CISO Attestation Leadership Portfolio

Reference’s Response

Document Owner: Heather Hinton

Document Authors: Heather Hinton, Steve Zalewski, Tyson Kopczynski

2/19/2025 V.10

# Candidate Information

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Email: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Reference Information

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Email: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Your (Current) Organization, Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Confidentiality

The Professional Association of CISOs, including its members, will make a reasonable effort to keep confidential the contents of a Leadership Portfolio package, including the outcomes and recommendations. The PAC may be required to divulge details regarding a member’s Leadership Portfolio, by court order or other legal process in some circumstances. The Association will comply with all legally valid requests.

# Change History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Change | Approved |
| 2/129/2025 | 0.910 | Initial Draft | HH/SZ |

Substantive changes must have at least two of Heather, Steve, Tyson as approvers. Minor changes including grammar, formatting, can be added by one individual.

# Reference’s Response

### How do you know the candidate:

Please include organizations, roles, responsibilities, reporting, etc – information to allow us to determine the context in which you observed and are evaluating the candidate’s competencies as marked below.

### How to answer:

1. Yes: have observed, Candidate has demonstrated to level documented
2. Blank cells imply “No Comment”: have not observed, do not wish to comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Reference’s Assessment** | | | |
| **No Opportunity to Observe** | **Limited Practical Application** | **Demonstrated, Practiced** | **Demonstrated in Complex Situations**  **(CISO Accreditation Requirement)** |
| **Domain Expertise** |  |  |  |  |
| Regulatory & Legal Expertise |  |  |  |  |
| Crisis / Incident Response |  |  |  |  |
| Cybersecurity Risk Leadership |  |  |  |  |
| Technical Expertise |  |  |  |  |
| **Leadership Competencies** |  |  |  |  |
| General Leadership |  |  |  |  |
| Business Acumen |  |  |  |  |
| Communications |  |  |  |  |
| Collaboration, Relationship Building |  |  |  |  |
| Build/Maintain High Functioning Teams |  |  |  |  |
| Strategic Thinking |  |  |  |  |

## Additional Comments:

Is there anything you would like to tell us about the candidate and their overall cybersecurity leadership? Please feel free to add comments here if yes.

# Appendix: Demonstrating Leadership Competencies

Ultimately, as cybersecurity leaders and CISOs, we are charged with ensuring the reporting on the organization’s cybersecurity program and the adequacy of controls to manage the cybersecurity risks and threats, and the overall cybersecurity risk posture, in support of the organization’s ongoing business goals.

The leadership portfolio is an increasingly detailed assessment of a member’s skills, experience, expertise, knowledge and behaviors contributing to the overall assessment of their competencies in given areas. The leadership portfolio also serves as a measure of the member’s growth and improvement throughout the accreditation process and may act as the basis of a learning plan throughout the member’s career.

All accreditation portfolios will address the identified technical skills and leadership competencies, in increases levels of rigor, with increasingly high standards of accomplishment.

## Learn, Practice, Mastery

The PAC’s focus is oriented towards the learning, practicing and continued growth across the leadership competencies needed to succeed as a cybersecurity leader. We believe that behaviors cannot be tested with an exam; they must be evaluated through observation including self-reflection and discussion of an individual’s actual response to a situation.

As a candidate moves through their accreditation journey, they move from the learning and acquisition of skills and competencies (demonstrated with Associated CISO) to the demonstration and practice of these skills and competencies (CISO Attestation) to the mastery of these skills and competencies in complex situations (CISO Accreditation).

CISO Attestation s focuses on practice through self-evaluation and reflection, confirmed by independent references. Consider that knowing how one is expected to behave in a given situation is not always how one actually responds when in that situation. This is the basis of the common adage that “no plan survives first contact with the enemy.” The only way to have confidence in one’s in-the-moment behavior is to continue growth through the cycle of practice-reflect-refine-practice: this is why we are focused on the demonstration and practice of behaviours at the CISO Attestation level.

## Demonstration of Competencies

Throughout the evaluation of a portfolio, candidates should describe their skills and knowledge and the behavior that reflects the acquisition or mastery of a competency. Behaviors must be demonstrated and continually practiced to maintain and grow the level of competency required for success as a cybersecurity leader.

The continuum of evaluation therefore covers

* Not (Yet) Demonstrated  / No Opportunity to Demonstrate
* Limited Practical Experience
* Demonstrated Experience
  + Demonstrated in Complex Situations

### Not (Yet) Demonstrated

Also referred to as (Possession of) Fundamental Awareness and Basic Knowledge.

