The Chief Information Security Officer's First 100 Days

How you perform in the first 100 days in the role is critical to your success or failure as a chief information security officer. Gartner provides target outcomes, advice and supporting resources to help you maximize your success during this pivotal transition phase.

Key Findings

■ Most chief information security officers (CISOs) who fail do so because they do not understand or meet business requirements and expectations, or they don’t effectively communicate how they have met the expectations.

■ The successful CISO is primarily a leader, a manager and a communicator, not a technologist.

■ A CISO’s success will depend on two complementary achievements: (1) establishing a foundational personal brand of credibility and leadership; and (2) laying the foundation for a sound security program.

■ New CISOs who approach the role with a strong plan for the first 100 days are likely to enjoy success in the role.

Recommendations

■ Maximize your chances of success by creating detailed plans for activities through your first few months in the role.

■ Set your priorities carefully, and avoid overcommitting. Identify the five most pressing issues that you have to deal with, and then select two of these that you will focus on during your first three months.
Stay as far away from technical details as possible, and focus on the relationship of security to the business.

Assume some inevitable portion of your time will be spent handling unpredictable security events.

Avoid criticizing the actions and strategies of your predecessor in front of your team or your stakeholders.

Table of Contents

Introduction ............................................................................................................................................ 3
The First 100 Days................................................................................................................................. 5
Prepare Phase (Days -10 to 15)............................................................................................................ 5
  Target Outcomes for the Prepare Phase.......................................................................................... 5
  Actions for the Prepare Phase........................................................................................................ 5
  Communicating in the Prepare Phase............................................................................................ 6
  Resources for the Prepare Phase.................................................................................................... 7
Assess Phase (Days 0 to 30)............................................................................................................ 8
  Target Outcomes for the Assess Phase........................................................................................ 8
  Actions for the Assess Phase........................................................................................................ 8
  Communicating in the Assess Phase........................................................................................... 10
  Resources for the Assess Phase.................................................................................................. 11
Plan Phase (Days 15 to 45)............................................................................................................. 12
  Target Outcomes for the Plan Phase.......................................................................................... 12
  Actions for the Plan Phase......................................................................................................... 12
  Communicating in the Plan Phase............................................................................................. 13
  Resources for the Plan Phase.................................................................................................... 13
Act Phase (Days 30 to 80).............................................................................................................. 14
  Target Outcomes for the Act Phase.......................................................................................... 14
  Actions for the Act Phase......................................................................................................... 14
  Communicating in the Act Phase.............................................................................................. 15
  Resources for the Act Phase..................................................................................................... 16
Measure Phase (Days 45 to 100).................................................................................................... 17
  Target Outcomes for the Measure Phase.................................................................................. 17
  Actions for the Measure Phase................................................................................................ 17
  Communicating in the Measure Phase...................................................................................... 18
  Resources for the Measure Phase............................................................................................ 18
Introduction

The first 100 days constitute an expected "honeymoon" or transition period. This all-too-brief period is yours to formulate a course of action, make connections, and establish and communicate a personal management style. It is within this critical period that you establish yourself and create the basic perceptions that others will, for better or worse, associate with your subsequent plans and actions.

Proper preparation, assessment, planning, acting, measuring and, above all, communicating can greatly enhance your chances of success. This research highlights the key activities that focus on critical issues, and provides actions and resources to help you achieve your intended outcomes. Gartner also offers a unique companion experience in Peer Connect, Gartner’s online community. Use our dedicated forum to connect with fellow security leaders to discuss common challenges and gain practical insight and support for success in your role.

We break down your first 100 days into six phases, each overlapping with suggested durations that you can customize. Each phase includes critical target outcomes, actions and resources, as well as some optional ideas to consider as time and resources allow. The communicate phase spans the full duration, and we include specific actions for effective communication for each phase.

Figure 1 provides a handy road map to help you identify key milestones as you transition into your new leadership role.
In brief, a successful agenda for the first 100 days should:

- Begin prior to the new leader's arrival.
- Focus on a subset of priority issues, and drive actions that deliver near-term improvements.
- Bridge the delivery of business value and internal security operational excellence.
- Forge solid relationships with all key stakeholders (customers, IT and business leadership, security employees, suppliers and partners).
- Establish a current-state baseline that becomes a foundation for continuous improvement.
- Encompass management disciplines of people, process, technology and business.
- Communicate the CISO’s compelling future vision.
- Highlight future opportunities while encouraging everyone to learn from past mistakes.
- Define and communicate realistic and measurable, time-bound goals, and establish tracking systems to check when the goals are achieved.
- Provide the new CISO credibility, and elevate the image of the security organization.
The First 100 Days

Prepare Phase (Days -10 to 15)

Don't wait until your first day on the job to prepare. Take some key actions before your start date to inform yourself, learn about your colleagues and staff, and draft communications to make a great impression on Day 1.

