Gartner

Gartner for IT Leaders

Protect Business Assets With a Roadmap for Maturing Information Security

What are the critical components necessary to increase security capability and effectiveness?

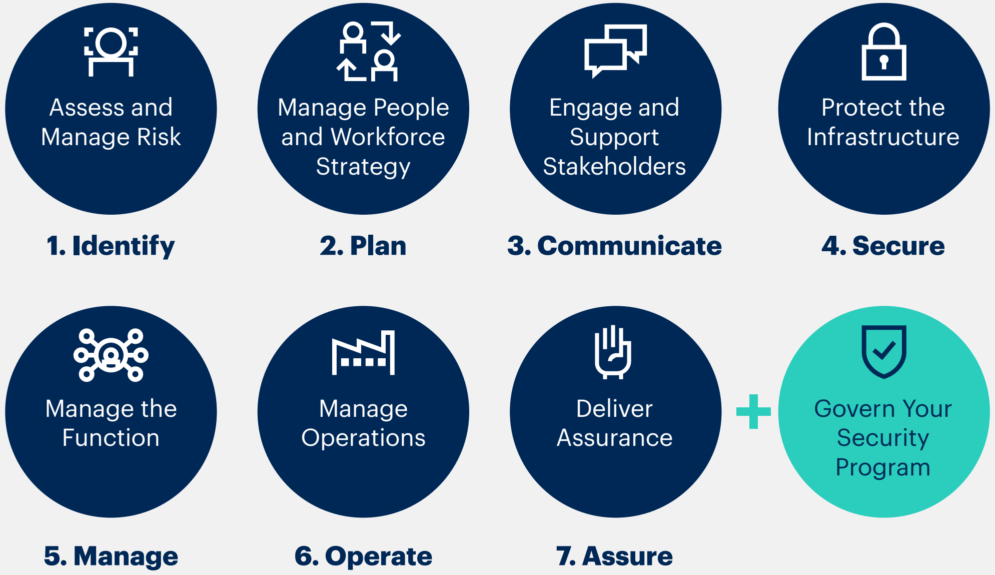
The importance of information security is rising rapidly as senior executives become aware that poor security can cause irreparable damage to the business. By 2023, 30% of chief information security officers' (CISOs') effectiveness will be directly measured on their ability to create value for the business.

Security and risk management leaders must craft and implement an information security vision that supports both the creation of digital value at scale and pragmatic management of security risks. Increasing security capability and effectiveness is critically dependent on the implementation of a mature framework that plans, architects, reports and modifies security activities depending on both internal and external factors.

Without a security program, an organization's security activities will be no more than a collection of technical implementations that do not systematically address risks and countermeasures.

A mature security program has seven components that make it effective in meeting organizational objectives.

7+1 Objectives of a Security Program



Assess and Manage Risk — 1. Identify

Manage People and Workforce Strategy — 2. Plan

Engage and Support Stakeholders — 3. Communicate

Protect the Infrastructure — 4. Secure

Manage the Function — 5. Manage

Manage Operations — 6. Operate

Deliver Assurance — 7. Assure

+ Govern Your Security Program

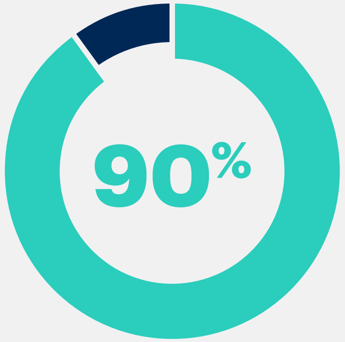
Source: Gartner

How can you adapt your security program to meet new landscape threats?

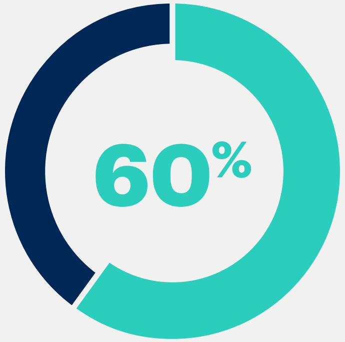
A mature security program is a strongly governed collection of policies, processes and architectural practices that provide:

- Boundaries for user, system and configuration activities
- Guidance for design, implementation and operations

A mature security program must be adaptive to the threat landscape and the resulting risks to the organization. The program must fit business needs and requirements. It takes time to develop, is highly evolutionary and will be self-adjusting to change. Achieving such maturity is a team effort. Effective chief information security officers realize heads of sales, marketing and other business units are key partners as users of technology and, subsequently, risk happens outside of IT at scale.



Interest in security and risk management is increasing at the board level, with 90% of security and risk management leaders having reported to the board at least once in the past year.



By 2024, 60% of CISOs will establish critical partnerships with key market-facing executives in sales, finance and marketing.

