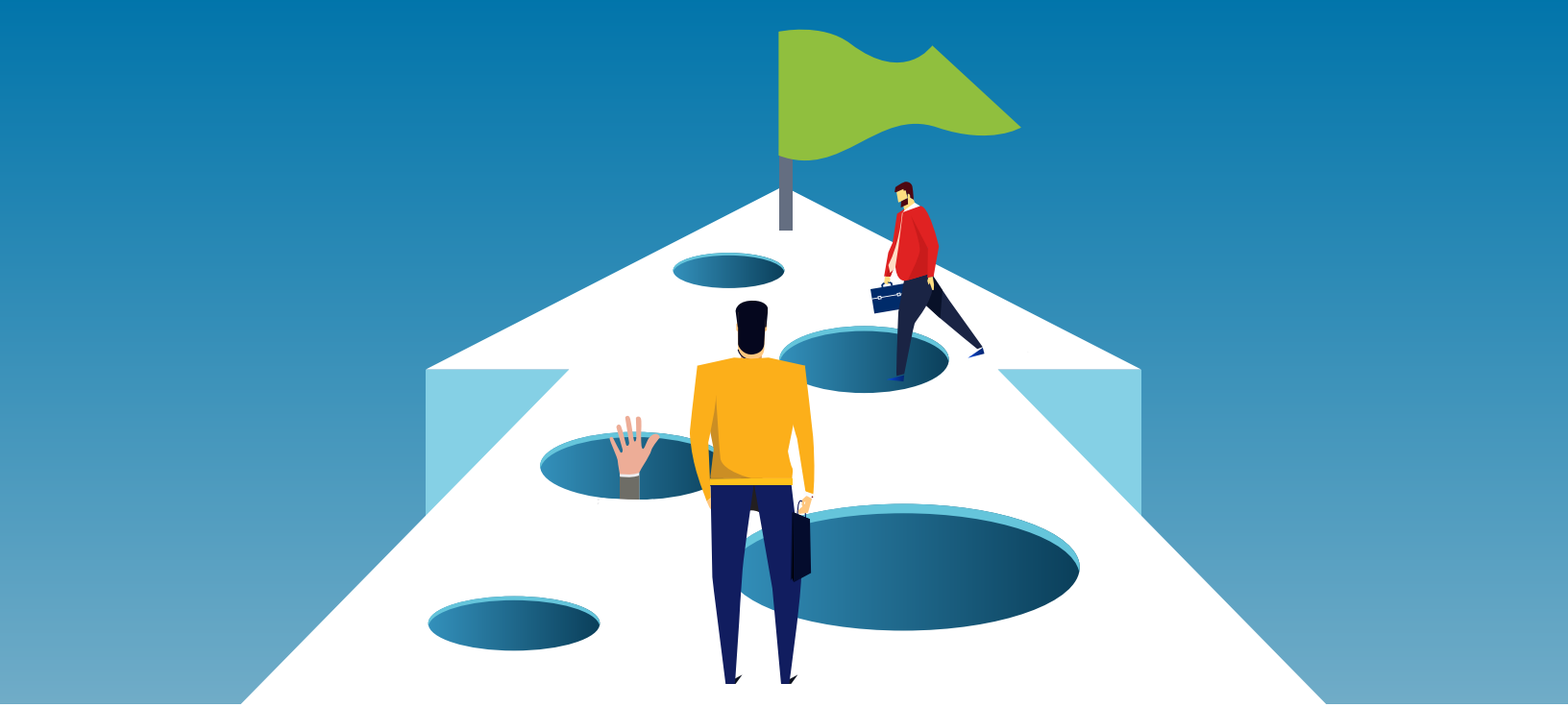
Communicate the plan

Once you have your 100-day plan in place, you need to communicate it and ensure that everyone has seen and understands it. By providing precise direction and defining the goals around your plan, you'll get everyone on the same page and clear on the expectations you have of them. It also ensures that roles, responsibilities, and expectations will be understood and more easily met.



Take action

Nothing would be worse than developing a plan and failing to provide tangible results. In order to create an effective plan, you should start by measuring your current software security program and comparing it with industry peers. You can use this reference as a justification for budgeting and resource needs. You should select feasible and manageable projects that you can accomplish within your first 100 days. Beyond the first 100 days, you should also have goals in place for your first year; showing measurable and tangible results is the surest way to prove your impact and success to your organization.



