Gartner for IT Leaders

The CISO’s Guide to Your First 100 Days

By William Candrick, Sam Olyaei, Tom Scholtz

Gartner®

The CISO's Guide to Your First 100 Days

Published 24 May 2021 - ID G00747118 - 20 min read

By Analyst(s): William Candrick, Sam Olyaei, Tom Scholtz

Initiatives: Security and Risk Management Leaders

Your first 100 days in the chief information security officer (or equivalent) role determine your success as a security and risk management leader. Gartner provides guidance and support to help new CISOs maximize their success during this pivotal transition phase.

Overview

Key Findings

- Successful chief information security officers (CISOs) are primarily leaders, managers and communicators — not technologists.
- A CISO's success depends on two important achievements: (1) establishing a personal brand of credibility and leadership, and (2) laying the foundation for a defensible security program.
- New CISOs struggle when they fail to understand leadership expectations or fail to effectively communicate how security supports business outcomes.

Recommendations

For security and risk management leaders in their first 100 days in the CISO role:

- Strengthen the cybersecurity program's relationship with the business by linking your leadership priorities to business outcomes and objectives.
- Define a strategy for security before diving into technical details and technology decisions.
- Maximize your chances of success by identifying two to five priorities you can accomplish in the first 100 days.
- Budget extra time for unpredictable security incidents before they inevitably occur to avoid delaying strategic initiatives.

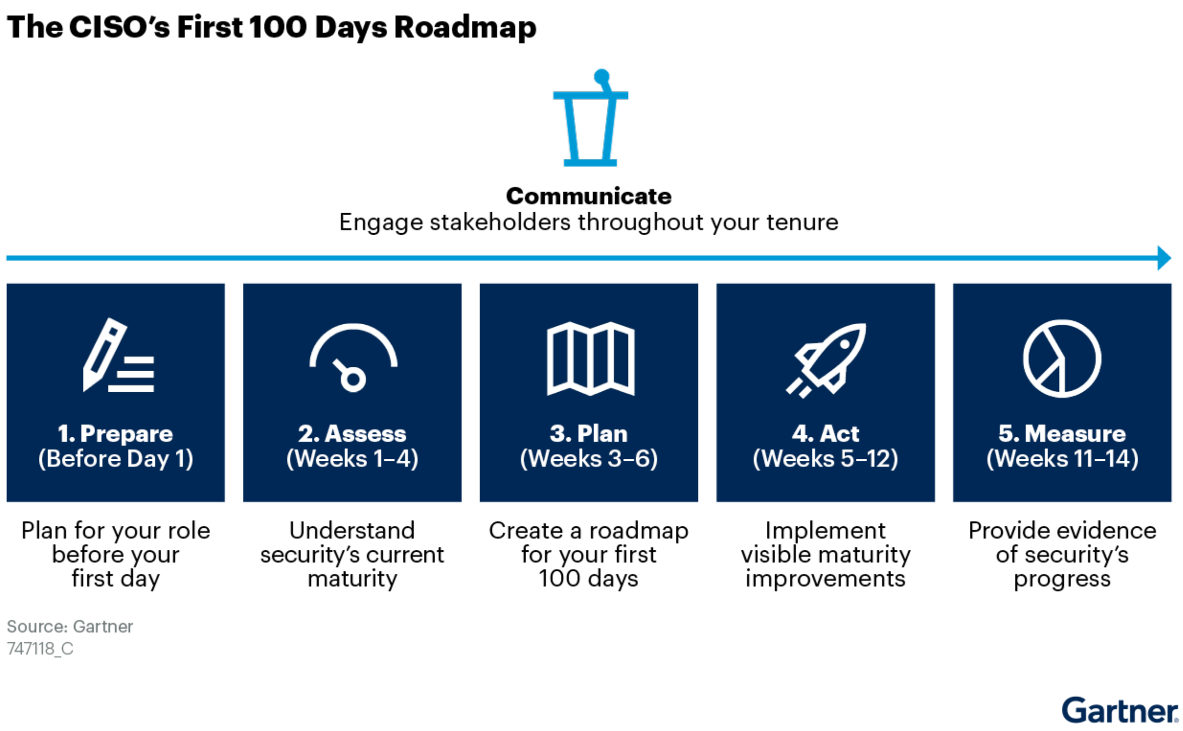
- Win the security team's support by sharing a strategic vision, showing how staff fit into that vision and avoiding publicly criticizing predecessors.

