

Hire or Develop a World-Class CISO

Find a strategic and security-focused
champion for your business.

Info-Tech Research Group Inc. is a global leader in providing IT research and advice.
Info-Tech's products and services combine actionable insight and relevant advice
with ready-to-use tools and templates that cover the full spectrum of IT concerns.
© 1997-2023 Info-Tech Research Group Inc.

INFO~TECH
RESEARCH GROUP

Analyst Perspective

Create a plan to become the
security leader of tomorrow



The days are gone when the security leader can stay at a desk and watch the perimeter. The rapidly increasing sophistication of technology, and of attackers, has changed the landscape so that a successful information security program must be elastic, nimble, and tailored to the organization's specific needs.

The Chief Information Security Officer (CISO) is tasked with leading this modern security program, and this individual must truly be a Chief Officer, with a finger on the pulses of the business and security processes at the same time. The modern, strategic CISO must be a master of all trades.

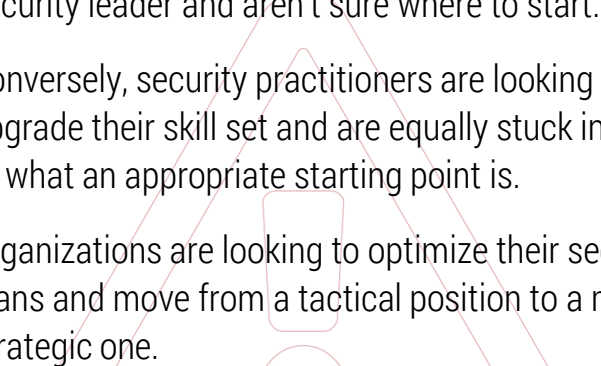
A world-class CISO is a business enabler who finds creative ways for the business to take on innovative processes that provide a competitive advantage and, most importantly, to do so securely.

Cameron Smith

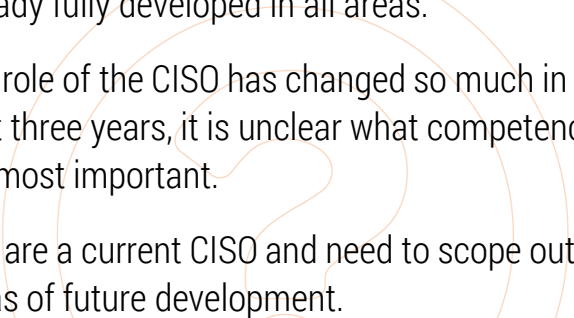
Research Lead, Security & Privacy
Info-Tech Research Group

Executive Summary

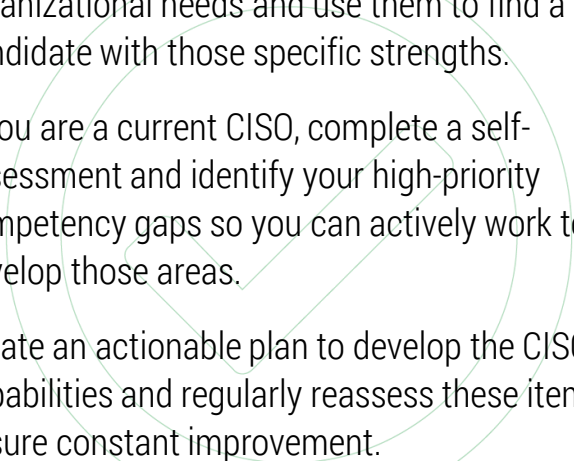
Your Challenge

- CEOs/CXOs are looking to hire or develop a senior security leader and aren't sure where to start.
 - Conversely, security practitioners are looking to upgrade their skill set and are equally stuck in terms of what an appropriate starting point is.
 - Organizations are looking to optimize their security plans and move from a tactical position to a more strategic one.
- 

Common Obstacles

- It is difficult to find a “unicorn”: a candidate who is already fully developed in all areas.
 - The role of the CISO has changed so much in the past three years, it is unclear what competencies are most important.
 - You are a current CISO and need to scope out your areas of future development.
- 

Info-Tech's Approach

- Clarify the competencies that are important to your organizational needs and use them to find a candidate with those specific strengths.
 - If you are a current CISO, complete a self-assessment and identify your high-priority competency gaps so you can actively work to develop those areas.
 - Create an actionable plan to develop the CISO's capabilities and regularly reassess these items to ensure constant improvement.
- 

Info-Tech Insight

The new security leader must be strategic, striking a balance between being tactical and taking a proactive security stance. They must incorporate security into business practices from day one and enable secure adoption of new technologies and business practices.

Your challenge

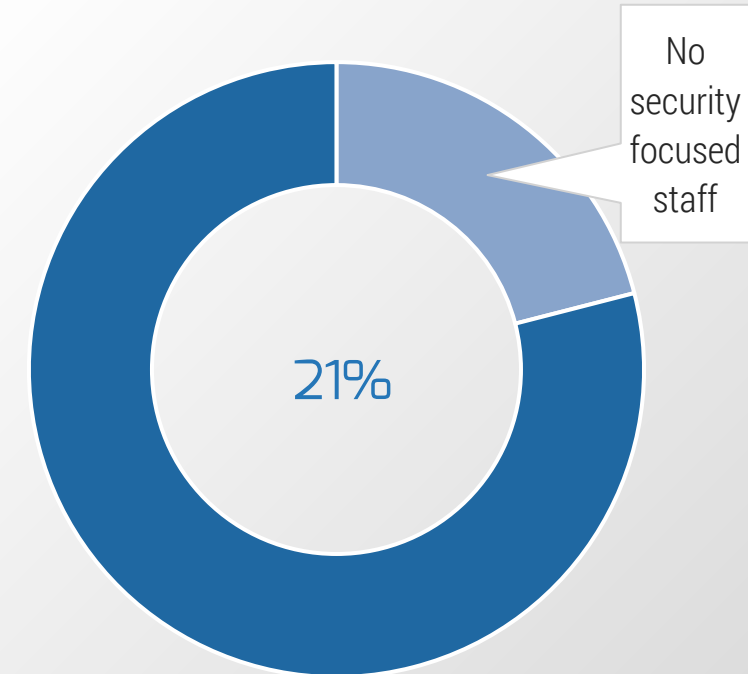
This Info-Tech blueprint will help you hire and develop a strategic CISO

- Security without strategy is a hacker's paradise.
- The outdated model of information security is tactical, where security acts as a watchdog and responds.
- The new security leader must be strategic, striking a balance between being tactical and taking a proactive security stance. They must incorporate security into business practices from day one and enable secure adoption of new technologies and business practices.

Info-Tech Insight

Assigning security responsibilities to departments other than security can lead to conflicts of interest.

Around one in five organizations don't have an individual with the sole responsibility for security¹



¹ Navisite

Common obstacles

It can be difficult to find the right CISO for your organization

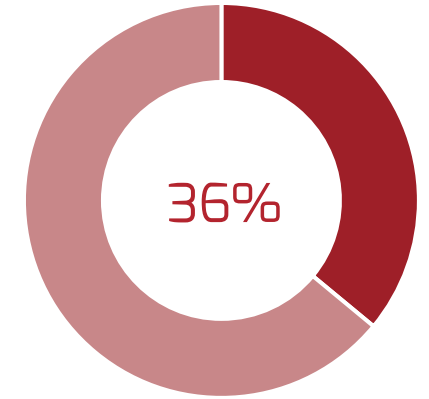
- The smaller the organization, the less likely it will have a CISO or equivalent position.
- Because there is a shortage of qualified candidates, qualified CISOs can demand high salaries and many CISO positions will go unfilled.
- It is easier for larger companies to attract top CISO talent, as they generally have more resources available.

Source: Navisite

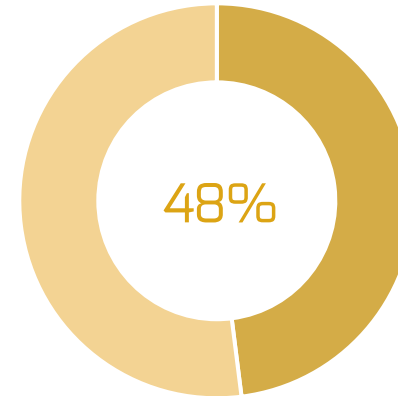
Info-Tech Insight

Developing an internal CISO candidate will likely be easier than trying to hire an external candidate.

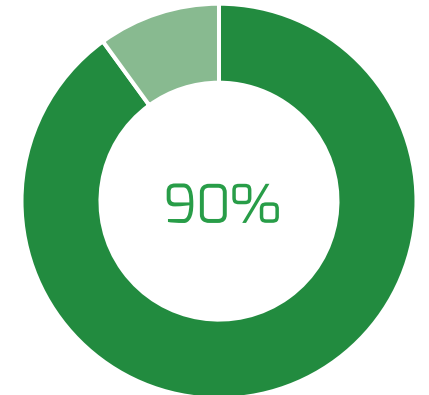
Only 36% of small businesses have a CISO (or equivalent position).



48% of mid-sized businesses have a CISO.



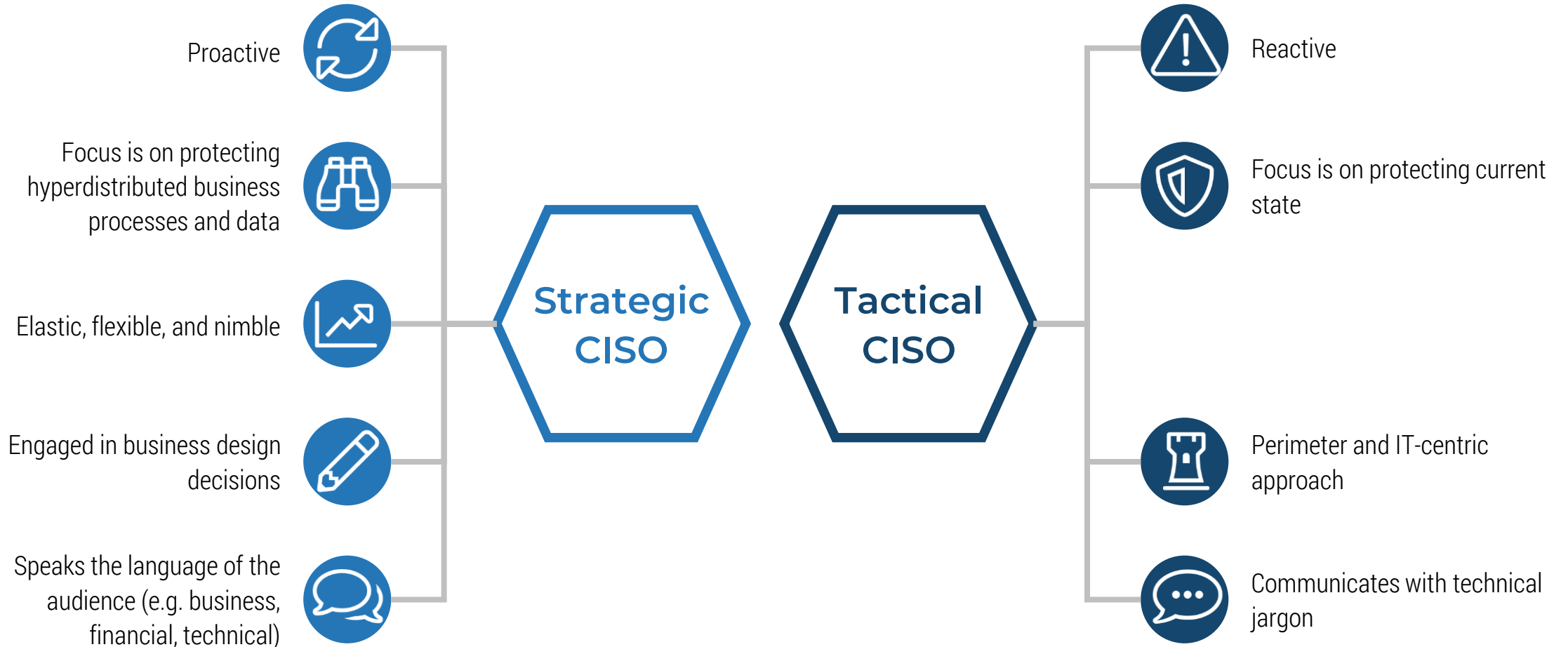
90% of large organizations have a CISO.



Source: Navisite

Strategic versus tactical

CISOs should provide leadership based on a strategic vision ¹



¹ Journal of Computer Science and Information Technology

Info-Tech has identified three key behaviors of the world-class CISO

To determine what is required from tomorrow's security leader, Info-Tech examined the core behaviors that make a world-class CISO. These are the three areas that a CISO engages with and excels in.

Later in this blueprint, we will review the **competencies and skills** that are required for your CISO to perform these behaviors at a high level.



Info-Tech Insight

Through these three overarching behaviors, you can enable a security culture that is aligned to the business and make security elastic, flexible, and nimble to maintain the business processes.