Target Outcomes for the Prepare Phase

- A common agreement and understanding of your role, and the expectations of you, among yourself, your management, senior stakeholders and new staff
- The foundations for developing meaningful relationships with your new staff and stakeholders
- An initial understanding among your staff, management and some other stakeholders of your management philosophy and approach

Actions for the Prepare Phase

Don't make the mistake of approaching your new role with ad hoc communications and plans. A few hours of investment in planning before you start your new job will ensure critical preparations are completed.

Actions Before Day 1

To help maximize the value of the first week, complete the preparation phase by taking the following actions in the week or two before your arrival.

Reinforce new connections: Send thank-you notes to interview participants to build relationships and set a positive tone for your next interaction. Set up lunches with a few key people. These actions will show that you are a people person too, in addition to being an exceptional technology leader.

Set logistics: Connect with HR representatives and your future administrative support to resolve any logistics that can be completed in advance, including a meet and greet on your first day. This will drive the point home that you want to be active and productive from Day 1 and will expect the same from others too.

Understand your organization's structure: Request organization charts and other basic materials to understand the structure of your new team's position and key leadership roles across the organization. Request overall organization material and specifics for IT and security.

List key stakeholders: Compile an initial list of key stakeholders to meet the first week.
Communicating in the Prepare Phase

Communications Before Day 1

Assess your communication skills: Resolve, in all communications, to follow these best practices for effective communication:

- Use business language wherever possible. Avoid detailed technical terms, and clearly define any specialist terms, such as IT abbreviations and acronyms.
- Be brief, clear and consistent in your message across forums and audiences.
- Avoid generic statements — for example, "Security is a critical input to the business." Focus on only what is specific to your organization’s performance.
- Connect plans explicitly to the strategic investment objectives of the enterprise, thus demonstrating that the security organization is synchronized with the business.
- Socialize your plans to peers and business leaders across the organization, and actively solicit feedback.

Write an introduction: Prepare introductory communication material about yourself, your background, and your initial thoughts on joining the organization. Make this content as fact-based and neutral as possible, and keep it short and succinct. For example, try a 100-word short bio, along with some personal information about your key priorities in life and work, your value systems, and your integrity.

Draft discussion guides:

- **Stakeholder discussions**: Prepare a list of no more than five questions (some specific, others open-ended) that will ensure the early stakeholder conversations yield insights beyond the polite meet and greets. For example, while meeting key business stakeholders, ask them about their perception and satisfaction levels on the current state of the security program and organization, any urgent issues that must be resolved as quickly as possible according to them, any chronic pain areas, priorities, and general expectations.

- **Staff discussions**: Prepare a list of similar questions for your first meeting with your staff. Ask them about their key work challenges and constraints, and their perception and satisfaction levels with their own team and organization.

Actions and Communications on Day 1

Since your first day on the job is all about listening and communicating, we’ve combined this phase’s actions and communications tasks.

Meet and greet: Call a meeting for everyone on your direct team in person, and through videoconferencing or audioconferencing for remote workers. This meeting has two objectives: (1) to introduce yourself; and (2) to show that you are approachable and available to everyone. Offer no
opinions of any kind. Explain that you are still gathering information and are not yet ready to make decisions or changes.

During the meet and greet:

- Deliver the introductory message you drafted in advance. State when you will report back to the team with updates on your progress.
- Let the people attending the meeting introduce themselves in their own way and ask whatever questions are on their mind.
- Remember some detail about each person that will help you start conversations later.
- Be mindful of any apparent biases — identify political/social issues that may remain from your predecessors.
- Be careful of coming on too strong and appearing as a threat or hurdle — first impressions are lasting ones.
- Understand your direct reports' concerns, priorities and their career aspirations. Which ones understand and can describe the bigger picture? Which ones seem siloed in their views? Where do they need immediate help?