Introduction

Your first 100 days in the CISO role represent an opportunity to define your role and professional relationships. This short "honeymoon" period typically provides the leeway to develop a strategy, make C-suite connections, secure leadership support, establish trust with your new team and signal your leadership style. This opportunity is especially valuable if the enterprise needs a major overhaul to cyber risk governance or significantly better security program maturity.

This research examines how leading CISOs make full use of their first 100 days. We break this period into six phases: prepare, assess, plan, act, measure and communicate (Figure 1).

Figure 1: The CISO's First 100 Days Roadmap


The CISO's First 100 Days Roadmap
Communicate
Engage stakeholders throughout your tenure
1. Prepare (Before Day 1)
Plan for your role before your first day
2. Assess (Weeks 1–4)
Understand security's current maturity
3. Plan (Weeks 3–6)
Create a roadmap for your first 100 days
4. Act (Weeks 5–12)
Implement visible maturity improvements
5. Measure (Weeks 11–14)
Provide evidence of security's progress
Gartner

Source: Gartner
747118_C

Phases and Goals of a CISO's First 100 Days: Click links to jump to sections

Phase	Goal
Prepare	Plan for your role before your first day.
Assess	Understand security's current maturity.
Plan	Create a roadmap for your first 100 days.
Act	Implement visible maturity improvements.
Measure	Provide evidence of security's progress.

The First 100 Days Plan

In brief, a successful agenda for the first 100 days should:

- Establish your credibility as a CISO and elevate the security enterprise's internal brand and image.
- Establish the current maturity of the security program (see IT Score for Security and Risk Management).
- Focus on a subset of strategic initiatives that are selected and prioritized by a defensible methodology (e.g., maturity assessment, risk assessment).
- Bridge the gap between security operational excellence and business value (e.g., C-suite priorities).
- Define realistic, measurable, time-bound goals — and establish metrics to track progress.

The remainder of this research note provides actionable guidance to achieve these objectives.

Prepare Phase (Before Day 1)

Back to top

Prepare for your new role before your first day on the job. A little initial planning sets the stage for a successful start and establishes the relationships you'll need throughout your tenure as a CISO.

Target Outcomes for the Prepare Phase

Target the following outcomes as you prepare for the CISO role:

- A **common understanding** of your role and the expectations of your staff, senior stakeholders and leadership team.
- A **basic engagement plan** to meet leadership stakeholders and security staff.

This phase focuses on listening and learning — not decision making. Avoid making sweeping announcements or decisions in your first few weeks in the CISO role.

Actions for the Prepare Phase

Take the following actions before you begin your first day:

Assess the type of CISO that your enterprise requires: Enterprises have different requirements based on culture, industry, political challenges and other factors. Some will require an operationally-driven CISO, while others will require a more business-focused one. Gartner recommends that security and risk management leaders view the CISO Effectiveness Index and work on developing profiles based on their enterprise's needs.

Understand your enterprise's structure: Request organization charts and operational documents (e.g., process maps) to understand the structure of security, IT and the overall enterprise. Ensure you understand security's current governance and operational role in the enterprise.

Identify key stakeholders: Create a list of leadership stakeholders with whom you'll be working. This list may include (but is not limited to) the CEO, CFO, CIO, general counsel, head of HR, chief privacy officer (CPO) and chief risk officer (CRO).

Establish new connections: Engage leadership stakeholders and security staff, ideally before your first day in the role. Engagement tactics include thank-you notes after interviews and LinkedIn connections (with personalized notes).

Schedule initial meetings: Work with your administrative assistant (or a friendly contact within the enterprise) to set up your initial round of meetings. Plan a Day 1 all-hands security team meeting, and a Week 1 series of meet-and-greets with key stakeholders across the enterprise. The first few weeks are an opportunity to make introductions and establish yourself across the enterprise.

Communications in the Prepare Phase

Before Day 1, your focus should primarily be on learning about the enterprise and preparing messages for stakeholders and your team. Success in your initial few weeks will depend on effective communication — not decision making.

Focus on the following before Day 1 and in your initial weeks in the role:

Understand your C-suite's priorities: Effective CISOs understand that they are corporate executives — not just operational managers or technical subject matter experts. Achieving your full potential as a CISO requires understanding your enterprise's business and the priorities that are top of mind for the C-suite and board. Consider the following sources of information before your first day:

- Learn your company's mission statement from the "About us" webpage.
- Understand leadership priorities and concerns by reading recent public financial filings (e.g., 10-Q or 10-K reports for publicly traded U.S. companies).
- Read and watch recent leadership communications and interviews (and consider following leadership social media accounts).
- Identify any competing priorities within the C-suite, and prepare to navigate security through these leadership complexities.