Hire or Develop a World-Class Chief Information Security Officer (CISO)

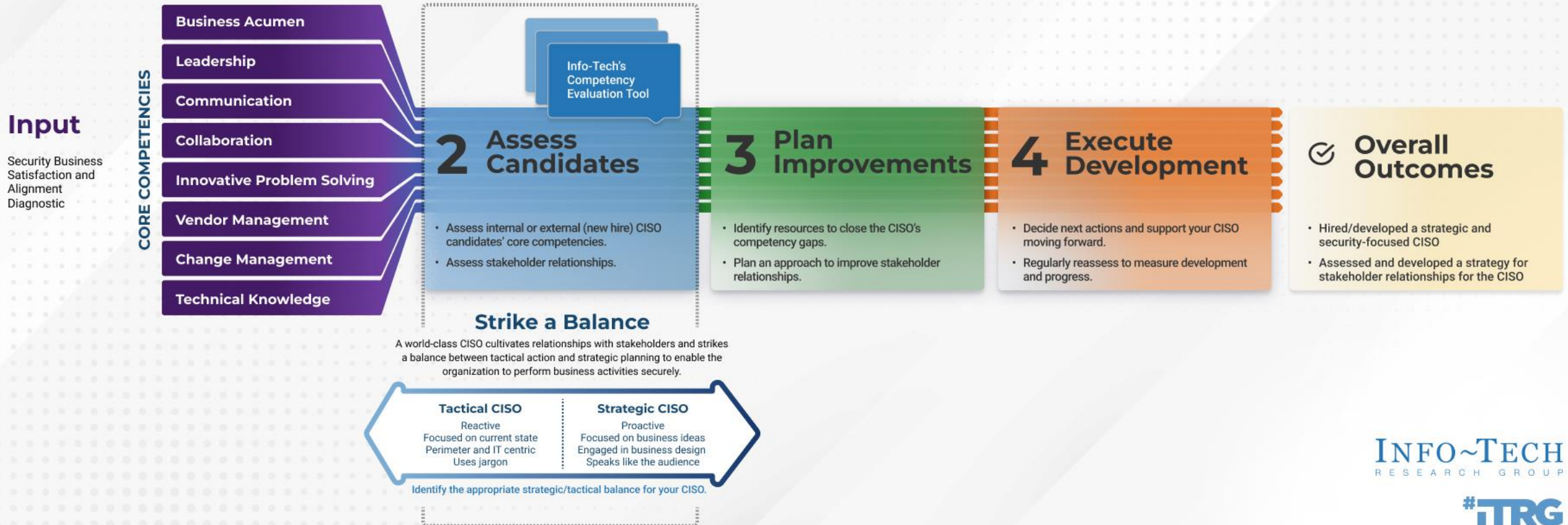
Find a strategic and security-focused champion for your business.

Problem

CEOs/CXOs looking to hire or develop a chief information security officer (CISO) or senior security leader may not be sure where to start.

Without strong security leadership, organizations will have difficulty optimizing their security plans and moving from a tactical position to a more strategic one.

1 Understand What Your Organization Needs in a CISO



Info-Tech's methodology to Develop or Hire a World-Class CISO

	1. Launch	2. Assess	3. Plan	4. Execute
Phase Steps	<ol style="list-style-type: none"> Understand the core competencies Measure security and business satisfaction and alignment 	<ol style="list-style-type: none"> Assess stakeholder relationships Assess core competencies 	<ol style="list-style-type: none"> Identify resources to address your CISO's competency gaps Plan an approach to improve stakeholder relationships 	<ol style="list-style-type: none"> Decide next actions and support your CISO moving forward Regularly reassess to measure development and progress
Phase Outcomes	<p>At the end of this phase, you will have:</p> <ul style="list-style-type: none"> Determined the current gaps in satisfaction and business alignment for your IT security program. Identified the desired qualities in a security leader, specific to your current organizational needs. 	<p>At the end of this phase, you will have:</p> <ul style="list-style-type: none"> Used the core competencies to help identify the ideal candidate. Identified areas for development in your new or existing CISO. Determined stakeholder relationships to cultivate. 	<p>At the end of this phase, you will have:</p> <ul style="list-style-type: none"> Created a high-level plan to address any deficiencies. Improved stakeholder relations. 	<p>At the end of this phase, you will have:</p> <ul style="list-style-type: none"> Created an action-based development plan, including relevant metrics, due dates, and identified stakeholders. This plan is the beginning, not the end. Continually reassessing your organizational needs and revisiting this blueprint's method will ensure ongoing development.

Key deliverable:



CISO Development Plan Template

The *CISO Development Plan Template* is used to map specific activities and time frames for competency development to address gaps and achieve your goal.

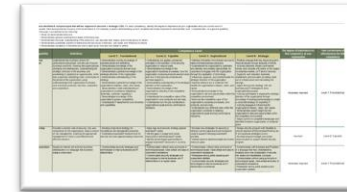
Area for Development	Item for Development	Next Action Required	Key Stakeholders / Owners	Target Outcome	Due Date	Completed
Process Maturity: Response & Recovery	Disaster Recovery	Read Info-Tech blueprint on Disaster Recovery		Disaster recovery and back-up policies in place		[Y/N]
Core Competencies: Communication	Improve Stakeholder Relationships	Email Bryce from finance to arrange lunch		Improved relationship with finance department		[Y/N]
Technology Maturity: Security Prevention	Asset Inventory	Write RFP for Asset Inventory system		All IT assets accounted for		[Y/N]
Core Competencies: Communication	Executive Communication	Take economics course to learn business language		Course completed		[Y/N]
Technology Maturity: Security Prevention	IAM system	Call Info-Tech to arrange call on IAM solutions		90% of employees entered into IAM system		[Y/N]
Process Maturity: Response & Recovery	Crisis Management	Meet with business stakeholders to discuss		Crisis Management policy written and in place		[Y/N]

Blueprint deliverables

Each step of this blueprint is accompanied by supporting deliverables to help you accomplish your goals:



CISO Core Competency Evaluation Tool



Assess the competency levels of a current or prospective CISO and identify areas for improvement.



Stakeholder Power Map Template

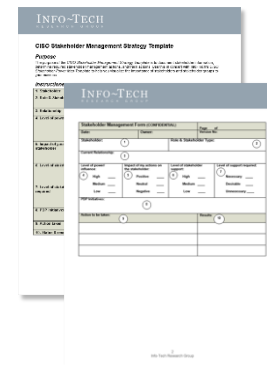


Visualize the importance of various stakeholders and their concerns.



Stakeholder Management Strategy Template

Document a plan to manage stakeholders and track actions.



Strategic competencies will benefit the organization and the CISO

Career development should not be seen as an individual effort. By understanding the personal core competencies that Info-Tech has identified, the individual wins by developing relevant new skills and the organization wins because the CISO provides increased value.

Organizational Benefits

- Increased alignment between security and business objectives
- Development of information security that is elastic, nimble, and flexible for the business
- Reduction in wasted efforts and resources, and improvement in efficiency of security and the organization as a whole
- True synergy between security and business stakeholders, where the goals of both groups are being met

Individual Benefits

- Increased opportunity as you become a trusted partner within your organization
- Improved relationships with peers and stakeholders
- Less resistance and more support for security initiatives
- More involvement and a stronger role for security at all levels of the organization

Measured value of a world-class CISO

Organizations with a CISO saw an average of \$145,000 less in data breach costs.¹

However, we aren't talking about hiring just any CISO. This blueprint seeks to develop your CISO's competencies and reach a new level of effectiveness.

Organizations invest a median of around \$375,000 annually in their CISO.² The CISO would have to be only 4% more effective to represent \$15,000 more value from this position. This would offset the cost of an Info-Tech workshop, and this conservative estimate pales in comparison to the tangible and intangible savings as shown below.

Your specific benefits will depend on many factors, but the value of protecting your reputation, adopting new and secure revenue opportunities, and preventing breaches cannot be overstated. There is a reason that investment in information security is on the rise: Organizations are realizing that the payoff is immense and the effort is worthwhile.

Tangible cost savings from having a world-class CISO

- Cost savings from **incident reduction**.
- Cost savings achieved through **optimizing information security investments**, resulting in savings from previously misdiagnosed issues.
- Cost savings from ensuring that dollars spent on security initiatives **support business strategy**.
- **More opportunities** to create new business processes through greater alignment between security and business.

Intangible cost savings from having a world-class CISO

- **Improved reputation** and brand equity achieved through a proper evaluation of the organization's security posture.
- **Continuous improvement** achieved through a good security assessment and measurement strategy.
- **Ability to plan for the future** since less security time will be spent firefighting and more time will be spent engaged with key stakeholders.

¹ IBM Security

² Heidrick & Struggles International, Inc.

Case Study

In the middle of difficulty lies opportunity

SOURCE

Kyle Kennedy

CISO, CyberSN.com

Challenge

The security program identified vulnerabilities at the database layer that needed to be addressed.

The decision was made to move to a new vendor. There were multiple options, but the best option in the CISO's opinion was a substantially more expensive service that provided more robust protection and more control features.

The CISO faced the challenge of convincing the board to make a financial investment in his IT security initiative to implement this new software.

Solution

The CISO knew he needed to express this challenge (and his solution!) in a way that was meaningful for the executive stakeholders.

He identified that the business has \$100 million in revenue that would move through this data stream. This new software would help to ensure the security of all these transactions, which they would lose in the event of a breach.

Furthermore, the CISO identified new business plans in the planning stage that could be protected under this initiative.

Results

The CISO was able to gain support for and implement the new database platform, which was able to protect current assets more securely than before. Also, the CISO allowed new revenue streams to be created securely.

This approach is the opposite of the cautionary tales that make news headlines, where new revenue streams are created before systems are put in place to secure them.

This proactive approach is the core of the world-class CISO.

Info-Tech offers various levels of support to best suit your needs

DIY Toolkit

"Our team has already made this critical project a priority, and we have the time and capability, but some guidance along the way would be helpful."

Guided Implementation

"Our team knows that we need to fix a process, but we need assistance to determine where to focus. Some check-ins along the way would help keep us on track."

Workshop

"We need to hit the ground running and get this project kicked off immediately. Our team has the ability to take this over once we get a framework and strategy in place."

Consulting

"Our team does not have the time or the knowledge to take this project on. We need assistance through the entirety of this project."

Diagnostics and consistent frameworks are used throughout all four options.

Guided Implementation

What does a typical GI on this topic look like?



Call #1: Review and discuss CISO core competencies.



Call #3: Discuss the *CISO Stakeholder Power Map Template* and the importance of relationships.



Call #5: Discuss results of the *CISO Core Competency Evaluation* and identify resources to close gaps.



Call #7: Discuss and create your CISO development plan and track your development



Call #2: Discuss Security Business Satisfaction and Alignment diagnostic results.



Call #4: Discuss the *CISO Core Competency Evaluation Tool*.



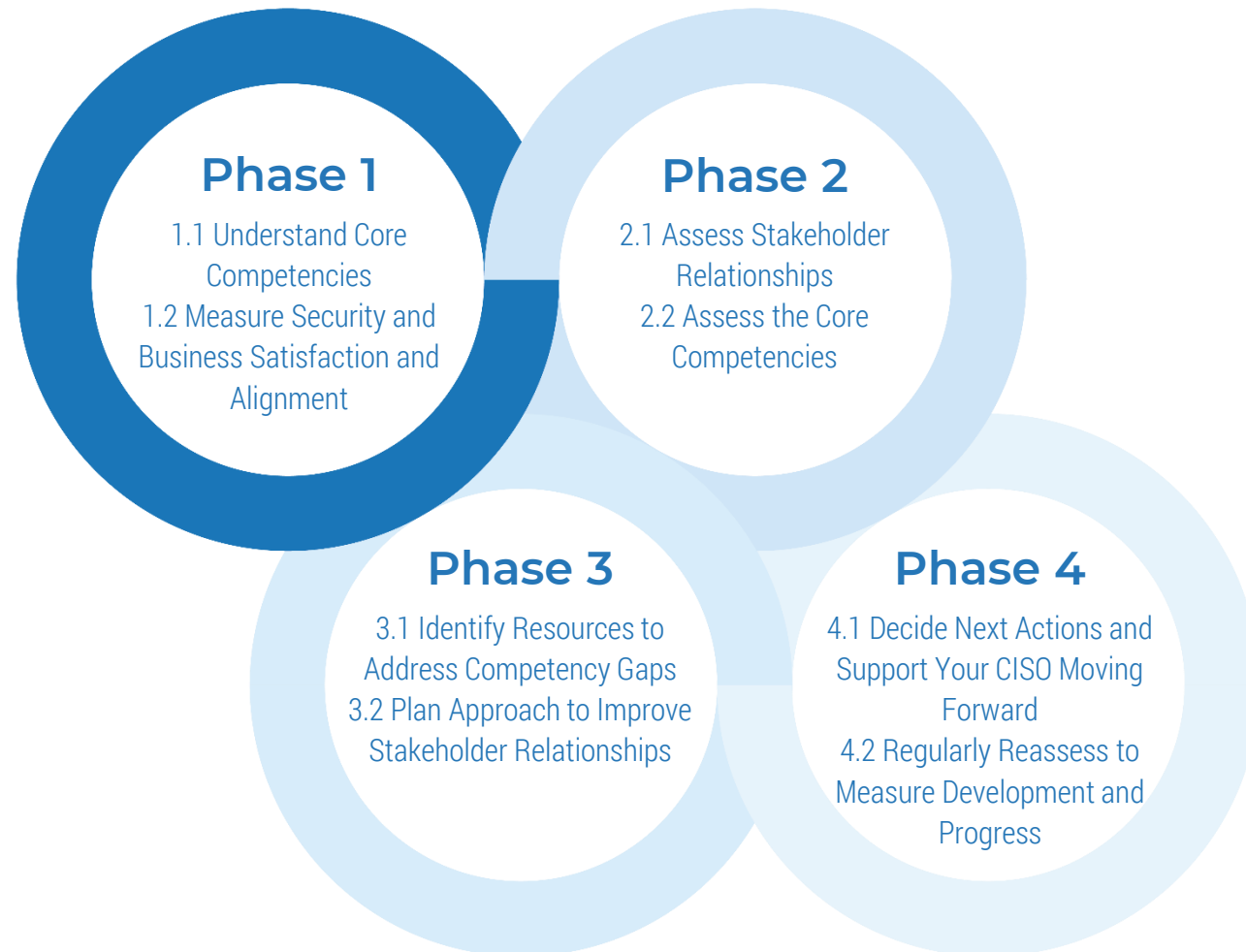
Call #6: Review organizational structure and key stakeholder relationships.