Source: Gartner

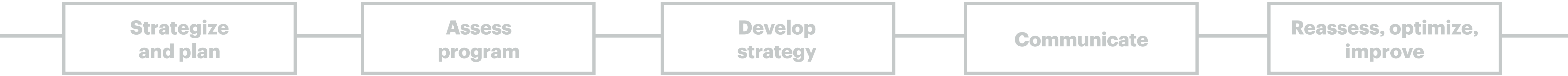
Some of the top questions about maturing information security initiatives are:

1. What is the process of implementing and maintaining a security program?
2. What are the components of an information security program?
3. How do you communicate the value of information security in business terms?

What are the key stages?

This best-practice insight is distilled from interactions with clients who have successfully implemented security programs. The roadmap shows the sequence of objectives and desired outcomes and is useful for aligning all stakeholders.

A few key milestones and a sample of associated Gartner resources are highlighted below, but the full roadmap includes complete details of all milestones and resources for each stage.



Strategize and plan

Assess program

Develop strategy

Communicate

Reassess, optimize, improve

Strategize and plan

Security plan and key outcomes defined

Actions to take:

□ Understand key business priorities and define program mission, vision; identify business, technology and threat drivers.

□ Identify goals and program value, key stakeholders, roles, responsibilities.

□ Define security control in line with organizational strategies and map to standardized security framework.

+ more

Associated Gartner resources include:

- Research: Leadership Vision for 2021: Security and Risk Management
- Research: IT Score for Security and Risk Management
- Research: Information Security Controls Mapping Tool
- Analyst inquiry to identify goals and program value and define key stakeholders with roles and responsibilities

+ more

Assess program

Current state assessment and roadmap created

Selected tasks include:

□ Assess existing systems, people, processes, tools, technologies, user awareness, interactions with third parties.

□ Undergo baseline current maturity and define target state and gap analysis.

□ Use audit results to develop draft strategy and milestones aligned to program objective; get stakeholder feedback.

+ more

Associated Gartner resources include:

- Phone consultation for introduction to the Gartner BuySmart™ process and review of strategic, financial and technical requirements to identify where spend management is needed
- Analyst inquiry to develop security architecture, policy framework and solution layer and discuss a more functional assessment approach for security

+ more

Develop strategy

Strategy document created to enable initial implementation

Selected tasks include:

□ Establish security team roles and responsibilities; identify stakeholders to be accountable, consulted, informed.

□ Develop critical competencies in information security; train for desired and missing skills.

□ Use metrics and incentives to drive accountability among owners.

+ more

Associated Gartner resources include:

- Research: Rules for Presenting Status Reports to the Board of Directors
- Analyst inquiry to identify and build strategic partners and vendors and discuss a more functional assessment approach for security

+ more

Communicate

Communication plan implemented to get stakeholder buy-in

Selected tasks include:

□ Get Executive Board of Directors' buy-in, resource backing and seat at the executive decision-making table.

□ Develop advanced reporting and response; craft communications plan for cyberbreach.

□ Assess progress against key metrics; communicate value delivered to date.

+ more

Associated Gartner resources include:

- Phone consultation to develop organization and board communication plan on value deliverance
- On-site workshop to instill culture of secure employee behavior; tailor training and awareness campaigns
- Attend the Gartner IT Symposium/Xpo™ conference

+ more

Reassess, optimize, improve

Program reassessment, accuracy tracking and improvement

Selected tasks include:

□ Develop program structure to monitor and combat advanced threats.

□ Build competency in reverse malware engineering, hunting, cause and origin determination; determine cause and origin.

□ Revisit maturity assessment for further optimization.

+ more

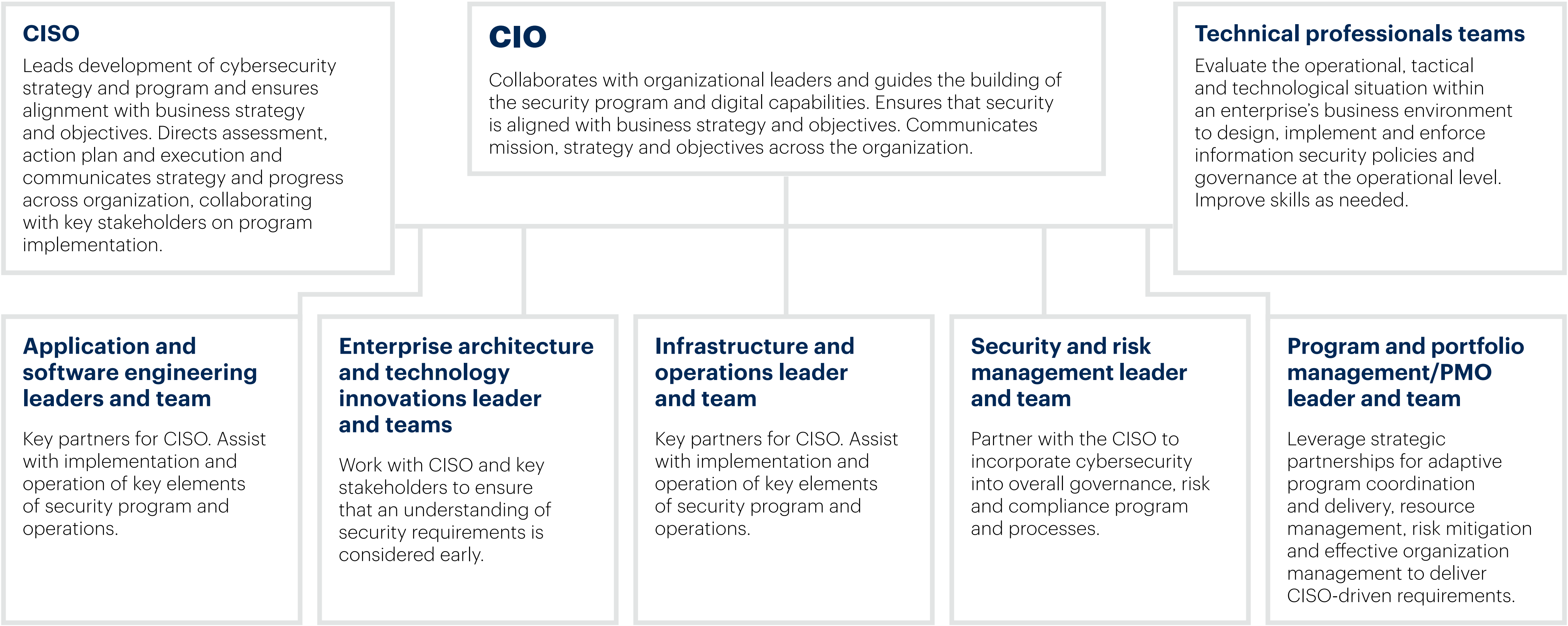
Associated Gartner resources include:

- Phone consultation to discuss the key points that can help to further optimize cybersecurity preparation in the organization
- Analyst inquiry to build competency in reverse malware engineering, hunting, cause and origin determination; determine cause and origin
- Research: How to Build an Effective Cybersecurity and Technology Risk Presentation

+ more

Who needs to be involved?

The most successful companies establish cross-functional teams for their modernization initiatives. We have outlined the recommended functions to involve and their roles to ensure the best success in hitting the milestones.



CISO

Leads development of cybersecurity strategy and program and ensures alignment with business strategy and objectives. Directs assessment, action plan and execution and communicates strategy and progress across organization, collaborating with key stakeholders on program implementation.

CIO

Collaborates with organizational leaders and guides the building of the security program and digital capabilities. Ensures that security is aligned with business strategy and objectives. Communicates mission, strategy and objectives across the organization.

Technical professionals teams

Evaluate the operational, tactical and technological situation within an enterprise's business environment to design, implement and enforce information security policies and governance at the operational level. Improve skills as needed.

Application and software engineering leaders and team

Key partners for CISO. Assist with implementation and operation of key elements of security program and operations.

Enterprise architecture and technology innovations leader and teams

Work with CISO and key stakeholders to ensure that an understanding of security requirements is considered early.

Infrastructure and operations leader and team

Key partners for CISO. Assist with implementation and operation of key elements of security program and operations.

Security and risk management leader and team

Partner with the CISO to incorporate cybersecurity into overall governance, risk and compliance program and processes.

Program and portfolio management/PMO leader and team

Leverage strategic partnerships for adaptive program coordination and delivery, resource management, risk mitigation and effective organization management to deliver CISO-driven requirements.

Client success story: Improving Security Risk Management to Enable Digital Growth

Most critical priority

The client's objective was to develop more mature security capabilities to protect the business and enable digital growth while striking the appropriate balance between risk management, ease of operation and cost.

How Gartner helped

Gartner experts guided an approach and engagement strategy to help the risk team understand business drivers more deeply, communicate the business impact of cyber risk and gain agreement on the business value of security across the organization.

The Gartner risk management framework was also utilized, focusing on business KPIs and KRIs to build an integrated risk management strategy.

Mission accomplished

With the support of Gartner, the client was able to:

- Significantly improve the business's understanding of how investments in the security program supported critical business objectives
- Link the business risk and performance management program with the security risk management program
- Improve ongoing business engagement in security governance
- Pivot executive-level security metrics from purely operational measures to strategic business outcome measures

Actionable, objective insight

Explore these additional complimentary resources and tools on cybersecurity

Roadmap
The IT Roadmap for Cybersecurity

Follow these best practices to create a resilient, scalable and agile cybersecurity strategy.

Tool
Gartner IT Score for Security and Risk Management

Gain perspective on your highest-priority activities to drive business outcomes.

eBook
Top Priorities for IT: Leadership Vision for 2021

Discover emerging trends, expected challenges and next steps for security and risk management leaders in 2021.

Webinar
3 Ways to Gain Support for Your Security Awareness Program

Three ways for security and risk management executives to gain organizational support for their security awareness programs.

Access other roadmaps in this series:

Modernize Business Through Technology Roadmap

The CIO Roadmap to Strategic Cost Optimization

The IT Roadmap for Cloud Migration

Enhance Your Roadmap for Effective Data Governance

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

Gartner for IT Leaders

Follow Us on LinkedIn

Become a Client

Get More.

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

U.S.: 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

Gartner®