The candidate has a common or theoretical knowledge, including an understanding of the concepts and techniques, but has not been able to put these into practice.

Additional learning may be required in addition to time in a role in which the candidate can begin to practice and demonstrate these skills and competencies.

### Limited Practical Experience

Also known as Limited Experience; we prefer “limited practical experience” as it reinforces the difference from practical experience in the form of “on the job” training and situations.

The candidate understands and can discuss concepts, principles and issues related to this competency and their importance as for leadership success.

The candidate has a level of experience gained through acting as an individual contributor or a first-level manager role. They may need coaching / mentoring in addition to in-role experience and practice, including in a wider scope and business impact.

Working with a mentor or coach will help the candidate to (continue to) focus on developing and demonstrating this skill/competency through on-the-job experience.

### Has Relevant Experience

Also known as Meets Expectations; we prefer “has relevant experience” as expectations will differ based on organization, situation, and even point in time. By focusing on “has relevant experience” we can focus on the candidate as an individual in the context of their experience, their organization and their organization’s needs and how they are able to meet those needs.

The candidate continually leverages and demonstrates this competency to as part of their role. They can highlight these skills through discussion of personal and professional situations where they have leveraged these skills and demonstrated competency in these areas, including the self-awareness to understand how and where they need to improve.

The candidate understands and can discuss the application and implications of changes to processes, policies, and procedures in this area. They coach and mentor others in the application of these skills and the development of this as a competency.

Note that by “Has Relevant Experience” we do mean meaningful experience where the candidate has successfully demonstrated the skills and attainment of competency.

When evaluating a candidate’s competencies, we will further consider the complexity of the situation, as reflected in the defined rubrics.

# Appendix: Leadership Portfolio

The leadership portfolio is a multi-purpose document. It is intended to allow the PAC accreditation reviewers to evaluate a candidate’s skills, knowledge and competencies in support of their overall CISO accreditation journey. It is also intended to be used by the candidate to document and reflect their leadership journey, their skills, knowledge and behaviors, and to build a learning and experience plan to help the candidate to continuously improve.

In the portfolio we are looking at four types of leadership competency:

1. General leadership
2. Technical Leadership
3. Core CISO Leadership
4. Business Leadership

These competencies are defined in detail in the separate Leadership Competencies white paper, with brief reminder-style introductions below.

## General Leadership

*Remember that leadership focuses setting a vision and motivating teams towards the goals and objectives that support that vision whereas management is how you execute leadership to accomplish that vision and goals.*

We are looking for both self-awareness of how others view a candidate’s leadership style(s), as well as how they have responded to this awareness by adapting and changing how they work with others.

We are also looking for self-awareness of how others view the candidate and how the candidate has continued to learn and grow and adapt based on interactions with your peers, colleagues and staff.

## Technical Leadership

Leaders are generally assumed to have the basic technical knowledge to support their role: CFOs must understand the details of budgeting, forecasting, market movement, compliance with regulations and so on; accountants must understand the ins and outs of tax regulations; civil (structural) engineers must understand the implications of bridge styles and reinforcement.

As technical leaders, CISOs must understand how their organization depends on and uses technology, the risks that are posed by this usage, and the appropriateness and effectiveness of technologies intended to control (technology, cybersecurity and business) risk.

CISOs must also understand the impact of (cybersecurity) regulations and laws on their organization, including the effectiveness of different technologies in meeting the goals of those regulations and laws. CISO must be able to articulate the impact on the organization’s security posture of emerging laws and regulations and help the organization balance these obligations within the organization’s stated risk appetite.

## Core CISO Leadership

At some point in their career, a CISO (or any leader for that matter) will find themselves in a crisis situation, including cybersecurity incidents. A core part of every CISO’s mandate and value to the organization is the leadership they provide to help an organization prepare for a cybersecurity incident.

Preparing an organization to handle an incident includes helping the organization understand their security posture and the risks that may lead to a cybersecurity incident.  This means that CISOs must understand the business context and impact of risks that may lead to incidents or violations of regulatory or legal requirements and how to best manage those risks within your organization.

## Business Leadership

McKinsey describes leadership as “set of mindsets and behaviors that aligns people in a collective direction, enables them to work together and accomplish shared goals, and helps them adjust to changing environments.”