A Guided Implementation (GI) is a series of calls with an Info-Tech analyst to help implement our best practices in your organization.

A typical GI is 6 to 10 calls over the course of 3 to 6 months.

Phase 1

Launch



This phase will walk you through the following activities:

- Review and understand the core competencies of a world-class CISO.
- Launch your diagnostic survey.
- Evaluate current business satisfaction with IT security.
- Determine the competencies that are valuable to your IT security program's needs.

Hire or Develop a World-Class CISO

Case study

Mark Lester
InfoSec Manager, SC Ports Authority

An organization hires a new Information Security Manager into a static and well-established IT department.

Situation: The organization acknowledges the need for improved information security, but there is no framework for the Security Manager to make successful changes.

Challenges

- The Security Manager is an outsider in a company with well-established habits and protocols. He is tasked with revamping the security strategy to create unified threat management.
- Initial proposals for information security improvements are rejected by executives. It is a challenge to implement changes or gain support for new initiatives.

Next Steps

- The Security Manager will engage with individuals in the organization to learn about the culture and what is important to them.
- He will assess existing misalignments in the business so that he can target problems causing real pains to individuals.

Follow this case study throughout the deck to see this organization's results

Step 1.1

Understand the Core Competencies of a World-Class CISO

Activities

Review core competencies the security leader must develop to become a strategic business partner

Launch



This step involves the following participants:

- CEO or other executive seeking to hire/develop a CISO

or

- Current CISO seeking to upgrade capabilities

Outcomes of this step

Analysis and understanding of the eight strategic CISO competencies required to become a business partner

Core competencies

Info-Tech has identified eight core competencies affecting the CISO's progression to becoming a strategic business partner.

Business Acumen

A CISO must focus primarily on the needs of the business.

Leadership

A CISO must be a security leader and not simply a practitioner.

Communication

A CISO must have executive communication skills.

Technical Knowledge

A CISO must have a broad technical understanding.



Innovative Problem Solving

A good CISO doesn't just say "no," but rather finds creative ways to say "yes."

Vendor Management

Vendor and financial management skills are critical to becoming a strategic CISO.

Change Management

A CISO improves security processes by being an agent of change for the organization.

Collaboration

A CISO must be able to use alliances and partnerships strategically.

1.1 Understand the core competencies a CISO must focus on to become a strategic business partner

< 1 hour

Over the next few slides, review each world-class CISO core competency. In Step 1.2, you will determine which competencies are a priority for your organization.

CISO Competencies	Description
Business Acumen	<p>A CISO must focus primarily on the needs of the business and how the business works, then determine how to align IT security initiatives to support business initiatives. This includes:</p> <ul style="list-style-type: none">• Contributing to business growth with an understanding of the industry, core functions, products, services, customers, and competitors.• Understanding the business' strategic direction and allowing it to securely capitalize on opportunities.• Understanding the key drivers of business performance and the use of sound business practice.
Leadership	<p>A CISO must be a security leader, and not simply a practitioner. This requires:</p> <ul style="list-style-type: none">• Developing a holistic view of security, risk, and compliance for the organization.• Fostering a culture of risk management.• Choosing a strong team. Having innovative and reliable employees who do quality work is a critical component of an effective department.<ul style="list-style-type: none">○ This aspect involves <i>identifying</i> talent, <i>engaging</i> your staff, and <i>managing</i> their time and abilities.

1.1 Understand the core competencies (continued)

CISO Competencies	Description
Communication	<p>Many CISOs believe that using technical jargon impresses their business stakeholders – in fact, it only makes business stakeholders become confused and disinterested. A CISO must have executive communication skills. This involves:</p> <ul style="list-style-type: none">• Clearly communicating with business leaders in meaningful language (i.e. business, financial, social) that they understand by breaking down the complexities of IT security into simple and relatable concepts.• Not using acronyms or technological speak. Easy-to-understand translations will go a long way.• Strong public speaking and presentation abilities.
Technical Knowledge	<p>A CISO must have a broad technical understanding of IT security to oversee a successful security program. This includes:</p> <ul style="list-style-type: none">• Understanding key security and general IT technologies and processes.• Assembling a complementary team, because no individual can have deep knowledge in <i>all</i> areas.• Maintaining continuing education to stay on top of emerging technologies and threats.

1.1 Understand the core competencies (continued)

CISO Competencies	Description
Innovative Problem Solving	<p>A good CISO doesn't just say "no," but rather finds creative ways to say "yes." This can include:</p> <ul style="list-style-type: none">• Taking an active role in seizing opportunities created by emerging technologies.• Facilitating the secure implementation of new, innovative revenue models.• Developing solutions for complex business problems that require creativity and ingenuity.• Using information and technology to drive value around the customer experience.
Vendor Management	<p>With the growing use of "anything as a service," negotiation, vendor, and financial management skills are critical to becoming a strategic CISO.</p> <ul style="list-style-type: none">• The CISO must be able to evaluate service offerings and secure favorable contracts with the right provider. It is about extracting the maximum value from vendors for the dollars you are spending.• Vendor products must be aligned with future business plans to create maximum ongoing value.• The CISO must develop financial management skills. This includes the ability to calculate total cost of ownership, return on investment, and project spending over multiyear business plans.

1.1 Understand the core competencies (continued)

CISO Competencies	Description
Change Management	<p>A world-class CISO improves security processes by being an agent of change for the organization. This involves:</p> <ul style="list-style-type: none">• Leading, guiding, and motivating teams to adopt a responsible risk management culture.• Communicating important and complex ideas in a persuasive way.• Demonstrating an ability to change themselves and taking the initiative in adopting more efficient behaviors.• Handling unplanned change, such as unforeseen attacks or personnel changes, in a professional and proactive manner.
Collaboration	<p>A CISO must be able to use alliances and partnerships strategically to benefit both the business and themselves. This includes:</p> <ul style="list-style-type: none">• Identifying formal and informal networks and constructive relationships to enable security development.• Leveraging stakeholders to influence positive outcomes for the organization.• Getting out of the IT or IT security sphere and engaging relationships in diverse areas of the organization.

Step 1.2

Evaluate satisfaction and alignment between the business and IT security

Activities

- Conduct the Information Security Business Satisfaction and Alignment diagnostic
- Use your results as input into the *CISO Core Competency Evaluation Tool*

Launch



This step involves the following participants:

- CEO or other executive seeking to hire/develop a CISO
- or
- Current CISO seeking to upgrade capabilities

Outcomes of this step

Determine current gaps in satisfaction and alignment between information security and your organization.

If seeking to hire/develop a CISO: Your diagnostic results will help develop a profile of the ideal CISO candidate to use as a hiring and interview guide.

If developing a current CISO, use your diagnostic results to identify existing competency gaps and target them for improvement.

For the CISO seeking to upgrade capabilities: Use the core competencies guide to self-assess and identify competencies that require improvement.

1.2 Get started by conducting Info-Tech's Information Security Business Satisfaction and Alignment diagnostic

Suggested Time: One week for distribution, completion, and collection of surveys
 One-hour follow-up with an Info-Tech analyst


The primary goal of IT security is to protect the organization from threats. This does not simply mean bolting everything down, but it means enabling business processes securely. To do this effectively requires alignment between IT security and the overall business.

- Once you have completed the diagnostic, call Info-Tech to review your results with one of our analysts.
- The results from this assessment will provide insights to inform your entries in the *CISO Core Competency Evaluation Tool*.



Info-Tech Insight

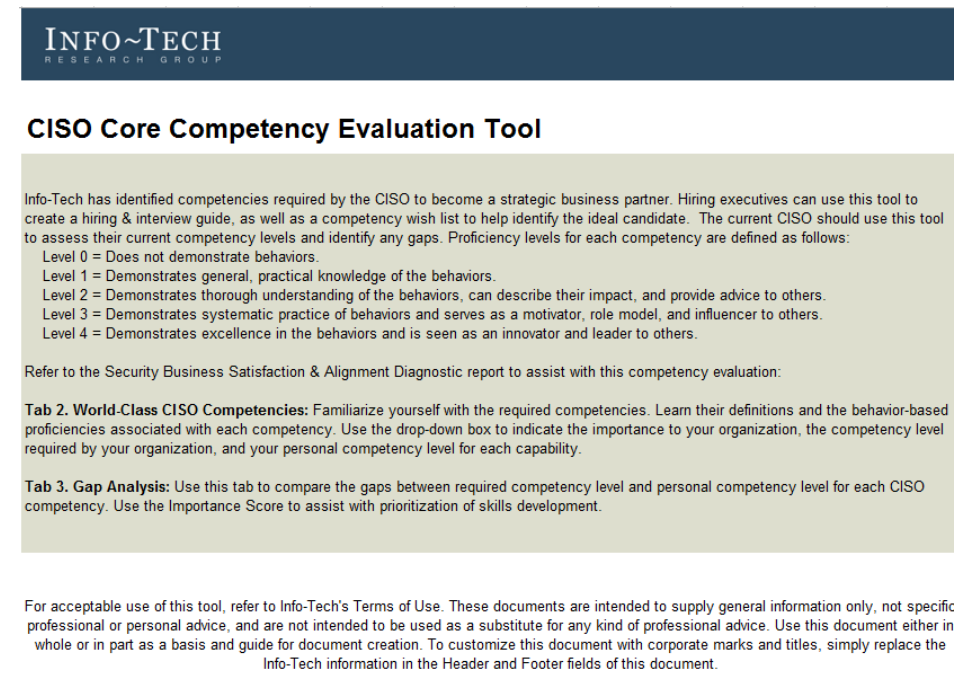
Focus on the high-priority competencies for your organization. You may find a candidate with perfect 10s across the board, but a more pragmatic strategy is to find someone with strengths that align with your needs. If there are other areas of weakness, then target those areas for development.

 Call an analyst to review your results and provide you with recommendations.

1.2 Use Info-Tech's *CISO Core Competency Evaluation Tool* to understand your organizational needs

After completing the Info-Tech diagnostic, use the [CISO Core Competency Evaluation Tool](#) to determine which CISO competencies are a priority *for your organization*.

- Your diagnostic results will indicate where your information security program is aligned well or poorly with your business.
- For example, the diagnostic may show significant misalignment between information security and executives over the level of external compliance. The CISO behavior that would contribute to solving this is **aligning security enablement with business requirements**.
 - This misalignment may be due to a misunderstanding by either party. The competencies that will contribute to resolving this are **communication, technical knowledge, and business acumen**.
 - This mapping method is what will be used to determine which competencies are most important for *your* needs at the present moment.



INFO~TECH
RESEARCH GROUP

CISO Core Competency Evaluation Tool

Info-Tech has identified competencies required by the CISO to become a strategic business partner. Hiring executives can use this tool to create a hiring & interview guide, as well as a competency wish list to help identify the ideal candidate. The current CISO should use this tool to assess their current competency levels and identify any gaps. Proficiency levels for each competency are defined as follows:

- Level 0 = Does not demonstrate behaviors.
- Level 1 = Demonstrates general, practical knowledge of the behaviors.
- Level 2 = Demonstrates thorough understanding of the behaviors, can describe their impact, and provide advice to others.
- Level 3 = Demonstrates systematic practice of behaviors and serves as a motivator, role model, and influencer to others.
- Level 4 = Demonstrates excellence in the behaviors and is seen as an innovator and leader to others.

Refer to the Security Business Satisfaction & Alignment Diagnostic report to assist with this competency evaluation:

Tab 2. World-Class CISO Competencies: Familiarize yourself with the required competencies. Learn their definitions and the behavior-based proficiencies associated with each competency. Use the drop-down box to indicate the importance to your organization, the competency level required by your organization, and your personal competency level for each capability.

Tab 3. Gap Analysis: Use this tab to compare the gaps between required competency level and personal competency level for each CISO competency. Use the Importance Score to assist with prioritization of skills development.

For acceptable use of this tool, refer to Info-Tech's Terms of Use. These documents are intended to supply general information only, not specific professional or personal advice, and are not intended to be used as a substitute for any kind of professional advice. Use this document either in whole or in part as a basis and guide for document creation. To customize this document with corporate marks and titles, simply replace the Info-Tech information in the Header and Footer fields of this document.



Download the *CISO Core Competency Evaluation Tool*

1.2 Use Info-Tech's *CISO Core Competency Evaluation Tool* to understand your organizational needs

After completing the Info-Tech diagnostic, use the [CISO Core Competency Evaluation Tool](#) to determine which CISO competencies are a priority *for your organization*.

1. Starting on **Tab 2: CISO Core Competencies**, use your understanding of each competency from section 1.1 along with the definitions described in the tool.
 - For each competency, assign a **degree of importance** using the drop-down menu in the second column from the right.
 - Importance ratings will range from **not at all important** at the low end to **critically important** at the high end.
 - Your importance score will be influenced by several factors, including:
 - The current alignment of your information security department.
 - Your organizational security posture.
 - The size and structure of your organization.
 - The existing skills and maturity within your information security department.

INFO~TECH
RESEARCH GROUP

CISO Core Competency Evaluation Tool

Info-Tech has identified competencies required by the CISO to become a strategic business partner. Hiring executives can use this tool to create a hiring & interview guide, as well as a competency wish list to help identify the ideal candidate. The current CISO should use this tool to assess their current competency levels and identify any gaps. Proficiency levels for each competency are defined as follows:

- Level 0 = Does not demonstrate behaviors.
- Level 1 = Demonstrates general, practical knowledge of the behaviors.
- Level 2 = Demonstrates thorough understanding of the behaviors, can describe their impact, and provide advice to others.
- Level 3 = Demonstrates systematic practice of behaviors and serves as a motivator, role model, and influencer to others.
- Level 4 = Demonstrates excellence in the behaviors and is seen as an innovator and leader to others.