Common pitfalls: Things to avoid

Getting caught up in expectation vs. reality. Often, when a new CISO takes on the role, the reality of the organization's innerworkings may be disappointing or vary greatly from the details communicated in the interview process. It's important not to get caught up in rationalizing these differences. Focus on the reality of what is, not what you thought it would be. Time spent lamenting or discussing unmet expectations detracts from the time you can spend on meaningful work.

Playing the blame game. It's easy to come into a new role and blame shortcomings or challenges you're facing on your predecessor. By blaming past actions and decisions, you set a negative tone for the organization, and inevitably foster feelings of resentment or distrust among those who played key roles in the very practices you're ridiculing. It's great to analyze older ways of doing things and provide structured direction and action for improvement, but refrain from placing blame. Focus on the future, not the past.

Trying to do too much, too soon. Perhaps one of the easiest pitfalls is trying to do too much. In your first 100 days, you should focus on identifying and accomplishing feasible tasks. It's far better to accomplish smaller tasks successfully than attempt and fail to accomplish tasks that are too involved or too complex for your first 100 days. Small successes are always favorable to large failures.

Your action plan: The 100-day cheat sheet

Now let's get into the specifics. This five-phase approach will help you create your 100-day plan and ensure you're taking impactful action.

Five-phase overview

1. **Research.** The more background information and details you have about your position and the organization as a whole, the better off you'll be when formulating your plan. You should start this research even before you begin the role. The more insight you have, the more proactive you can be.
2. **Process and understand.** Collect an inventory of your organization's security practices, its systems, and its overall security footprint. Are there gaps in security? Areas that need immediate attention? Ensure that you have a full understanding of the current state of your organization, so you can begin your planning with the maximum level of intelligence. This phase should involve and in-depth measurement and analysis of your existing software security program. Comparisons and market analysis and research can be particularly helpful toward this end.
3. **Prioritize.** You should begin formulating a draft of your plan, including all the data and information you gathered. Any actions needed to support this plan should be undertaken early—for example, hire additional resources or team members prior to starting your plan.
4. **Get to work.** Now that you're armed with an informed plan and all the resources you need, it's time to get to work. As noted earlier, nothing is more important than your ability to deliver visible and tangible results as soon as possible.
5. **Report.** It's critical that you clearly communicate your successes and progress to key stakeholders. Don't assume they know what you accomplished. Regular reporting with evidence and data is key. This is an opportunity to underline challenges you're facing and wins you delivered.

Five-phase details

Phase	Key activities
 **Research** Days 0–15	• Analyze relevant reports, shared spaces, support systems, tools, solutions • Schedule key stakeholder meetings • Perform team outreach and introductions
 **Process and Understand** Days 0–45	• Collect information and data regarding the maturity and state of the security program • Develop a working knowledge of which activities and practices are working, and which are not • Understand immediate needs and long-term requirements • Identify business needs and priorities
 **Prioritize** Days 15–60	• Identify your goals for the first 100 days, and the first year • Calculate budgets and resource needs • Prioritize several quick wins you can tackle easily
 **Get to work** Days 30–80	• Get stakeholder buy-in and approval of your plan • Communicate your plan to all key players, ensuring roles and responsibilities are clearly understood • Deliver education and training, as needed • Tackle your quick wins
 **Report** Days 45–100	• Provide evidence of your early progress to key stakeholders • Provide data that demonstrates your success—process improvement metrics that are irrefutable • Determine and deliver a success report cadence; we recommend monthly executive reporting on your wins • Provide a progress report on your longer-term projects

Conclusion

The first 100 days of your role as CISO can make or break you. Alignment, communication, and action are all vital to your success. While you cannot possibly tackle all organizational challenges and issues in your first 100 days, you should be well on your way to providing meaningful change and progress. We hope that our suggestions will help get you on your way to developing your own plan. Choosing to take meaningful and measured action will set you up for success as you take on this challenging new role. Go to our Building Security in Maturity Model (BSIMM) webpage to help you succeed on your 100-day journey.

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.