**Distribute your introduction:** Distribute the introductory remarks to the wider IT organization. See if you can post it on the company intranet.

**Regroup with your manager:** Wrap up the prepare phase with a meeting with your manager that covers:

- From your point of view, key security challenges and opportunities
- Your preliminary strategic vision for security
- A communications schedule for the future between the two of you

**Resources for the Prepare Phase**

**Gartner Research and Tools**

Review these few key Gartner resources to get started:

- "Gartner for IT Leaders Overview: The Chief Information Security Officer" — Use this research to remind yourself of the role of a typical CISO.
- "IT Key Metrics Data 2014: Key IT Security Measures: by Industry" — Use this research to arm yourself with data about the current state of play in your industry.
- "Define the Structure and Scope for an Effective Information Security Program" — Use this document to confirm the basic elements of an effective information security program.
"Develop the Skills of the Contemporary CISO" — Study these valuable insights into the skills and capabilities required for your new role, and how to acquire them.

"Creating the Communications Core: The CIO’s Guide to Effective Communications" — Read this to learn about effective communication approaches for all IT leaders.

Other Suggested Resources

Company and industry websites — Develop an understanding of the fundamentals of your new employer’s industry. This insight will give you the first glimpse into the market pressures that will impact the security team.

Published financial reports — Utilize public financial and performance data, such as stock exchange filings, to gauge the recent trends with the company relative to the financial results.

Press releases and other news reports — Look beyond the financial data for other information on the company to understand how it is performing.

Professional networking and employee feedback sites — Find out what current and former employees think of the company.

Job sites — Assess how many other IT and non-IT positions are open in the company to get an early indication of whether the business is expanding or has high staff turnover in any areas.

Assess Phase (Days 0 to 30)

Use this period to gain a comprehensive insight into the current state of the security program in the organization.

Target Outcomes for the Assess Phase

- Solid insight into the current state of the security program
- Early indications of what’s working and what isn’t
- A list of the top five challenges that you will prioritize for the first three to six months

Actions for the Assess Phase

Inventory your resources: During your first week as CISO, try to spend most of your time creating an inventory of the resources you will need to manage the security organization: people, reports, available metrics and financial parameters. Review the existing security strategy, policies, standards and architecture. Compile as much information as possible, and take detailed notes, but do not try to identity and resolve issues. Pay attention to anything your predecessor may have done well.

Perform a high-level, current-state assessment: You now need to identify, at a macro level, which elements of the company’s security program are functioning at or near top performance, and which elements you must overhaul or replace. You can measure security in four ways:

- Technical accomplishments (the absence or existence of damaging security incidents)
Performance metrics tied to financial or satisfaction measurements

Assessment of the maturity of the current program

Responsiveness in relation to industry standards or benchmarks

Review recent vulnerability assessment and penetration test reports, and current audit findings. If there aren’t any recent vulnerability assessments, consider commissioning a quick assessment of the external-facing applications and infrastructure. Perform a quick maturity assessment of the current program.

Focus your assessments on several areas of your security mission:

- Governance (organization and budget)
- Delivery (are failures happening or not)
- Policies, procedures and standards
- Process maturity
- Technology effectiveness and planning
- Legal concerns and regulatory compliance
- User and executive awareness
- All current projects and initiatives
- The current operational and project budgets

Depending on your company’s or your industry’s maturity level, you may also want to add some other areas:

- Staff skills measurement and succession planning
- Audit relationship and response
- Research and development (Security R&D involves studying the security characteristics of various technologies and processes that typically are not yet in production.)
- Identification of collected metrics (Find out what information is available, where it is stored and how you can best use it. Make a list of metrics by name, find out their content and the frequency with which they are collected or reported, and try to determine their business value.)

**Establish the scope of your remit:** Once you’ve arrived in your new office, you need to confirm the scope of your remit. Have a discussion with your manager to agree on which security and risk management functions are included in your role. Do they include IT and information security? Physical security? Business continuity management? Privacy? Risk management? Compliance? For functions that are not included in your remit, find out where they fit into the organization, and who the respective managers are with whom you will have to establish working relationships. Also inquire about what happened before your appointment, identifying any possible hurdles or broken
relationships that are a legacy from the previous management. Be cognizant of what happened before to avoid making the same mistakes.