Refer to the Security Business Satisfaction & Alignment Diagnostic report to assist with this competency evaluation:

Tab 2. World-Class CISO Competencies: Familiarize yourself with the required competencies. Learn their definitions and the behavior-based proficiencies associated with each competency. Use the drop-down box to indicate the importance to your organization, the competency level required by your organization, and your personal competency level for each capability.

Tab 3. Gap Analysis: Use this tab to compare the gaps between required competency level and personal competency level for each CISO competency. Use the Importance Score to assist with prioritization of skills development.

For acceptable use of this tool, refer to Info-Tech's Terms of Use. These documents are intended to supply general information only, not specific professional or personal advice, and are not intended to be used as a substitute for any kind of professional advice. Use this document either in whole or in part as a basis and guide for document creation. To customize this document with corporate marks and titles, simply replace the Info-Tech information in the Header and Footer fields of this document.



Download the *CISO Core Competency Evaluation Tool*

1.2 Use Info-Tech's *CISO Core Competency Evaluation Tool* to understand your organizational needs

After completing the Info-Tech diagnostic, use the [CISO Core Competency Evaluation Tool](#) to determine which CISO competencies are a priority for your organization.

2. Still on **Tab 2. CISO Core Competencies**, you will now assign a **current level of effectiveness** for each competency.
 - This will range from **foundational** at a low level of effectiveness up to **capable**, then **inspirational**, and at the highest rating, **transformational**.
 - Again, this rating will be very specific to your organization, depending on your structure and your current employees.
 - Fundamentally, these scores will reflect what you want to improve in the area of information security. This is not an absolute scale, and it will be influenced by what skills you want to support your goals and direction as an organization.

INFO~TECH
RESEARCH GROUP

CISO Core Competency Evaluation Tool

Info-Tech has identified competencies required by the CISO to become a strategic business partner. Hiring executives can use this tool to create a hiring & interview guide, as well as a competency wish list to help identify the ideal candidate. The current CISO should use this tool to assess their current competency levels and identify any gaps. Proficiency levels for each competency are defined as follows:

- Level 0 = Does not demonstrate behaviors.
- Level 1 = Demonstrates general, practical knowledge of the behaviors.
- Level 2 = Demonstrates thorough understanding of the behaviors, can describe their impact, and provide advice to others.
- Level 3 = Demonstrates systematic practice of behaviors and serves as a motivator, role model, and influencer to others.
- Level 4 = Demonstrates excellence in the behaviors and is seen as an innovator and leader to others.

Refer to the Security Business Satisfaction & Alignment Diagnostic report to assist with this competency evaluation:

Tab 2. World-Class CISO Competencies: Familiarize yourself with the required competencies. Learn their definitions and the behavior-based proficiencies associated with each competency. Use the drop-down box to indicate the importance to your organization, the competency level required by your organization, and your personal competency level for each capability.

Tab 3. Gap Analysis: Use this tab to compare the gaps between required competency level and personal competency level for each CISO competency. Use the Importance Score to assist with prioritization of skills development.

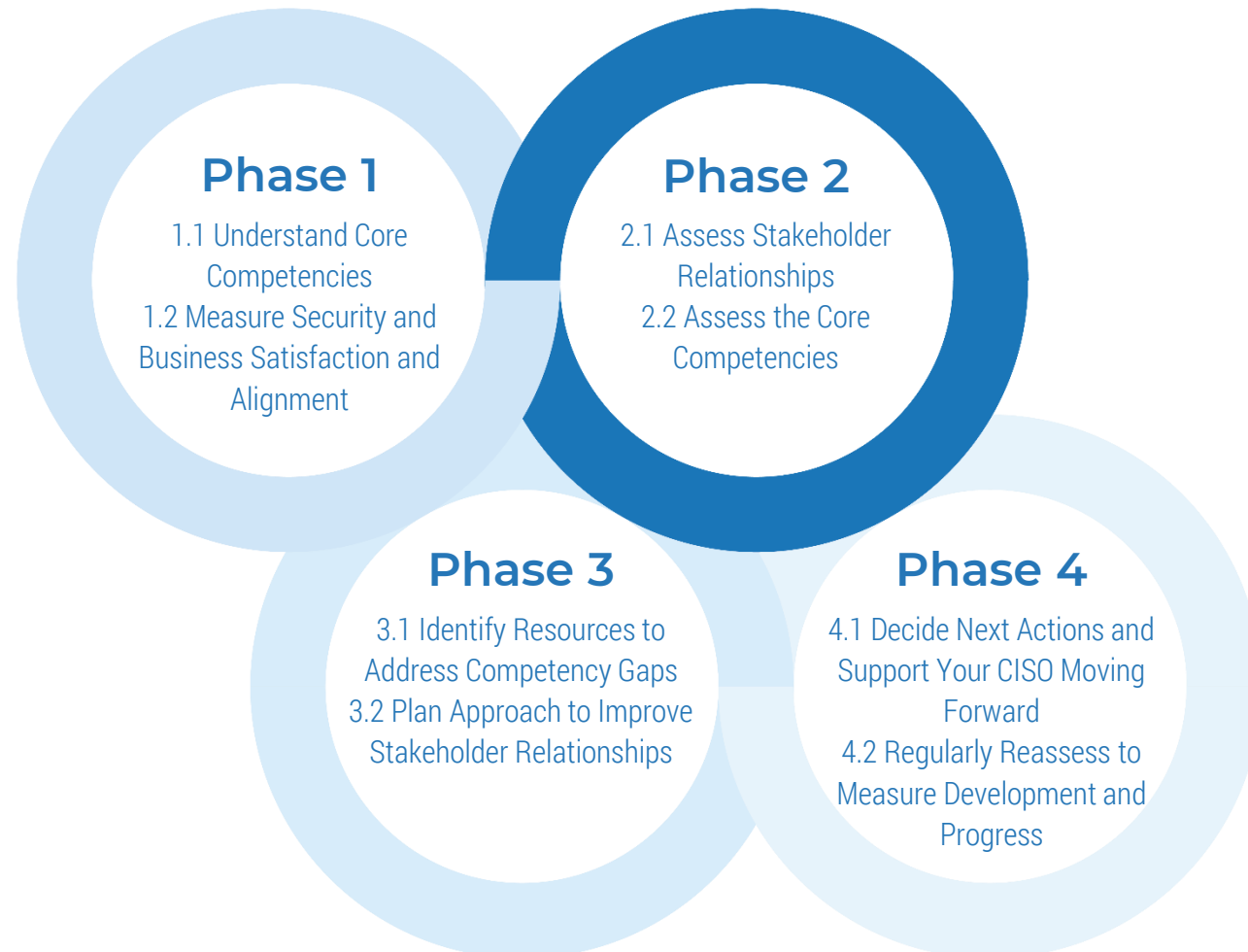
For acceptable use of this tool, refer to Info-Tech's Terms of Use. These documents are intended to supply general information only, not specific professional or personal advice, and are not intended to be used as a substitute for any kind of professional advice. Use this document either in whole or in part as a basis and guide for document creation. To customize this document with corporate marks and titles, simply replace the Info-Tech information in the Header and Footer fields of this document.



Download the *CISO Core Competency Evaluation Tool*

Phase 2

Assess



This phase will walk you through the following activities:

- Use the *CISO Core Competency Evaluation Tool* to create and implement an interview guide.
- Assess and analyze the core competencies of your prospective CISOs. Or, if you are a current CISO, use the *CISO Core Competency Evaluation Tool* as a self-analysis and identify areas for personal development.
- Evaluate the influence, impact, and support of key executive business stakeholders using the *CISO Stakeholder Power Map Template*.

Hire or Develop a World-Class CISO

Case study

Mark Lester
InfoSec Manager, SC Ports Authority

The new Security Manager engages with employees to learn the culture.

Outcome: Understand what is important to individuals in order to create effective collaboration.
People will engage with a project if they can relate it to something they value.

Actions

- The Security Manager determines that he must use low-cost small wins to integrate with the organizational culture and create trust and buy-in and investment will follow.
- The Security Manager starts a monthly newsletter to get traction across the organization, create awareness of his mandate to improve information security, and establish himself as a trustworthy partner.

Next Steps

- The Security Manager will identify specific ways to engage and change the culture.
- Create a persuasive case for investing in information security based on what resonates with the organization.

Follow this case study throughout the deck to see this organization's results

Step 2.1

Identify key stakeholders for the CISO and assess current relationships

Activities

Evaluate the power, impact, and support of key stakeholders

Assess



This step involves the following participants:

- CEO or other executive seeking to hire/develop a CISO
- or
- Current CISO seeking to upgrade capabilities

Outcomes of this step

- Power map of executive business stakeholders
- Evaluation of each stakeholder in terms of influence, impact, and current level of support

Identify key stakeholders who own business processes that intersect with security processes

Info-Tech Insight

Most organizations don't exist for the sole purpose of doing information security. For example, if your organization is in the business of selling pencils, then information security is in business to enable the selling of pencils. All the security in the world is meaningless if it doesn't enable your primary business processes. The CISO must always remember the fundamental goals of the business.

The above insight has two implications:

1. The CISO needs to understand the key business processes and who owns them, because these are the people they will need to collaborate with. Like any C-level, the CISO should be one of the most knowledgeable people in the organization regarding business processes.
2. Each of these stakeholders stands to win or lose depending on the performance of their process, and they can act to either block or enable your progress.
 - To work effectively with these stakeholders, you must learn what is important to them, and pose your initiatives so that you *both* benefit.

When people are not receptive to the CISO, it's usually because the CISO has not been part of the discussion when plans were being made. This is the heart of proactivity.

You need to be involved from the start ... from the earliest part of planning.

The job is not to come in late and say "No" ... the job is to be involved early and find creative and intelligent ways to say "Yes."

The CISO needs to be the enabling security asset that drives business.

– Elliot Lewis, CEO at Keyavi Data

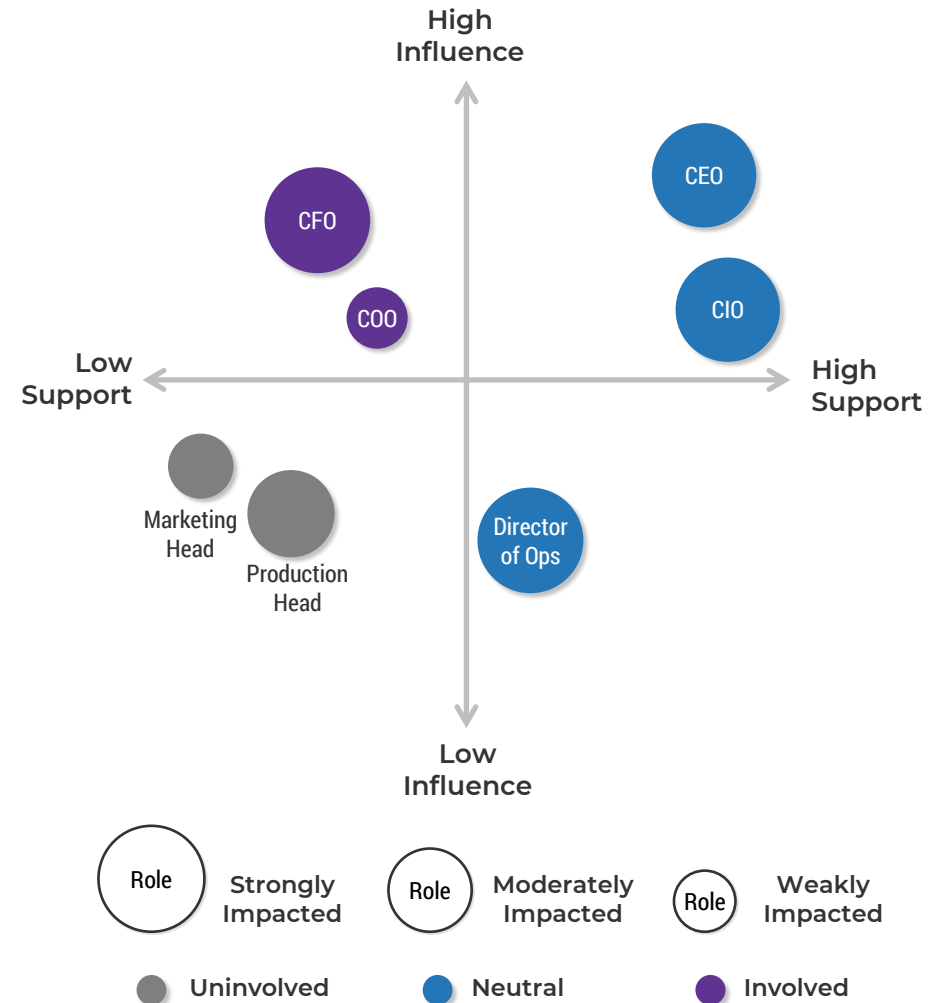
Evaluate the importance of business stakeholders and the support necessary from them

The [CISO Stakeholder Power Map Template](#) is meant to provide a visualization of the CISO's relationships within the organization. This should be a living document that can be updated throughout the year as relationships develop and the structure of an organization changes.

At a glance, this tool should show:

- How influential each stakeholder is within the company.
- How supportive they currently are of the CISO's initiatives.
- How strongly each person is impacted by IT security activities.