Introduce yourself: Create a short bio that covers your personal background, your career path and your initial thoughts on joining the enterprise. Use this bio in presentations and meet-and-greets so that everyone understands who you are and where you come from. Avoid announcing bold, disruptive decisions in these initial introductions. Rather, your primary goal is to be welcomed by your peers and team.

Use storytelling: Storytelling is an effective way to change perspectives and gain acceptance. For example, a new CISO may tell a story that illustrates how security's role is to help the enterprise move fast and secure — not slow things down in order to reduce every risk to as low a level as possible. Giving an illustrative example from past experience or events in the news helps stakeholders understand how security, and by extension the CISO, is a resource — not a roadblock.

Create discussion guides: Prepare questions and talking points before your initial round of meet-and-greet meetings. For example, consider the following:

- **Stakeholder discussions:** For these meetings, focus on stakeholder perceptions of security and the CISO role. Gathering this information early in your first 100 days will help you plan changes in the months ahead, including changing leadership perspectives and (re)defining the CISO role. Questions to ask include:
  - What are your most urgent business priorities?
  - What's your current perception of the security function?
  - What are your biggest pain points working with security?
  - What's going well working with security?

- **Staff discussions:** Prepare questions that diagnose (1) the current state of security governance and operations, and (2) staff perceptions of the team and work environment. Questions to ask include:
  - Where do you focus most of your time?
  - What would make your job easier?
  - What's most challenging about your role?
  - How can I better support you and your team?
  - What do you think security's top priorities should be?
  - What do you see as the enterprise's top objectives?

Resources for the Prepare Phase

Review the following Gartner resources to get started.

Gartner Research and Tools

The Roadmap to CISO Effectiveness — Tailor your leadership approach based on proven best practices sourced from leading CISOs.

Develop the Skills of the Contemporary CISO — Identify and build skills to develop into a well-rounded and capable CISO.

CISO Effectiveness: A Report on the Behaviors and Mindsets That Impact CISO Effectiveness — Identify the behaviors and mindsets that most strongly correlate with CISO effectiveness.

Assess Phase (Weeks 1-4)

Back to top

Assess security’s current maturity and performance. A quality security assessment surfaces gaps that will inform strategic planning. Successful CISOs rely on objective assessments, rather than instinct, so that decision making is defensible and repeatable.

Target Outcomes for the Assess Phase

Target the following outcomes as you assess the security program:

- An **executive mentor** that provides insight into the culture of the enterprise.
- An understanding of the **resources available to you** — including funding, headcount and technology.
- A **list of security gaps** surfaced via formal maturity assessments, team conversations and stakeholder engagement.
- A prioritized list of **three to five strategic priorities** that address security gaps and align to business outcomes.

Actions for the Assess Phase

Take the following actions within your first month in role:

Seek out an executive mentor: One of your most valuable assets will be a senior-level mentor. Look for a leader who has insight into the inner workings of senior executive staff. Knowledge of the security field is not necessary; in fact, your mentor will best serve you if she has little knowledge of security so that you gain a realistic, objective sense for how your proposals and leadership is received.

Establish security's roles and responsibilities: Your first priority in the CISO role is to clarify and define security's roles and responsibilities. Have a discussion with your manager to fully scope the security function and your role. Consider clarifying ownership in areas such as:

- Physical security
- Business continuity and disaster recovery (BC/DR)
- Privacy
- Compliance
- IT risk
- Risk governance
- Security operations

For areas outside security's remit, ensure you develop working relationships with peer managers and leaders (e.g., head of ERM, chief privacy officer, general counsel).

Inventory your information sources: Quickly take inventory of information sources you'll need to manage the security function. For example, locate any existing policies, org charts, strategic plans, current projects, technology roadmaps and metrics. Use these information sources to inform your understanding of security's current state and immediate plans.

Perform maturity assessments: Create a safe environment for security staff to candidly assess security's maturity. These assessments surface gaps that inform forward-looking strategy setting — not backward-looking blame. As a new CISO, you should at least perform the following core assessments, and consider adding additional ones if possible.