**Seek an executive mentor:** One of your most valuable assets as CISO will be a senior-level mentor. In your first two weeks, begin looking for someone you can talk to who has insight into the inner workings of the senior executive staff. Knowledge of the security field is not necessary. In fact, it would be best if your mentor had little knowledge of your specialty, so that you can gain a realistic, objective sense of how well others will receive your proposals and ideas.

**Identify five key issues:** These assessments will help you identify the top five issues that you need to address in the next three to six months. These are the issues that represent major obstacles or challenges to the existing program. They provide you with a golden opportunity to cement your presence. Examples include a lack of executive support for security, dysfunctional security governance structures, or pressing regulatory compliance gaps. Use the following decision criteria to determine the top five issues:

- Is the issue a major obstacle to establishing (or re-establishing) an effective information security program?
- Will dealing with the issue result in clear business benefits?
- Will dealing with the issue help lay the foundation for work you need to do in the next one to two years?
- Will dealing with the issue establish your credibility within the organization?

**Communicating in the Assess Phase**

Use the discussion guides you prepared before Day 1 to get started.

**Meet team leads:** Hold one-on-one meetings with your group or team leaders to gauge their opinions on the state of the security program. This is your opportunity to begin establishing areas of responsibility, to solicit informed opinions about urgent tasks and to determine how to approach them. Solicit input and support from your staff to make it clear that you understand you can’t achieve anything alone.

**Interview stakeholders:** Interview two or three key stakeholders (for example, the CIO, chief risk officer and data protection/privacy officer) to establish their opinions on the current security program and any changes they might propose.

**Engage key business leaders:** Meet with key business unit leaders and members of the security steering committee. These leaders will be among your most crucial allies. They need to know that you will put their business needs first as you develop and execute your plans. To be successful in balancing their demands, begin an open and cooperative relationship with them. Understand their key business objectives and their concerns with the information security function. Ask for their advice, and make a point of writing down their answers. They will probably have opinions about what security has done for them lately. Their views will give you a clear road map of how to respond to their needs.
Identify influencers: Identify which senior influencers you will be able to co-opt into your informal "virtual coalition" of allies. Such a coalition will be invaluable in reinforcing important messages to the executive audience in the near future. It will also help you avoid being a lone voice trying to initiate cultural change.

Refine expectations: If necessary, set up another meeting with your line manager to refine the expectations and the authority of your role.

Document findings: Document your findings in a succinct interim report, and share this with your line manager, security steering committee and key stakeholders.

Resources for the Assess Phase

Gartner Research and Tools

- "ITScore for Information Security" — Use Gartner’s self-assessment tool to gauge the maturity of the information security program you have inherited. You will likely need input from security staff and other IT leaders. You might need these tools, too:
  - "ITScore for Identity and Access Management"
  - "ITScore for Risk Management"
  - "ITScore for Compliance"
  - "ITScore for Business Continuity Management"
  - "ITScore for Privacy"
- "Toolkit: Applying the Gartner Risk Assessment Methodology to Critical Enterprise Assets" — Use this to help you assess the current risk situation of the organization's mission-critical assets.
- "Toolkit: Avoid Audit Headaches by Planning an Information Security Self-Audit" — Use this Toolkit to design a security audit as part of your current-state assessment.
- "The Security Processes You Must Get Right" — Read this to understand the bedrock processes that any security program must have in place.
- "How to Differentiate and Align the Roles of Security and Audit" — Use this to understand how the audit function can support your assessment and planning activities.

Other Suggested Resources

- The last two vulnerability assessment and/or penetration reports, and internal or external audit reports — Study these as long as they are still current.
- Existing information security documentation — Examine these sources, which include policies, principles, charters, standards, strategy plans, program plans and road maps.
Recent minutes from steering committee meetings — Use these to gain insight into executive issues and hot topics.

The current information security budget — Request material available on the actual to plan expense and capital spending activities. Seek any available forecast information, too.

Existing executive and operational reports — Study these to get additional insight into any challenges and opportunities inherent in the security program.

Plan Phase (Days 15 to 45)

The plan phase synthesizes the abundant assess phase information into the areas of focus, transforming all you’ve learned during your first weeks on the job into a blueprint for action.