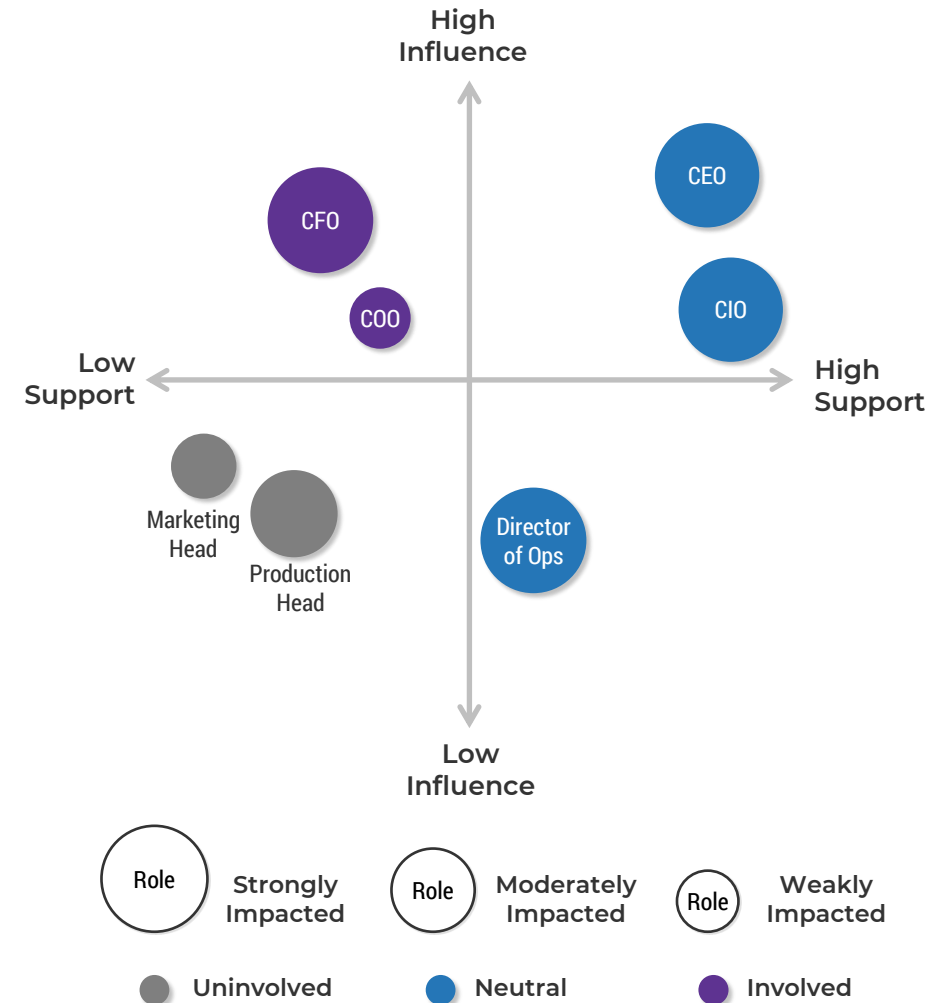
Once this tool has been created, it provides a good reference as the CISO works to develop lagging relationships. It shows the landscape of influence and impact within the organization, which may help to guide the CISO's strategy in the future.



Download the [CISO Stakeholder Power Map Template](#)

Evaluate the importance of business stakeholders and the support necessary from them

1. Identify key stakeholders.
 - a. Focus on owners of important business processes.
2. Evaluate and map each stakeholder in terms of:
 - a. **Influence** (up/down)
 - b. **Support** (left/right)
 - c. **Impact** (size of circle)
 - d. **Involvement** (color of circle)
3. Decide whether the level of support from each stakeholder needs to change to facilitate success.



Info-Tech Insight

Some stakeholders must work closely with your incoming CISO. It is worth consideration to include these individuals in the interview process to ensure you will have partners that can work well together. This small piece of involvement early on can save a lot of headache in the future.

Where can you find your desired CISO?

Once you know which competencies are a priority in your new CISO, the next step is to decide where to start looking. This person may **already exist** in your company.



Internal

Take some time to review your current top information security employees or managers. It may be immediately clear that certain people will or will not be suitable for the CISO role. For those that have potential, proceed to Step 2.2 to map their competencies.



Recruitment

If you do not have any current employees that will fit your new CISO profile, or you have other reasons for wanting to bring in an outside individual, you can begin the recruitment process. This could start by posting the position for applications or by identifying and targeting specific candidates.



Ready to start looking for your ideal candidate?
You can use Info-Tech's *Chief Information Security Officer* job description template.



Use the CISO job description template

Alternatives to hiring a CISO

Small organizations are less able to muster the resources required to find and retain a CISO,



Technical Counselor Seat

In addition to having access to our research and consulting services, you can acquire a Technical Counselor Seat from our Security & Risk practice, where one of our senior analysts would serve with you on a retainer. You may find that this option saves you the expense of having to hire a new CISO altogether.



Virtual CISO

A virtual CISO, or vCISO, is essentially a “CISO as a service.” A vCISO provides an organization with an experienced individual that can, on a part-time basis, lead the organization’s security program through policy and strategy development.

Why would an organization consider a vCISO?

- A vCISO can provide services that are flexible, technical, and strategic and that are based on the specific requirements of the organization.
- They can provide a small organization with program maturation within the organization’s resources.
- They can typically offer depth of experience beyond what a small business could afford if it were to pursue a full-time CISO.

Source: Georgia State University

Why would an organization not consider a vCISO?

- The vCISO’s attention is divided among their other clients.
- They won’t feel like a member of your organization.
- They won’t have a deep understanding of your systems and processes.

Source: InfoSec Insights by Sectigo Store

Step 2.2

Assess CISO candidates and evaluate their current competency

Activities

Assess CISO candidates in terms of desired core competencies

or

Self-assess your personal core competencies

Assess



This step involves the following participants:

- CEO or other executive seeking to hire/develop a CISO
- or
- Current CISO seeking to upgrade capabilities
- and
- Any key stakeholders or collaborators you choose to include in the assessment process

Outcomes of this step

- You have assessed your requirements for a CISO candidate.
- The process of hiring is under way, and you have decided whether to **hire** a CISO, **develop** a CISO, or consider a Counselor Seat as another option.

2.2 Use Info-Tech's *CISO Core Competency Evaluation Tool* to assess your CISO candidate

Use the *Desired Competency* and *Candidate's Competency* cells to enter the target and current competency for your new CISO.

Current Organizational Competency and Importance are imported automatically from Tab 2.

Capability	Current Organizational Competency Level	Importance Score	Desired Competency Level	CISO Candidate's Competency Level	Candidate Suitability
Business Acumen	Level 1: Foundational	Not at all important (or not applicable)	Level 2: Capable	Level 1: Foundational	Competent
Leadership	Level 2: Capable	Important	Level 3: Inspirational	Level 2: Capable	Competent
Communication Skills	Level 1: Foundational	Moderately important	Level 2: Capable	Level 1: Foundational	Competent
Technical Knowledge	Level 2: Capable	Important	Level 1: Foundational	Level 3: Inspirational	Ideal
Innovative Problem Solving	Level 1: Foundational	Critically important	Level 2: Capable	Level 1: Foundational	Competent
Vendor Management	Level 2: Capable	Critically important	Level 3: Inspirational	Level 3: Inspirational	Ideal
Change Management	Level 4: Transformational	Important	Level 4: Transformational	Level 3: Inspirational	Needs Development
Collaboration	Level 4: Transformational	Critically important	Level 4: Transformational	Level 3: Inspirational	Needs Development

Info-Tech Insight

The most important competencies should be your focus. Unless you are lucky enough to find a candidate that is perfect across the board, you will see some areas that are not ideal. Don't forget the importance you assigned to each competency. If a candidate is ideal in the most critical areas, you may not mind that some development is needed in a less important area.

↓ Download the *CISO Core Competency Evaluation Tool*

↑ Use the *Suitability* column to determine which competencies should be prioritized.

2.2 Use Info-Tech's *CISO Core Competency Evaluation Tool* to evaluate your candidates

After deciding the importance of and requirements for each competency in Phase 1, assess your CISO candidates.

Your first pass on this tool will be to look at internal candidates. This is the **develop a CISO** option.

1. In the previous phase, you rated the *Importance* and *Current Effectiveness* for each competency in Tab 2. CISO Core Competencies. In this step, use Tab 3. Gap Analysis to enter a **Minimum Level** and a **Desired Level** for each competency. Keep in mind that it may be unrealistic to expect a candidate to be fully developed in all aspects.
2. Next, enter a rating for your candidate of interest for each of the eight competencies.
3. This scorecard will generate an overall suitability score for the candidate. The **color** of the output (from red to green) indicates the suitability, and the **intensity** of the color indicates the importance you assigned to that competency.

Capability	Current Organizational Competency Level	Importance Score	Desired Competency Level	CISO Candidate's Competency Level	Candidate Suitability
Business Acumen	Level 1: Foundational	Not at all important (or not applicable)	Level 2: Capable	Level 1: Foundational	Competent
Leadership	Level 2: Capable	Important	Level 3: Inspirational	Level 2: Capable	Competent
Communication Skills	Level 1: Foundational	Moderately important	Level 2: Capable	Level 1: Foundational	Competent
Technical Knowledge	Level 2: Capable	Important	Level 1: Foundational	Level 3: Inspirational	Ideal
Innovative Problem Solving	Level 1: Foundational	Critically important	Level 2: Capable	Level 1: Foundational	Competent
Vendor Management	Level 2: Capable	Critically important	Level 3: Inspirational	Level 3: Inspirational	Ideal
Change Management	Level 4: Transformational	Important	Level 4: Transformational	Level 3: Inspirational	Needs Development
Collaboration	Level 4: Transformational	Critically important	Level 4: Transformational	Level 3: Inspirational	Needs Development

 [Download the *CISO Core Competency Evaluation Tool*](#)

2.2 Use Info-Tech's *CISO Core Competency Evaluation Tool* to evaluate your candidates

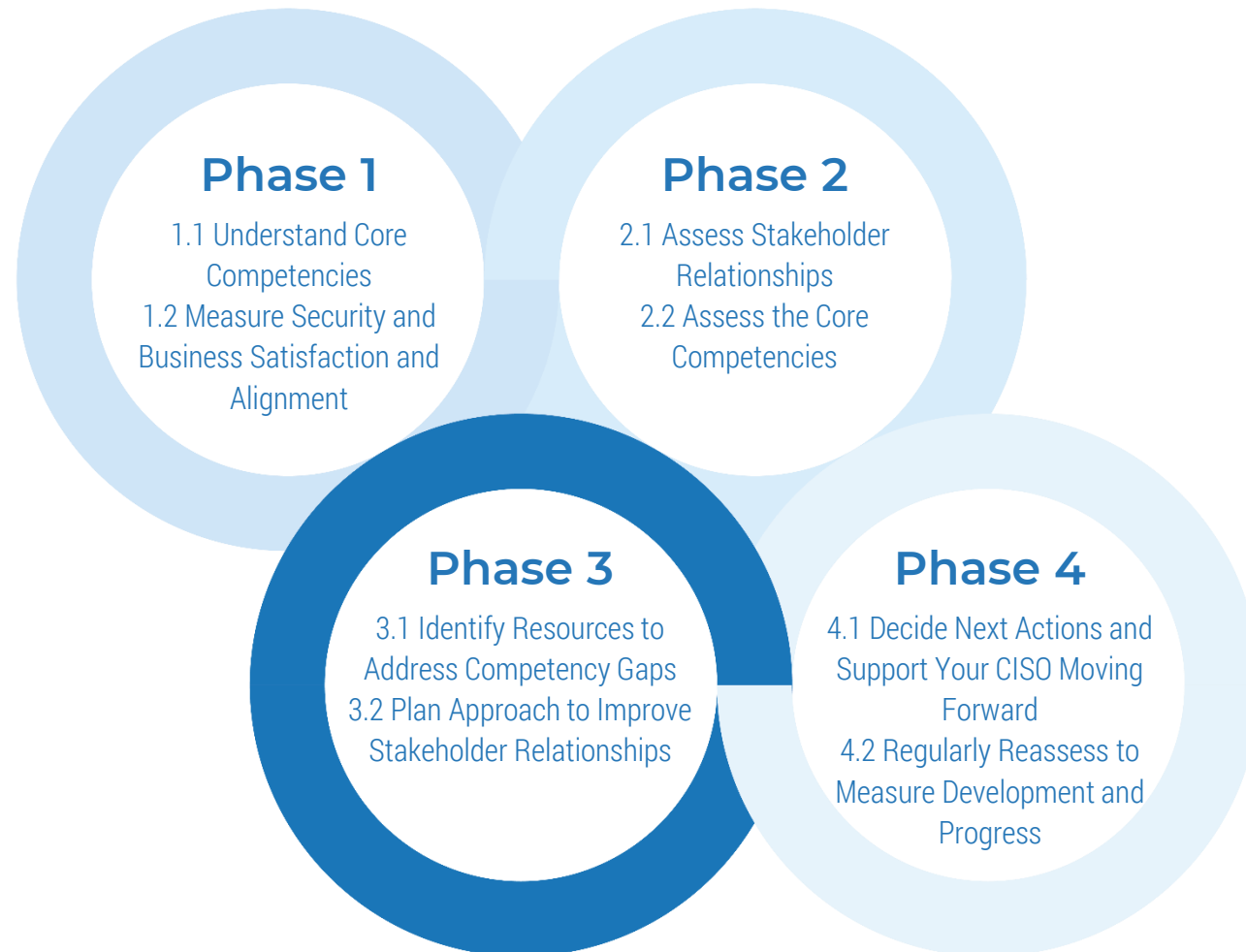
- If the internal search does not identify a suitable candidate, you will want to expand your search.
- Repeat the scoring process for external candidates until you find your new CISO.
- You may want to skip your external search altogether and instead contact Info-Tech for more information on our Counselor Seat options.