In the context of the CISO journey, we assert that business leadership is applying the skills, knowledge and behavior associated with leading teams and organizations, regardless of the technical context, in support of a business’s goals, as business leaders.

We assert that success in the core CISO leadership competencies requires strong business leadership competencies, including understanding the organization’s business, and being able to communicate, collaboration, build relationships and level strategic thinking when working with stakeholders across the organization, including peers, colleagues, stakeholders, executive leadership and stakeholders.

Business leadership includes understanding the business, including budgeting and financial management (business acumen), collaborating with stakeholders (collaboration, relationship building), effectively communicating with these stakeholders (communications), motiving and leading teams (build, maintain high functioning teams), and understanding how one’s role and function supports the overall business (strategic thinking).

## Paths to CISO

We believe that there are three main paths to CISO are: business leader, auditor/GRC leader and technical leader. Each path is a valid path to CISO, but each path comes with its own strengths and blind spots in the overall requirements of experience and leadership competencies required to succeed as a CISO. Understanding the different focus areas of these paths will help the CISO candidate build the learning plans necessary to succeed as a CISO.

Regardless of the path to CISO, all CISOs must demonstrate and practice a common set of skills and competencies that are evaluated through the CISO accreditation journey. The PAC CISO Accreditation journey is structured to allow all individuals, regardless of their background, to understand, acquire, practice and master the leadership competencies required to be a successful, accredited CISO.

Business Leadership

This path to CISO is more oriented towards the business leadership side of an organization and explicitly includes individuals who have a background at a consultancy as may be found with a Big 4 or global consultancy (think PWC, Wipro, Kyndryl). These individuals have experience leading and presenting, including presenting and interacting with senior leaders and even the board. These leaders do not (typically) have experience with the operational aspects of a CISO role and may or may not have technical experience found with individuals who rise up through the ranks as technical contributors.

The consultant’s path to CISO is often directly from consultancy to a CISO role at a customer of the consultancy firm, while internally, an individual may move laterally to a CISO role from within the organization.

Auditor / GRC Leader

The path to CISO is typically found for individuals acting in an auditor type of role in a compliance focused environment. These individuals have experience presenting and influencing, typically developed when responding to or leading audits. These individuals will have developed a high-level understanding of controls as required for compliance with common audit frameworks but do not (typically) have a deep understanding of the organization’s technical risks, including the threats associated with the actions of bad actors, or the experience in the evaluation, selection and roll out of technologies and technology-based programs in support of an organization’s overall risk posture.

Technical Leader

This path to CISO is more oriented towards the "tool jockey" who grew up as an engineer within the IT, development or operations departments. These individuals have experience deploying and managing security tools, products and projects, and understand the implications of technology choices, threats posed by bad actors, and how to use technology and processes to remediate technical risks. These individuals typically have limited experience presenting and interacting with senior leaders or the board and do not (typically) have experience with the senior leadership or business management aspects of a CISO role.

This path to CISO is typically found within a technology heavy firm, including vendors, SaaS providers and security vendors.

# Appendix: Responding to Leadership Portfolio Prompts

*These are the instructions provided to the candidates on responding to a series of prompts. In the responses, the candidate documents situations where they demonstrated and practiced the various leadership competencies.*

As a note on these prompts: we care less about the “successful outcome” of the situation and more about what you learned, how you grew, and how this demonstrated both your practice of the competencies and your continued improvement in these competencies.

## Your Answers

In all prompts, we will consider your writing skills – is your answer concise, easy to understand and to the point? Can an evaluator read this and understand the situation and how you handled it? This is in part an evaluation of your communication skills as you will be required to write Board memos, status reports, emails, blogs, and more.

As general guidelines, we don’t think you will be able to answer the prompts effectively in 3-5 sentences – we expect that you will write several paragraphs at least. The more concise your writing, the better. You can assume that the reviewers are experienced former or current CISOs and understand the realities and complications of life in the CISO hot set.

## Addressing the Competencies

Note that we don’t have explicit prompts for the business leadership competencies. The leadership portfolio uses “technically/CISO-role informed” prompts to allow you to demonstrate your technical/CISO-role specific skills and knowledge a part of the prompt itself and then address your business leadership skills, knowledge, expertise and behavior within these prompts. For this reason, we have given you a table (see the Prompt Coverage section) where you can check off the explicit competencies that you have addressed in the individual prompts.