Target Outcomes for the Plan Phase

- A draft of the security program vision
- A planned operational security budget for the next two to three months
- An interim program strategy for the first six to 12 months of your tenure, which identifies the two key issues that you will focus on over the next three months

Actions for the Plan Phase

Design/refine your new security organization: There is no such thing as a perfect universal organizational model for information security. Structure the security organization in a manner that reflects the maturity of the organization’s security and management practices, and in a way that is compatible with the organizational culture. Consider all alternatives for resourcing security operations functions, including selective outsourcing.

Plan your operational security budget for the next two to three months: You should now have a reasonably accurate picture of your monthly security operations budget. This budget may expand or contract as you develop your program, but you should be able to provide fairly specific answers to any questions about where the security money goes. You have an obligation to be open and honest in discussing these issues. Do not worry about any such discussions reflecting poorly on you, as you probably inherited the budget. However, be careful not to criticize your predecessor’s financial planning and operational methods too harshly.

Select two key issues to focus on: Examine the five key issues you defined in the assessment phase, and then identify two key issues that you will focus on over the next three months. This could be as simple as publishing the new charter and initiating a DLP project, or as complex as rearchitecting the enterprise-wide information security organizational model and re-insourcing the security monitoring and response capability.

Use the following criteria to select these two focus areas:

- Will you be able to achieve successful conclusion, or report substantial progress, within three months?
- Will you have the requisite executive support, resources and budget?
- Will successfully dealing with the issue have a meaningful impact on materially reducing the risk exposure of the enterprise?
- Is the risk of failure comparatively low?

Do not kill off existing projects at this stage, unless the current-state assessment highlights any critical issues with them. However, you might want to identify any existing projects that need reassessing for viability and relevance.

**Communicating in the Plan Phase**

**Draft and socialize a security program vision:** All information security programs and strategies require a clear, concise expression of the program vision to guide strategic decision making. Such a vision should derive from commonly accepted standards and best practices. A well-defined information security framework model acts as a strategic vision, a planning guide and a catalyst for executive communications. Draft and share this program vision with your team, line management and all relevant stakeholders, soliciting their input.

**Draft an interim program strategy:** In essence, this consists of pulling together much of the work you’ve done up to this point and collecting it in a single document:

- The program vision ("where we want to be")
- The security assessment ("where we currently are")
- A gap analysis between the current state and the vision, resulting in a list of current and new projects

**Resources for the Plan Phase**

**Gartner Research and Tools**

- "Security Management Strategy Planning Best Practices" — Adopt these best practices to establish a coherent strategy planning process for the security program.
- "Telkom SA Develops a Practical Information Security Framework" — This case study provides a concise, practical model that you can adapt to use as the basis for developing your security program vision.
- "Toolkit: Security Strategy Executive Briefing" — Use this Toolkit as the foundation for developing the executive presentation of your initial strategy.
- "Information Security Organization Dynamics" — Learn why your security organization must reflect the maturity of the security program that you inherited.
- "Tips and Guidelines for Sizing Your Security Organization" — Understand the factors that influence the team size team.
Other Suggested Resources

- **Existing IT strategy documents and budgets** — Study these to gain a good indication of the structure and format used for strategic planning in the enterprise.

- **Existing/old security strategy documents and budgets** — Use these sources to frame discussions with your new team and stakeholders to identify what worked well and what did not.

- **Existing enterprise architecture documentation** — Seek the planning principles and guidelines that can help you focus on business requirements during your planning process.

Act Phase (Days 30 to 80)

The act phase delivers visible results such as changes in the security program. Focus on the two key issues you identified as part of your interim program strategy, but also seek to address the other foundational areas discussed in this section.

Target Outcomes for the Act Phase

- A draft enterprise information security charter

- Publication of the interim program strategy, including the two key issues that you will focus on during the next two to four months

- Resolution of, or substantial progress with, the two high-priority issues that you’ve identified

- Initiation of the rest of the work required to establish your credibility and lay the foundations of the new security program (This includes your first security program budget.)

- Closer working relationships with the executive team

Actions for the Act Phase

**Refine your team:** This is your opportunity to recognize strengths, capitalize on motivational factors, implement a new team structure (if necessary) and allow each of your leaders to achieve the highest possible level of performance — with your guidance:

- Give your leaders their first assignment: to define the scope of their individual functions and develop performance metrics. Allow them to collaborate to develop and present to you a plan that covers all the areas for which you are responsible. If you believe you have leaders capable of providing support for other leaders, have all projects reviewed by a leader other than their primary manager as a quality assurance technique. Create a job description, a set of required skills (including accreditation or certification, where applicable) and a success measurement plan for any unfilled positions. Highlight that strong writing and presentation skills are key requirements for all managerial or team leaders.