Capability	Current Organizational Competency Level	Importance Score	Desired Competency Level	CISO Candidate's Competency Level	Candidate Suitability
Business Acumen	Level 1: Foundational	Not at all important (or not applicable)	Level 2: Capable	Level 1: Foundational	Competent
Leadership	Level 2: Capable	Important	Level 3: Inspirational	Level 2: Capable	Competent
Communication Skills	Level 1: Foundational	Moderately important	Level 2: Capable	Level 1: Foundational	Competent
Technical Knowledge	Level 2: Capable	Important	Level 1: Foundational	Level 3: Inspirational	Ideal
Innovative Problem Solving	Level 1: Foundational	Critically important	Level 2: Capable	Level 1: Foundational	Competent
Vendor Management	Level 2: Capable	Critically important	Level 3: Inspirational	Level 3: Inspirational	Ideal
Change Management	Level 4: Transformational	Important	Level 4: Transformational	Level 3: Inspirational	Needs Development
Collaboration	Level 4: Transformational	Critically important	Level 4: Transformational	Level 3: Inspirational	Needs Development


[Download the *CISO Core Competency Evaluation Tool*](#)

Phase 3

Plan



This phase will walk you through the following activities:

- Create a plan to develop your competency gaps.
- Construct and consider your organizational model.
- Create plan to cultivate key stakeholder relationships.

Hire or Develop a World-Class CISO

Case study

Mark Lester
InfoSec Manager, SC Ports Authority

The new Security Manager changes the security culture by understanding what is meaningful to employees.

Outcome: Engage with people on their terms. The CISO must speak the audience's language and express security terms in a way that is meaningful to the audience.

Actions

- The Security Manager identifies recent events where ransomware and social engineering attacks were successful in penetrating the organization.
- He uses his newsletter to create organization-wide discussion on this topic.
- This very personal example makes employees more receptive to the Security Manager's message, enabling the culture of risk management.

Next Steps

- The Security Manager will leverage his success in improving the information security culture and awareness to gain support for future initiatives.

Follow this case study throughout the deck to see this organization's results

Step 3.1

Identify resources for your CISO to remediate competency gaps

Activities

Create a plan to remediate competency gaps

Plan



This step involves the following participants:

- CEO or other executive seeking to hire/develop a CISO
 - The newly hired CISO
- or
- Current CISO seeking to upgrade capabilities

Outcomes of this step

- Identification of core competency deficiencies
- A plan to close the gaps

3.1 Close competency gaps with Info-Tech's *Cybersecurity Workforce Development Training*

Resources to close competency gaps

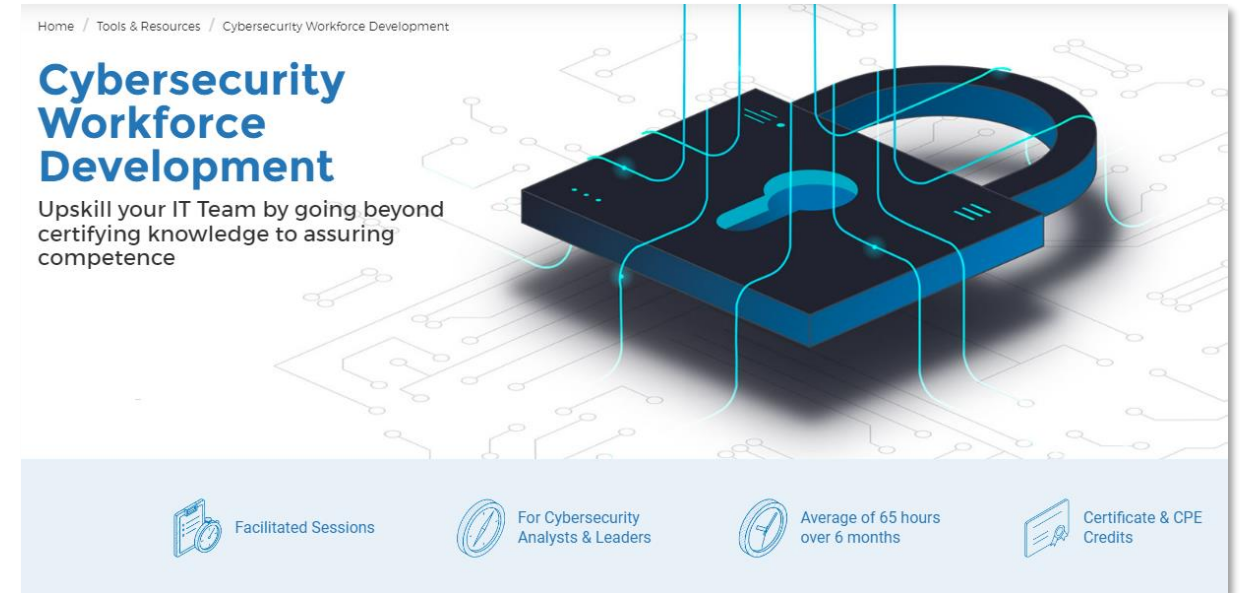
Info-Tech's Cybersecurity Workforce Training develops critical cybersecurity skills missing within your team and organization. The leadership track provides the same deep coverage of technical knowledge as the analyst track but adds hands-on support and has a focus on strategic business alignment, program management, and governance.

The program builds critical skills through:

- Standardized curriculum with flexible projects tailored to business needs
- Realistic cyber range scenarios
- Ready-to-deploy security deliverables
- Real assurance of skill development

Info-Tech Insight

Investing in a current employee that has the potential to be a world-class CISO may take less time, effort, and money than finding a unicorn.



Home / Tools & Resources / Cybersecurity Workforce Development

Cybersecurity Workforce Development

Upskill your IT Team by going beyond certifying knowledge to assuring competence

Facilitated Sessions

For Cybersecurity Analysts & Leaders

Average of 65 hours over 6 months

Certificate & CPE Credits



Learn more on the Cybersecurity Workforce Development webpage

3.1 Identify resources for your CISO to remediate competency gaps

< 2 hours

CISO Competencies	Description
Business Acumen	<p>Info-Tech Workshops & Blueprints</p> <ul style="list-style-type: none">• Document Your Business Architecture: Use business architecture to gain a clear understanding of the business strategy and align IT with the business.• Build an Information Security Strategy: Tailor best practices to effectively manage information security. <p>Actions/Activities</p> <ul style="list-style-type: none">• Take a business acumen course: Acumen Learning, What the CEO Wants You to Know: Building Business Acumen.• Meet with business stakeholders. Ask them to take you through the strategic plan for their department and then identify opportunities where security can provide support to help drive their initiatives.• Shadow another C-level executive. Understand how they manage their business unit and demonstrate an eagerness to learn.• Pursue an MBA or take a business development course.

3.1 Identify resources for your CISO to remediate competency gaps (continued)

< 2 hours

CISO Competencies	Description
Leadership	<p>Info-Tech Training and Blueprints</p> <ul style="list-style-type: none">• Improve IT Team Effectiveness: Four key factors to ensure IT teams are successful.• Build a Better Manager: Basic Management Skills: Offer tailored training that focuses on skill building and is aligned with measurable business goals to make your manager training a tangible success. <p>Action/Activities</p> <ul style="list-style-type: none">• Communicate your vision for security to your team. You will gain buy-in from your employees by including them in the creation of your program, and they will be instrumental to your success.

Info-Tech Insight

Surround yourself with great people. Insecure leaders surround themselves with mediocre employees that aren't perceived as a threat. Great leaders are supported by great teams, but you must choose that great team first.

3.1 Identify resources for your CISO to remediate competency gaps (continued)

< 2 hours

CISO Competencies	Description
Communication	<p>Info-Tech Workshops & Blueprints</p> <p><i>Build and Deliver an Optimized IT Update Presentation</i>: Show IT's value and relevance by dropping the technical jargon and speaking to the business in their terms.</p> <p><i>Master Your Security Incident Response Communications Program</i>: Learn how to talk to your stakeholders about what's going on when things go wrong.</p> <p><i>Develop a Security Awareness and Training Program That Empowers End Users</i>: Your weakest link is between the keyboard and the chair, so use engaging communication to create positive behavior change.</p> <p>Actions/Activities</p> <p>Learn to communicate in the language of your audience (whether business, finance, or social), and frame security solutions in terms that are meaningful to your listener.</p>
Technical Knowledge	<p>Actions/Activities</p> <ul style="list-style-type: none">• In many cases, the CISO is progressing from a strong technical background, so this area is likely a strength already.• However, as the need for executive skills are being recognized, many organizations are opting to hire a business or operations professional as a CISO. In this case, various Info-Tech blueprints across all our silos (e.g. Security, Infrastructure, CIO, Apps) will provide great value in understanding best practices and integrating technical skills with the business processes.• Pursue an information security leadership certification: GIAC, (ISC)², and ISACA are a few of the many organizations that offer certification programs.

3.1 Identify resources for your CISO to remediate competency gaps (continued)

< 2 hours

CISO Competencies	Description
Innovative Problem Solving	<p>Info-Tech Workshops & Blueprints</p> <ul style="list-style-type: none">• Kick-Start IT-Led Business Innovation: Start leading innovation now to demonstrate the art of the possible and build credibility as a strategic partner. <p>Actions/Activities</p> <ul style="list-style-type: none">• Sustain and Grow the Maturity of Innovation in Your Enterprise: Going to the next level of maturity for innovation.• Align disruptive technologies with ongoing business initiatives and the long-term outlook that the business has laid out.
Vendor Management	<p>Info-Tech Blueprints & Resources</p> <ul style="list-style-type: none">• Jump Start Your Vendor Management Initiative: Create and implement a vendor management framework to begin obtaining measurable results in 90 days.• SoftwareReviews has a variety of security-specific product and service reviews that help match you with the correct vendor for your needs. <p>Actions/Activities</p> <ul style="list-style-type: none">• Take a course in finance for nonfinancial executives: e.g. Finance and Accounting for the Nonfinancial Executive.• Attend vendor booths and info sessions at conferences. Review research on vendors and their products.

3.1 Identify resources for your CISO to remediate competency gaps (continued)

< 2 hours

CISO Competencies	Description
Change Management	<p>Info-Tech Blueprints</p> <ul style="list-style-type: none">• Optimize IT Change Management: Empower your team to prioritize and implement change according to business need and risk.• Master Organizational Change Management Practices: Ensure you don't just complete new projects but also realize the benefits. <p>Actions/Activities</p> <ul style="list-style-type: none">• Start with an easy-win project to create trust and support for your initiatives.
Collaboration	<p>Info-Tech Blueprints</p> <ul style="list-style-type: none">• Improve IT Team Effectiveness: Four key factors to ensure IT teams are successful. <p>Actions/Activities</p> <ul style="list-style-type: none">• Get out of your office. Have lunch with people from all areas of the business. Understanding the goals and the pains of employees throughout your organization will help you to design effective initiatives and cultivate support.• Be clear and honest about your goals. If people know what you are trying to do, then it is much easier for them to work with you on it. Being ambiguous or secretive creates confusion and distrust.

3.1 Create the CISO's personal development plan

- Use Info-Tech's [CISO Development Plan Template](#) to document key initiatives that will close previously identified competency gaps.
- The *CISO Development Plan Template* is used to map specific actions and time frames for competency development, with the goal of addressing competency gaps and helping you become a world-class CISO. This template can be used to document:
 - Core competency gaps
 - Security process gaps
 - Security technology gaps
 - Any other career/development goals
- If you have a coach or mentor, you should share your plan and report progress to that person. **Alternatively, call Info-Tech to speak with an executive advisor for support and advice.**
 - Toll-Free: 1-888-670-8889

What you will need to complete this exercise

- *CISO Core Competency Evaluation Tool* results
- Information Security Business Satisfaction and Alignment diagnostic results
- Insights gathered from business stakeholder interviews

INFO~TECH
RESEARCH GROUP

CISO Development Plan Template

How to Use This Template
A development plan represents a serious commitment to your career and achieving the milestones you need to move your role forward.

To use this template, identify the following:	Area for Development	Item for Development	Next Action Required	Key Stakeholders / Owners	Target Outcome	Due Date	Completed
The gaps identified in the CISO Core Competency Evaluation Tool	Process Maturity: Response & Recovery	Disaster Recovery	Read Info-Tech blueprint on Disaster Recovery		Disaster recovery and back-up policies in place		[Y/N]
For professional development	Core Competencies: Communication	Improve Stakeholder Relationships	Email Bryce from finance to arrange lunch		Improved relationship with finance department		[Y/N]
	Technology Maturity: Security Prevention	Asset Inventory	Write RFP for Asset Inventory system		All IT assets accounted for		[Y/N]
	Core Competencies: Communication	Executive Communication	Take economics course to learn business language		Course completed		[Y/N]
	Technology Maturity: Security Prevention	IAM system	Call Info-Tech to arrange call on IAM solutions		90% of employees entered into IAM system		[Y/N]
	Process Maturity: Response & Recovery	Crisis Management	Meet with business stakeholders to discuss		Crisis Management policy written and in place		[Y/N]

Step 3.2

Plan an approach to improve your relationships

Activities

- Review engagement strategies for different stakeholder types
- Create a stakeholder relationship development plan

Plan



This step involves the following participants:

- CEO or other executive seeking to hire/develop a CISO
 - The newly hired CISO
- or
- Current CISO seeking to upgrade capabilities

Outcomes of this step

- Stakeholder relationship strategy deliverable

Where should the CISO sit?

Where the CISO sits in the organization can have a big impact on the security program.