Core assessments for the first 100 days:

- **Functional maturity assessment:** Assess security's capability and process maturity. Consider Gartner's IT Score for Security and Risk Management.
- **Controls maturity assessment:** Assess security controls implementation maturity. Consider Gartner's Controls Maturity Benchmarking Service.
- **Risk assessment:** Assess information risks associated with applications and infrastructure across the enterprise. Risk assessments should be prioritized for the highest areas of risk, and information collected in any existing risk registers may help assess your enterprise's risk posture.

Additional assessments:

- Audit findings
- Vulnerability assessments
- Threat assessments
- Talent assessments
- Regulatory findings
- Penetration tests
- Phishing tests

Identify your top strategic priorities: Conducting assessments will reveal gaps that exist across the security program. Use these gaps to identify three to five strategic priorities to address in your first 100 days. These priorities should address fundamental challenges and make a positive impression on the security team and senior leadership.

Consider priorities that:

- Address fundamental requirements for a successful security program
- Clearly link to business outcomes
- Provide a foundation for multiyear maturity improvement
- Establish your credibility as an effective CISO and officer of the company

Communications in the Assess Phase

Assessing security's current state can be a challenging process. For example, some security staff may minimize gaps because they feel defensive or prefer to present things in the best possible light. Conversely, other security staff may exaggerate gaps in order to get investment and support for their narrow priorities. Remember, these are normal human tendencies and can be countered by creating an environment of open, safe and transparent communication.

Focus on the following communication opportunities:

- **Meet team leads:** Hold one-on-one meetings with security team leads. Gauge their opinions on the current state of the security program, and make clear that each leader plays a pivotal role in setting an executive security's strategy in the coming weeks, months and years ahead.
- **Interview stakeholders:** Interview stakeholders and gather their perceptions of the security function. Stakeholders to target include general counsel, chief privacy officer, CIO, chief audit executive and head of HR.
- **Identify influencers:** As you meet leaders across the enterprise, make note of senior influencers who can advance security priorities, give you a personal mandate and help you prepare for senior- and board-level communication.

Resources for the Assess Phase

Review the following Gartner resources to get started.

Gartner Research and Tools

IT Score for Security and Risk Management — Assess the maturity of your security function's processes and capabilities.

Controls Maturity Benchmarking Service — Benchmark the maturity of your technical controls with similar peers.

Plan Phase (Weeks 3-6)

Back to top

The plan phase synthesizes information from your assessments into a blueprint for action. Your initial planning sets the roadmap for your first 100 days, and guides security's success over your first year in the role.

Target Outcomes for the Plan Phase

Target the following outcomes as you conduct planning:

- A **documented strategic plan** that prioritizes two to three security initiatives for your first 100 days, and a loose roadmap for your first year.
- An **operational budget** that ensures sufficient resources to achieve priorities. If resources are lacking, then the strategic plan should be adjusted accordingly so it is achievable.

Actions for the Plan Phase

Take the following actions as you conduct planning:

Select a few top priorities: Examine your top priorities and select two to three to focus on over the next three months. Use the following criteria to filter down to these top priorities:

- Can the initiative be achieved within three months?
- Will you have the required executive support, resources and budget?
- Is the initiative linked to cyber-risk reduction?
- Is the risk of failure relatively low?

As you select priorities, help business leaders understand how security priorities support business outcomes. Making this connection early maximizes the credit that you and the security function receive for achieving strategic priorities.

Design or refine your security function: Structure the security function based on your mandate, priorities and enterprise's culture. Unfortunately, there's no one-size-fits-all approach to security org design; rather, you should design the function in such a way that roles and responsibilities are clear, managers are empowered and accountable, and connections to peers outside security (e.g., IT, privacy, legal) are clear.

Plan your operational budget: Your level of control over security's budget will depend on when you joined the enterprise (beginning, middle or end of fiscal year) and the current budgeting process. While some aspects of budgeting may not be flexible during your first 100 days, you should ensure that your operational budget can support your strategic priorities. You may consider reallocating resources to support priorities.

Communications in the Plan Phase

Document a security strategic plan: Your first 100 days strategic plan should consist of three parts:

1. The program vision ("where we want to be").

2. Results from your maturity assessments ("where we currently are").

3. A gap analysis and strategic priorities ("how we'll get there").

Create a security program vision: Information security programs require a clear, concise vision statement. This statement lays out security's high-level mandate and goals, and should be shared with your team, management and relevant stakeholders.

Resources for the Plan Phase

Review the following Gartner resources to get started.

Gartner Research and Tools

Ignition Guide to Strategic Planning for Information Security — Create a strategic plan using our step-by-step guidance.