- Identify underperforming personnel and develop skills. There are few factors more damaging to your mission — or more demotivating to the team — than allowing mediocre performance to continue. Poor performers usually are not underperforming deliberately. In most cases, they
simply need some help and direction to find their niches. How many times you find a star performer hiding inside a below-average employee will be a measure of your success. Develop skill improvement plans that will enable you to make effective use of the resources available to you.

**Get involved in existing projects:** You probably inherited several ongoing security projects. By this time, you have some understanding of how the security organization works, so you may be able to add some value to these projects that occupy your group’s time. Be careful you do not seem to be "taking over" a project team or undervaluing the team members’ skills. You should have only two objectives in this process: to keep the teams focused on the business value of their projects, and to prompt the team members, when necessary, to keep their execution crisp, smooth and effective. This may, of course, mean that you have to act as a "referee" at times. When this becomes necessary, try to lead the individuals or the group to a collaborative solution that does not leave anyone feeling that there is a "winner" or a "loser."

**Obtain approval for your security charter:** Ensure senior-management commitment for the security charter you developed. Schedule time for face-to-face meetings with executives. It is essential that you confirm what senior management expects from you. Discussing the highly focused security charter also presents you with an opportunity to begin establishing a close working relationship with the executive team. This should be another key goal for this period.

**Set budgets:**

- Take another look at your operational budget for the next six months, and highlight anything that has changed from the first review. Note any trends that you can identify, and look for items that seem to stand out as your top expense categories. These categories often present the most productive opportunities for financial savings. Develop a plan for cost reduction.

- Work through your funding plan for the first iteration of your security program. This is the initial budget required for the transformational work. It is over and above the current operational budget (although some existing project funding should be transferred to this budget, as appropriate).

**Establish (or re-establish) the security governance processes and forums:** Evaluate the effectiveness of any security governance processes and forums, using the assessment performed earlier as a starting point. Effective governance entails much more than assurance reporting and budgeting. It is primarily about instituting effective decision-making rights, linked to accountability, responsibility and authority.

**Communicating in the Act Phase**

**Draft (or review) and socialize an enterprise information security charter:** A security charter will provide the executive mandate for your information security program and establish formal accountabilities. The goal is to write a charter that can remain in place for many years. Use clear, simple language — avoiding technical jargon or "buzzwords" — and present a security strategy that is beyond challenge. Avoid discussions of specific technology or industry trends. Security charters
typically include straightforward, actionable phrases, such as "protect personal customer information," "provide reliable communications" and "maintain accuracy."

Future policies and procedures will use this document as both a foundation and justification for further definitions. The audience for the security charter includes all company employees, and may also include business partners, customers, independent contractors, customers, auditors or other stakeholders. The document will require CEO-level, and preferably board-level, approval. Share the draft charter with your line management and all relevant stakeholders, soliciting appropriate input.

**Meet teams to identify objectives:** Ask your operational teams to review their scope of operations and to consider their performance metrics. The teams' objectives should be clear and their scope well-defined. Ask what you can do to help them be successful, and follow through. Work with them to find a practical alternative if their expectations are unrealistic.

**Schedule and conduct monthly security team updates:** This will help you to develop consistent ways to measure the success of your teams. A standard update report from each team leader gives everyone the opportunity to understand what their colleagues are doing and pass that information to their direct reports. If you give your team the opportunity to report on their successes in front of their peers, it develops their confidence. Use good meeting management techniques.

**Conduct a senior management status meeting, and develop a quarterly schedule:** These will be some of the most valuable meetings you have as CISO. Listen to their questions, and try to determine how the team members receive your answers. The best way to maintain focus is to create an agenda that always has the same format:

- What did you say you were going to do during this period?
- What did you do during this period?
- What is the business value of what you did during the period?
- What business value would the executive team like you to deliver during the next period?

The members of the executive team will determine how to integrate security needs into their strategy. They must give you clearly defined expectations of what constitutes success. This will give you a clear mission and an objective for future meetings. Ensure you focus on meeting your business objectives.