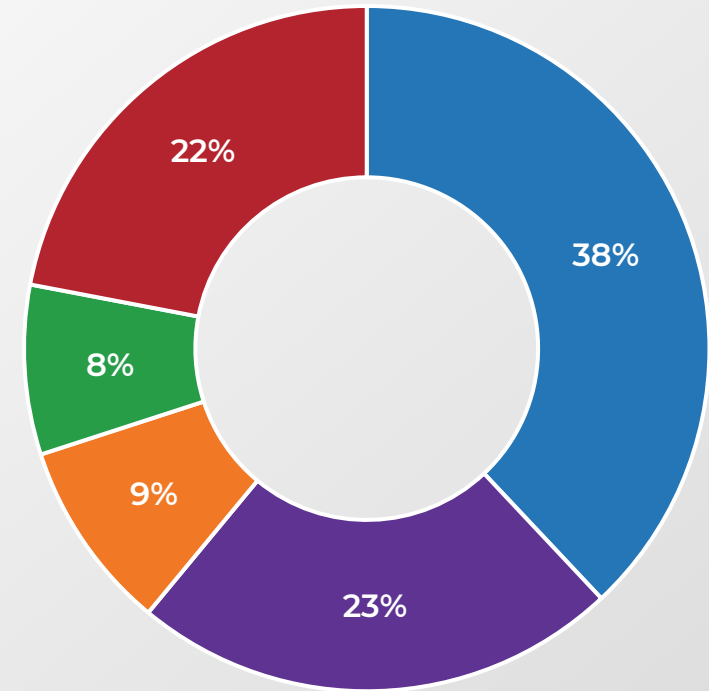
- Organizations with CISOs in the C-suite have a fewer security incidents.¹
- Organizations with CISOs in the C-suite generally have better IT ability.¹
- An organization whose CISO reports to the CIO risks conflict of interest.¹
- **51%** of CISOs believe their effectiveness can be hampered by reporting lines.²
- Only half of CISOs feel like they are in a position to succeed.²

A formalized security organizational structure assigns and defines the roles and responsibilities of different members around security. Use Info-Tech's blueprint *Implement a Security Governance and Management Program* to determine the best structure for your organization.



Download the *Implement a Security Governance and Management Program* blueprint

Who the CISO reports to, by percentage of organizations³

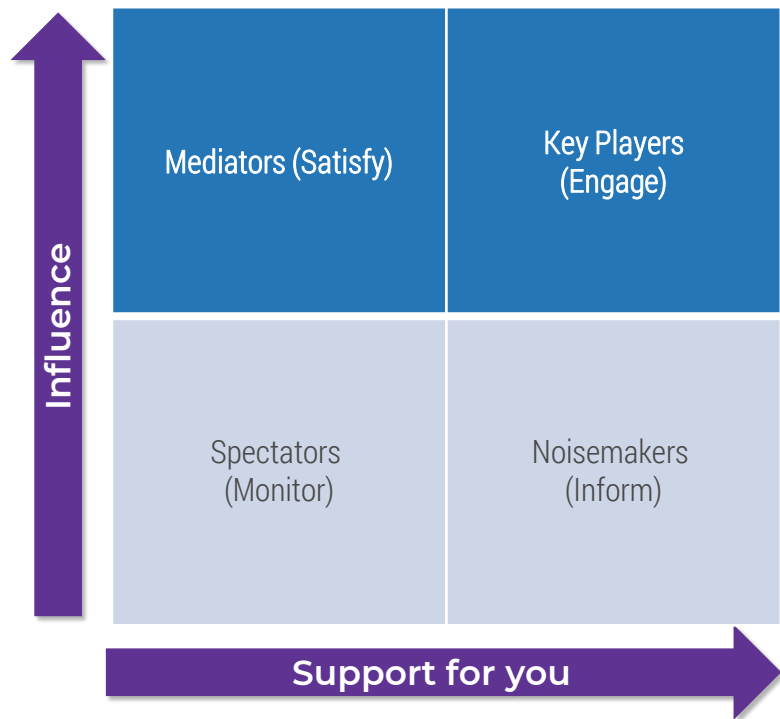


■ CIO ■ CTO or Global CISO ■ COO or CAO ■ CEO ■ Other

1. Journal of Computer Science and Information
2. Proofpoint
3. Heidrick & Struggles International, Inc

3.2 Make a plan to manage your key stakeholders

Managing stakeholders requires engagement, communication, and relationship management. To effectively collaborate and gain support for your initiatives, you will need to build relationships with your stakeholders. Take some time to review the stakeholder engagement strategies for different stakeholder types.



When building relationships, I find that what people care about most is getting their job done. We need to help them do this in the most secure way possible.

I don't want to be the "No" guy, I want to enable the business. I want to find to secure options and say, "Here is how we can do this."

– James Miller, Information Security Director, Xavier University



Download the *CISO Stakeholder Management Strategy Template*

Key players – Engage

Goal

Get **key players** to help champion your initiative and turn your detractors into supporters.

Keep It Positive

- Use their positive support to further your objectives and act as your foundation of support.
- Key players can help you build consensus among other stakeholders.
- Get supporters to be vocal in your town halls.
- Ask them to talk to other stakeholders over whom they have influence.

Action

Actively involve **key players** to take ownership.

Maintain a Close Relationship

- Get some quick wins early to gain and maintain stakeholder support and help convert them to your cause.
- Use their influence and support to help persuade blockers to see your point of view.
- Collaborate closely. Key players are tuned in to information streams that are important. Their advice can keep you informed and save you from being blindsided.
- Keep them happy. By definition, these individuals have a stake in your plans and can be affected positively or negatively. Going out of your way to maintain relationships can be well worth the effort.

Info-Tech Insight

Listen to your key players. They understand what is important to other business stakeholders, and they can provide valuable insight to guide your future strategy.

Mediators – Satisfy

Goal

Turn **mediators** into key players.

Keep It Positive

- Make stakeholders part of the conversation by consulting them for input on planning and strategy.
- Sample phrases:
 - “I’ve heard you have experience in this area. Do you have time to answer a few questions?”
 - “I’m making some decisions and I would value your thoughts. Can I get your perspective on this?”
- Enhance their commitment by being inclusive. Encourage their support whenever possible.

Action

Increase their support level.

Maintain a Close Relationship

- Make them feel acknowledged and solicit feedback.
- Listen to blockers with an open mind to understand their point of view. They may have valuable insight.
- Approach stakeholders on their individual playing fields.
 - They want to know that you understand their business perspective.
- Stubborn mediators might never support you. If consulting doesn’t work, keep them informed of important decision-making points and give them the opportunity to be involved if they choose to be.

Info-Tech Insight

Don’t dictate to stakeholders. Make them feel like valued contributors by including them in development and decision making. You don’t have to incorporate all their input, but it is essential that they feel respected and heard.

Noisemakers – Inform

Goal

Have **noisemakers** spread the word to increase their influence.

Keep It Positive

- Identify noisemakers who have strong relationships with key stakeholders and focus on them.
 - These individuals may not have decision-making power, but their opinions and advice may help to sway a decision in your favor.
- Look for opportunities to increase their influence over others.
- Put effort into maintaining the positive relationship so that it doesn't dwindle.

Action

Encourage **noisemakers** to influence key stakeholders.

Maintain a Close Relationship

- You already have this group's support, but don't take it for granted.
- Be proactive, pre-emptive, and transparent.
- Address issues or bad news early and be careful not to exaggerate their significance.
- Use one-on-one meetings to give them an opportunity to express challenges in a private setting.
- Show individuals in this group that you are a problem-solver:
 - "The implementation was great, but we discovered problems afterward. Here is what we're doing about it."

Spectators – Monitor

Goal

Keep **spectators** content and avoid turning them into detractors.

Keep It Positive

- A hands-on approach is not required with this group.
- Keep them informed with regular, high-altitude communications and updates.
- Use positive, exciting announcements to increase their interest in your initiatives.
- Select a good venue for generating excitement and assessing the mood of spectators.

Action

Keep them well informed.

Maintain a Close Relationship

- Spectators may become either supporters or blockers. Monitor them closely and keep in touch with them to stop these individuals from becoming blockers.
- Listen to questions from spectators carefully. View any engagement as an opportunity to increase participation from this group and generate a positive shift in interest.

3.2 Create the CISO's stakeholder management strategy

Develop a strategy to manage key stakeholders in order to drive your personal development plan initiatives.

- The purpose of the *CISO Stakeholder Management Strategy Template* is to document the results of the power mapping exercise, create a plan to proactively manage stakeholders, and track the actions taken.
- Use this in concert with Info-Tech's *CISO Stakeholder Power Map Template* to help visualize the importance of key stakeholders to your personal development. You will document:
 - Stakeholder role and type.
 - Current relationship with the stakeholder.
 - Level of power/influence and degree of impact.
 - Current and desired level of support.
 - Initiatives that require the stakeholder's engagement.
 - Actions to be taken – along with the status and results.

The image shows two overlapping pages of a document. The top page is the 'CISO Stakeholder Management Strategy Template' with a header 'INFO-TECH RESEARCH GROUP'. It contains a 'Purpose' section, 'Instructions' with a numbered list (1-10), and a 'Stakeholder Management Form (CONFIDENTIAL)'. The form has fields for 'Date', 'Client', 'Page ___ of ___', and 'Version No.'. It includes a table for 'Stakeholder' information with columns for 'Stakeholder', 'Role & Stakeholder Type', 'Current Relationship', 'Level of power/influence', 'Impact of the initiative on the stakeholder', 'Level of stakeholder support', and 'Level of support required'. Below this is a 'Security Initiatives' section, an 'Actions to be taken' table, and a 'Results' table. The bottom page is partially visible, showing the 'INFO-TECH RESEARCH GROUP' logo and the page number '2'.

What you will need to complete this exercise

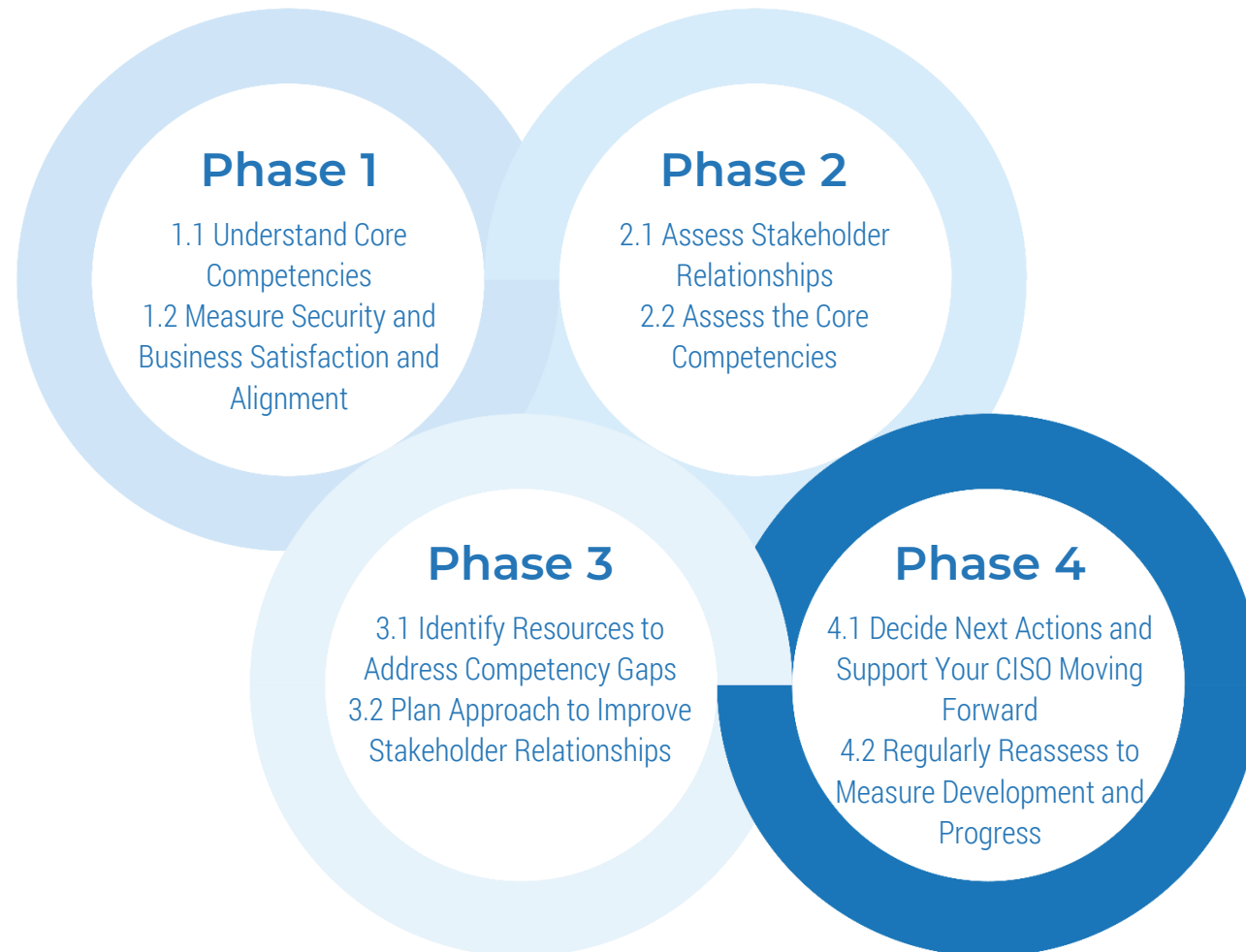
- Completed *CISO Stakeholder Power Map*
- Security Business Satisfaction and Alignment Diagnostic results



Download the *CISO Stakeholder Management Strategy Template*

Phase 4

Execute



This phase will walk you through the following activities:

- Populate the *CISO Development Plan Template* with appropriate targets and due dates.
- Set review and reassess dates.
- Review due dates with CISO.

Hire or Develop a World-Class CISO

Case study

Mark Lester
InfoSec Manager, SC Ports Authority

The new Security Manager leverages successful cultural change to gain support for new security investments.

Outcome: Integrating with the business on a small level and building on small successes will lead to bigger wins and bigger change.