Security Strategy Planning Best Practices — Develop an actionable strategic plan that establishes

credibility and generates support.

Security Portfolio Prioritization: Adding Rigor to Security Investment Decisions — Design a repeatable and defensible methodology to prioritize internal security projects.

Toolkit: Information Security Strategy on a Page — Deconstructed — Create a one-page strategy document that resonates with C-suite leadership.

Act Phase (Weeks 5-12)

Back to top

The act phase delivers security capability improvements. Actions in your first 100 days should focus on tangible, visible accomplishments that establish personal credibility and advance security's standing in the enterprise. Initial success secures more buy-in, which supports more success — thus creating a cycle of improvement and achievement for you and your team.

Target Outcomes for the Act Phase

Target the following outcomes as you take action:

- A series of **scheduled meetings** with security managers, staff and teams.
- An **assigned project owner** for each of security's top priorities.
- A **security budget** that ensures sufficient resources for your strategic priorities.
- A list of **tangible and measurable project results** that demonstrate progress against your strategic objectives.

Actions for the Act Phase

Take the following actions as you implement your plan:

Refine roles and responsibilities: First, ensure that all security managers have well-defined roles and responsibilities. Make clear what each security manager is accountable for, and how their performance will be assessed. Second, ensure that all line-level security staff have clear job descriptions and responsibilities that clearly reflect the work each employee actually does. Keep in mind that job descriptions and performance management metrics often differ from the realities of how work actually gets done — a gap that should be rectified under your new leadership.

Remember, security managers can help develop roles and responsibilities for themselves and their teams. As CISO, you should oversee this work, but don't feel you must complete all management tasks yourself.

Assign project ownership: Each of your strategic priorities should have a formal project owner. Establish a clear plan, expectations and outcomes for each project, and clarify these with respective project owners. One way to minimize the risk of project failure is to establish multiple project objectives and avoid projects that have binary outcomes (success or failure).

Secure leadership support: Use your strategic plan and security vision to engage leadership and get buy-in for your top priorities. Leadership support gives you and your team a mandate, which can be used to secure funding, influence stakeholders and motivate the security team.

Establish security governance processes and forums: Begin work to build effective information risk governance across the enterprise. This entails risk decision-making rights, risk accountability and the responsibilities of stakeholders across the enterprise for information risk. One of your largest challenges as a new CISO will likely be instilling proper risk ownership and decision making.

Implement any necessary budget changes: If necessary, implement budget changes to support your initial strategic priorities. Your top priority now is to ensure sufficient funding and resources over the next three to six months. Now is a good time to also begin planning your next fiscal year budget. As a new CISO, you may have considerable goodwill and leeway to reallocate funding or even secure additional resources. Keep in mind that your initial budget will likely serve as a benchmark of comparison in future years, so ensure you structure your budget to support a multiyear roadmap.

Communications in the Act Phase

Socialize your strategic plan and vision: Present your strategic plan and vision to leadership and stakeholders across the enterprise. As you socialize your plan, tailor your message to your audience by linking your plan to stakeholder priorities. Show the connection between information security and the priorities and objectives of leaders across the enterprise.

Schedule team and manager check-ins: People management is a major aspect of the CISO role. As a first step in managing your team, create recurring meetings across the security team. In particular, consider the following:

- Conduct weekly one-on-one check-ins with each security manager. Use these meetings to plan and track projects. Manager meetings are also a coaching opportunity, especially with regard to instilling business awareness and context into day-to-day security operations.
- Establish monthly or quarterly “skip level” one-on-ones with security staff. You can schedule these on a rolling basis so that you meet with multiple staff members every week. These meetings are an opportunity to directly communicate with staff, gather input and gauge morale.

- Schedule monthly all-hands meetings. As CISO, you can make major announcements, recognize top performers and provide important updates to the full team. As a development opportunity, you can select managers and staff members to present at these meetings.

- Encourage standing team meetings. Security managers should consider daily standing meetings with their respective teams. These short meetings (e.g., under 30 minutes) set the day's agenda, provide an opportunity for Q&A and facilitate collaboration. Daily standing meetings are especially important with virtual teams, as they replace "water cooler" conversations that occur among in-person teams.

Resources for the Act Phase

Review the following Gartner resources to get started.

Gartner Research and Tools

Information Security Presentation Support Center — Use "download and go" templates to strengthen your message to leadership and stakeholders across the enterprise.