**Resources for the Act Phase**

**Gartner Research and Tools**

Gartner offers a variety of written research and customizable Toolkits to help CISOs in the act phase, including sample charters, job descriptions and other resources. See gartner.com for these and other related resources:

- "Toolkit: Enterprise Security Charter Sample Templates" — Use one of the templates in this Toolkit as a starter kit for your new enterprise information security charter.
"Security Governance, Management and Operations Are Not the Same" — Use this research to gain a clear understanding of the difference between security governance, management and operations, and how it impacts your security team.

"The Security Processes You Must Get Right" — Learn why a catalog of core security processes is necessary to satisfy governance and audit requirements.

"Develop the Key Competencies Required by the New Security Team" — Discover why security staff need to continuously evolve and improve their skills.

"Toolkit: Job Description for Information Security Architect" — Use this, and many other job descriptions, to fill any open positions in your team.

Other Suggested Resources

- **Security and management consulting resources** — Leverage supplemental resources from external providers when internal resources don't exist to drive action in the targeted areas.

- **Existing security service providers** — Take advantage of the fact that security providers may be more flexible in offering assistance in addressing your targeted objectives as they seek to influence a new CISO. Beware that this can turn into a sole-sourced marketing exercise.

**Measure Phase (Days 45 to 100)**

The measure phase is your opportunity to start providing evidence of your impact. This phase overlaps significantly with the act phase. The overlap provides the opportunity for feedback so that act phase activities and deliverables can be adjusted, ensuring they produce the desired tangible results.

**Target Outcomes for the Measure Phase**

- An initial status report for executive management and the steering committee
- Evidence of early progress and achievements
- The foundations of an effective security reporting framework
- First-quarter status report

**Actions for the Measure Phase**

**Develop an executive reporting framework and process:** Effective metrics reporting often takes into account the characteristics of individuals that the report goes to. Concepts, language and areas of individual sensitivity are important. Identify your audience. Know each person's interest and expectations. Understand the decisions that each person makes every day. Refine the metrics that you have.
Communicating in the Measure Phase

**Monitor program and project progress:** You must still monitor the security projects you inherited, and remain involved with the projects you have initiated. Regular progress reports should be brief and focus on only the project information you need to discuss with business leaders and financial management. Keep your project managers focused on telling you how they're doing, not what they're doing. Ask occasional probing questions at greater levels of detail, to ensure that you can articulate the business value of the project team’s efforts.

**Highlight early wins, successes and challenges:** Schedule meetings with your line manager, team leaders, and key stakeholders to gather their thoughts on the progress made and challenges encountered during the first 90 days of your tenure. Collate the findings into a first-quarter status report for executive management and the steering committee. Report only on what is relevant to them. Don’t rely on just numbers. Interpret the metrics for your audience, and provide recommended courses of action.

Resources for the Measure Phase

**Gartner Research and Tools**

Use Gartner research and Toolkits to craft metrics and develop communications tools. Sample resources include:

- "Sharpen Your Security Metrics to Make Them Relevant and Effective" — Use this research to help you develop pragmatic, meaningful security metrics.
- "Five Required Characteristics of Security Metrics" — Ensure your security metrics satisfy these five characteristics before you report.
- "Toolkit: ITScore for Information Security Chart Maker" — Use this Toolkit to produce charts for inclusion in reports and presentations.
- "Why You Should Develop a Balanced Scorecard for Security and Risk Management" — Implement a balanced scorecard to provide a critical communication tool necessary for demonstrating value to the enterprise.
- "Toolkit: Developing a Balanced Scorecard for Security" — Use this Toolkit as a template for developing a balanced scorecard for your security program.

**Other Suggested Resources**

- **Industry best-practice frameworks** — Examine established frameworks, such as ISO 27002, COBIT and SANS, which offer an abundance of best-practice guidance for security leaders.

**Gartner Recommended Reading**

*Some documents may not be available as part of your current Gartner subscription.*
"Develop the Skills of the Contemporary CISO"

"Telkom SA Develops a Practical Information Security Framework"

"Creating the Communications Core: The CIO's Guide to Effective Communications"

"How to Manage and Defend Your Security Budget"

"CISOs Need to Understand the Components of Their Information Security Programs"

"Adapt Your Traditional Staffing Practices for Cybersecurity"

More on This Topic

This is part of an in-depth collection of research. See the collection:

- Job Descriptions for Risk and Security Leaders