Actions

- By fostering positive relationships throughout the organization, the Security Manager has improved the security culture and established himself as a trusted partner.
- In an organization that had seen very little change in years, he has used well developed **change management, business acumen, leadership, communication, collaboration,** and **innovative problem-solving** competencies to affect his initiatives.
- He can now return to the board with a great deal more leverage in seeking support for security investments.

Next Steps

- The Security Manager will leverage his success in improving the information security culture and awareness to gain support for future initiatives.

Step 4.1

Decide next actions and support your CISO moving forward

Activities

- Complete the Info-Tech *CISO Development Plan Template*
- Create a stakeholder relationship development plan

Execute



This step involves the following participants:

- CEO or other executive seeking to hire/develop a CISO
 - The newly hired CISO
- or
- Current CISO seeking to upgrade capabilities

Outcomes of this step

Next actions for each of your development initiatives

Establish a set of first actions to set your plan into motion

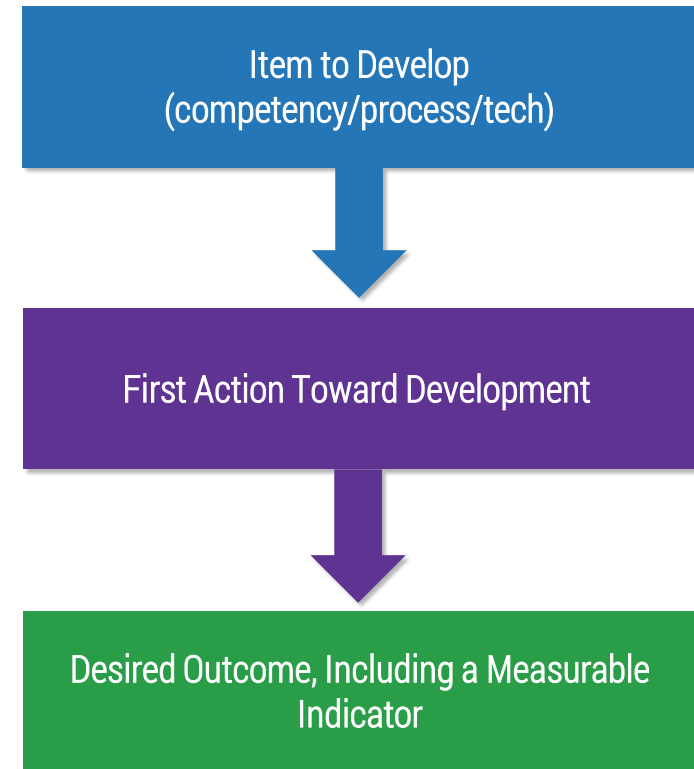
The *CISO Development Plan Template* provides a simple but powerful way to focus on what really matters to execute your plan.

- By this point, the CISO is working on the personal competency development while simultaneously overseeing improvements across the security program, managing stakeholders, and seeking new business initiatives to engage with. This can be a lot to juggle effectively.
- Disparate initiatives like these can hinder progress by creating confusion.
- By distilling your plan down to **Subject > Action > Outcome**, you immediately restore focus and turn your plans into actionable items.
- The outcome is most valuable when it is *measurable*. This makes progress (or lack of it) very easy to track and assess, so choose a meaningful metric.

Info-Tech Insight

You are now planning what your CISO will be doing. Earlier we identified key components in a successful CISO's plan, and this is a good time to recall these:

1. Aligning security controls with business requirements
2. Fostering a risk management culture
3. Managing talent and change



Download the *CISO Development Plan Template*

4.1 Create a CISO development plan to keep all your objectives in one place

Use Info-Tech's *CISO Development Plan Template* to create a quick and simple yet powerful tool that you can refer to and update throughout your personal and professional development initiatives. As instructed in the template, you will document the following:

Your Item to Develop

This could be a CISO competency, a security process item, a security technology item, or an important relationship (or something else that is a priority).



The Next Action Required

This could be as simple as "schedule lunch with a stakeholder" or "email Info-Tech to schedule a Guided Implementation call." This part of the tool is meant to be continually updated as you progress through your projects. The strength of this approach is that it focuses your project into simple actionable steps that are easily achieved, rather than looking too far down the road and seeing an overwhelming task ahead.



The Target Outcome

This will be something measurable like "reduce spending by 10%" or "have informal meeting with leaders from each department."

Info-Tech Insight

A good plan doesn't require anything that is outside of your control. Good measurable outcomes are behavior based rather than state based.

"Increase the budget by 10%" is a bad goal because it is ultimately reliant on someone else and can be derailed by an unsupportive executive. A better goal is "reduce spending by 10%." This is something more within the CISO's control and is thus a better performance indicator and a more achievable goal.

4.1 Create a CISO development plan to keep all your objectives in one place

Below you will find sample content to populate your *CISO Development Plan Template*. Using this template will guide your CISO in achieving the goals identified here.

You may also want to include improvements to the organization's security program as part of the CISO development plan.

The template itself is a metric for assessing the development of the CISO. The number of targets achieved by the due date will help to quantify the CISO's progress.

→ Check out the *First 100 Days as CISO* blueprint for guidance on bringing improvements to the security program

Area for Development	Item for Development	Next Action Required	Key Stakeholders/ Owners	Target Outcome	Due Date	Completed
Core Competencies: Communication	Executive communication	Take economics course to learn business language		Course completed	[Insert date]	[Y/N]
Core Competencies: Communication	Improve stakeholder relationships	Email Bryce from finance to arrange lunch		Improved relationship with finance department	[Insert date]	[Y/N]
Technology Maturity: Security Prevention	Identity and access management (IAM) system	Call Info-Tech to arrange call on IAM solutions		90% of employees entered into IAM system	[Insert date]	[Y/N]
Process Maturity: Response & Recovery	Disaster recovery	Read Info-Tech blueprint on disaster recovery		Disaster recovery and backup policies in place	[Insert date]	[Y/N]

4.1 Use your action plan to track development progress and inform stakeholders

- As you progress toward your goals, continually update the CISO development plan. It is meant to be a **living** document.
- The Next Action Required should be updated regularly as you make progress so you can quickly jump in and take meaningful actions without having to reassess your position every time you open the plan. This is a simple but very powerful method.
- To view your initiatives in customizable ways, you can use the drop-down menu on any column header to sort your initiatives (i.e. by due date, completed status, area for development). This allows you to quickly and easily see a variety of perspectives on your progress and enables you to bring upcoming or incomplete projects right to the top.

Area for Development	Item for Development	Next Action Required	Key Stakeholders/ Owners	Target Outcome	Due Date	Completed
Core Competencies: Communication	Executive communication	Take economics course to learn business language		Course completed	[Insert date]	[Y/N]
Core Competencies: Communication	Improve stakeholder relationships	Email Bryce from finance to arrange lunch		Improved relationship with finance department	[Insert date]	[Y/N]
Technology Maturity: Security Prevention	Identity and access management (IAM) system	Call Info-Tech to arrange call on IAM solutions		90% of employees entered into IAM system	[Insert date]	[Y/N]
Process Maturity: Response & Recovery	Disaster recovery	Read Info-Tech blueprint on disaster recovery		Disaster recovery and backup policies in place	[Insert date]	[Y/N]

Step 4.2

Regularly reassess to track development and progress

Activities

Create a calendar event for you and your CISO, including which items you will reassess and when

Execute



This step involves the following participants:

- CEO or other executive seeking to hire/develop a CISO
 - The newly hired CISO
- or
- Current CISO seeking to upgrade capabilities

Outcomes of this step

Scheduled reassessment of the CISO's competencies

4.2 Regularly evaluate your CISO's progress

< 1 day

As previously mentioned, **your CISO development plan is meant to be a living document**. Your CISO will use this as a companion tool throughout project implementation, but periodically it will be necessary to re-evaluate the entire program to assess your progress and ensure that your actions are still in alignment with personal and organizational goals.

Info-Tech recommends performing the following assessments **quarterly or twice yearly** with the help of our executive advisors (either over the phone or onsite).

1. Sit down and re-evaluate your CISO core competencies using the *CISO Core Competency Evaluation Tool*.
2. Analyze your relationships using the *CISO Stakeholder Power Map Template*.
3. Compare all of these against your previous results to see what areas you have strengthened and decide if you need to focus on a different area now.
4. Consider your *CISO Development Plan Template* and decide whether you have achieved your desired outcomes. If not, why?
5. Schedule your next reassessment, then create a new plan for the upcoming quarter and get started.

- Laptop
- *CISO Development Plan Template*

Participants

- CISO
- Hiring executive (possibly)

Output

- Complete CISO and security program development plan

Summary of Accomplishment

Knowledge Gained

- Understanding of the competencies contributing to a successful CISO
- Strategic approach to integrate the CISO into the organization
- View of various CISO functions from a variety of business and executive perspectives, rather than just a security view

Process Optimized

- Hiring of the CISO
- Assessment and development of stakeholder relationships for the CISO
- Broad planning for CISO development

Deliverables Completed

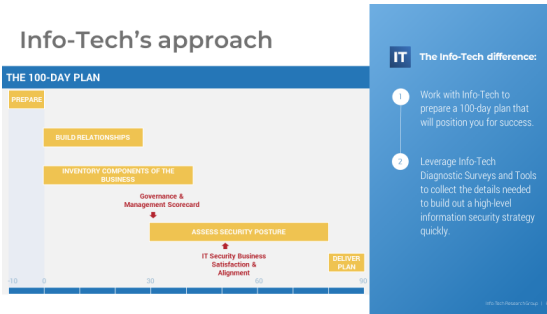
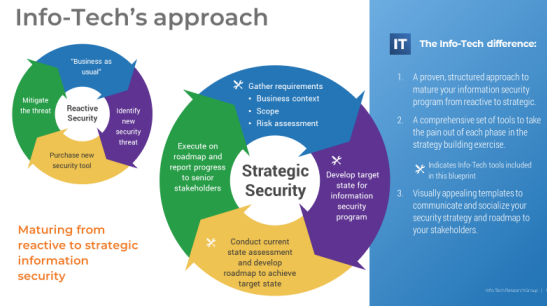
- IT Security Business Satisfaction and Alignment Diagnostic
- CISO Core Competency Evaluation Tool
- CISO Stakeholder Power Map Template
- CISO Stakeholder Management Strategy Template
- CISO Development Plan Template

If you would like additional support, have our analysts guide you through an Info-Tech workshop or Guided Implementation.

Contact your account representative for more information.

workshops@infotech.com
1-888-670-8889

Related Info-Tech Research



Build an Information Security Strategy

Your security strategy should not be based on trying to blindly follow best practices but on a holistic risk-based assessment that is risk aware and aligns with your business context.

The First 100 Days as CISO

Every CISO needs to follow Info-Tech's five-step approach to truly succeed in their new position. The meaning and expectations of a CISO role will differ from organization to organization and person to person, but the approach to the new position will be relatively the same.

Implement a Security Governance and Management Program

Business and security goals should be the same. Businesses cannot operate without security, and security's goal is to enable safe business operations.

Research Contributors

- Mark Lester, Information Security Manager, South Carolina State Ports Authority
- Kyle Kennedy, CISO, CyberSN.com
- James Miller, Information Security Director, Xavier University
- Elliot Lewis, Vice President Security & Risk, Info-Tech Research Group
- Andrew Maroun, Enterprise Security Lead, State of California
- Brian Bobo, VP Enterprise Security, Schneider National
- Candy Alexander, GRC Security Consultant, Towerall Inc.
- Chad Fulgham, Chairman, PerCredo
- Ian Parker, Head of Corporate Systems Information Security Risk and Compliance, Fujitsu EMEA
- Diane Kelly, Information Security Manager, Colorado State Judicial Branch
- Jeffrey Gardiner, CISO, Western University
- Joey LaCour, VP & Chief Security, Colonial Savings
- Karla Thomas, Director IT Global Security, Tower Automotive
- Kevin Warner, Security and Compliance Officer, Bridge Healthcare Providers
- Lisa Davis, CEO, Vicinage
- Luis Brown, Information Security & Compliance Officer, Central New Mexico Community College
- Peter Clay, CISO, Qlik
- Robert Banniza, Senior Director IT Center Security, AMSURG
- Tim Tyndall, Systems Architect, Oregon State

Bibliography

Dicker, William. "An Examination of the Role of vCISO in SMBs: An Information Security Governance Exploration." Dissertation, Georgia State University, May 2, 2021. Accessed 30 Sep. 2022.

Heidrick & Struggles. "2022 Global Chief Information Security Officer (CISO) Survey" *Heidrick & Struggles International, Inc.* September 6, 2022. Accessed 30 Sep. 2022.

IBM Security. "Cost of a Data Breach Report 2022" *IBM.* August 1, 2022. Accessed 9 Nov. 2022.

Mehta, Medha. "What Is a vCISO? Are vCISO Services Worth It?" *Infosec Insights by Sectigo*, June 23, 2021. Accessed Nov 22. 2022.

Milica, Lucia. "Proofpoint 2022 Voice of the CISO Report" *Proofpoint.* May 2022. Accessed 6 Oct. 2022.

Navisite. "The State of Cybersecurity Leadership and Readiness" *Navisite.* November 9, 2021. Accessed 9 Nov. 2022.

Shayo, Conrad, and Frank Lin. "An Exploration of the Evolving Reporting Organizational Structure for the Chief Information Security Officer (CISO) Function" *Journal of Computer Science and Information Technology*, vol. 7, no. 1, June 2019. Accessed 28 Sep. 2022.

The background is a dark blue gradient with several glowing red hexagons of varying sizes and opacities. Some hexagons have smaller red dots inside them. There are also faint, wispy light trails or particle paths scattered across the scene, particularly on the right side.

INFO~TECH
RESEARCH GROUP