Use relevant tools and templates to mature your processes:

- Ignition Guide to Developing a Security Incident Response Plan
- Ignition Guide to Designing and Launching a Security Champion Program
- Ignition Guide to Strategic Planning for Information Security
- Ignition Guide to Creating a Functional Health Dashboard for Information Security
- Ignition Guide to Building a Cyber Crisis Testing Program

Measure Phase (Weeks 11-14)

Back to top

The measure phase provides evidence of your impact on security and the enterprise. Measurement and communication are hallmarks of a successful CISO, and you should dedicate significant effort to this endeavor throughout your tenure.

Target Outcomes for the Measure Phase

Target the following outcomes as you measure performance:

- A **defined set of operational metrics** to track performance and progress across security initiatives.
- **Evidence of early progress** to be reported to stakeholders and the leadership team.
- An **established meeting and reporting cadence** for various stakeholders, including the CIO, risk steering committee, C-suite and board.

Actions for the Measure Phase

Define a portfolio of security metrics: Create a small portfolio of operational KPIs and then adapt these operational metrics into business-relevant metrics that resonate with leadership and the board. The best business-relevant metrics include business context and abstract away from technical details.

Develop an executive reporting process: Establish reporting frequency and audiences, such as the steering committees, C-suite briefings and board reporting (full board and risk committee). Once reporting expectations are set, spend time understanding the expectations and priorities of each audience. Then, create metrics and reports relevant to each audience, and establish processes and responsibilities for security staff to maintain and refresh these dashboards on a regular cadence.

Communications in the Measure Phase

Monitor program and project progress: Track security's progress and program maturity gains. Report progress to leadership, and use this momentum to make the business case for continued (or increased) funding and support as needed. Coach security managers and project leaders to articulate security in business-relevant terms. Your leadership team should be able to succinctly explain how security's priorities map to and support the enterprise's business objectives.

Highlight early wins and challenges: Maintain momentum by communicating wins and identifying solutions to address challenges as they emerge. Keep in mind that most security initiatives have multiple objectives (some smaller, some larger) — and even if some objectives are delayed or missed, others may be achieved.

Resources for the Measure Phase

Review the following Gartner resources to get started.

Gartner Research and Tools

Why You Should Develop a Balanced Scorecard for Security and Risk Management — Implement a balanced scorecard to communicate business-relevant metrics to leadership.

Toolkit: Developing a Balanced Scorecard for Security — Use this download-and-go tool to quickly create a security balanced scorecard.

Five Required Characteristics of Security Metrics — Design metrics that satisfy best practices.

Tool: A Simple NIST CSF Management Dashboard — Develop a security management dashboard that reflects industry standards (e.g., the NIST Cybersecurity Framework) and resonates with senior leaders across the enterprise.

Document Revision History

The Chief Information Security Officer's First 100 Days - 27 June 2014

The New CISO's Crucial First 100 Days - 17 February 2011

Toolkit: The New CISO's Crucial First 100 Days - 2 February 2007

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

The Roadmap to CISO Effectiveness

Security Strategy Planning Best Practices

IT Score for Security and Risk Management

Five Board Questions That Security and Risk Leaders Must Be Prepared to Answer

Phase	Goal
Prepare	Plan for your role before your first day.
Assess	Understand security's current maturity.
Plan	Create a roadmap for your first 100 days.
Act	Implement visible maturity improvements.
Measure	Provide evidence of security's progress.

Actionable, objective insight

Ensure your cybersecurity function is positioned for success. Explore these additional complimentary resources and tools for security and risk leaders:

Infographic

Protect Your Business Assets With a Roadmap for Maturing Information Security Program

Make sure your security adapts to current and new threats.

Download Infographic

eBook

3 Must-Haves in Your Cybersecurity Incident Response

Build a cybersecurity response plan for your organization today.

Download Now

Research

Predicts 2022: Cyber-Physical Systems Security — Critical Infrastructure in Focus

Prepare your enterprise for a secure future.

Download Now

Webinar

The Gartner Leadership Vision for 2022: Security and Risk Management

Plan for 2022 and stay ahead of the evolving challenges.

Watch On Demand

Already a client?
Get access to even more resources in your client portal. Log In

Gartner®

Connect With Us

Get actionable, objective insight to deliver on your mission-critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance. Contact us to become a client:

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

Become a Client

Learn more about Gartner for IT Leaders
gartner.com/en/information-technology

Stay connected to the latest insights

Attend a Gartner conference
View Conferences

Gartner®