CISO Attestation Leadership Portfolio

Candidate Response Template

Document Owner: Heather Hinton

Document Authors: Heather Hinton, Steve Zalewski, Tyson Kopczynski

2/12/2025 V.90

# Candidate Information

Name:

Email:

## Confidentiality

While this process is based on your practice of leadership competencies as demonstrated through your reflections and documentation, we do not want you to disclose confidential or sensitive information. You will need to balance putting in place enough information that we can validate your scenarios and confirm your scenarios when we talk to your references and referees. At the same time, please don’t include non-public details or information that would violate agreements with your employer.

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 |
| 2/12/2025 | 0.90 | Re-set version numbers to accommodate change history | HH/SZ |
| 2/12/2025 | 0.90 | Technical Leadership Prompt updated to be more generic and remove options (collapse both options into prompt and use examples instead) | HH/SZ |
| 2/12/2025 | 0.90 | Updated and clarified the “Responding to Leadership” section | 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.

# Responding to Leadership Portfolio Prompts

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.

## Prompt Coverage

Use this table to mark off which of the areas of domain expertise and leadership competencies you have addressed in which prompts. Note that we expect that you have addressed the areas of domain expertise in at least the prompts aligned with that domain, meaning you have addressed your regulatory and legal expertise as part of the prompt on “regulatory and legal considerations”. Following this logic, we have pre-populated some of the coverage boxes.

Please add “X” to mark the spot where you have provided further information demonstrating your knowledge, skills, expertise, and competencies. Note we have pre-populated some of the Prompt-Competency mappings for those cases where we are explicitly looking for a competency to be addressed.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Prompt** | | | | | | |
| **P1** | **P2** | **P3** | **P4** | **P5** | **P6** | **P7** |
| **General Leadership** |  |  |  |  |  |  |  |
| General Leadership |  | X |  |  |  |  |  |
| Communications |  |  |  |  |  |  |  |
| **Technical Leadership** |  |  |  |  |  |  |  |
| Technical Expertise |  | X |  |  |  |  |  |
| Regulatory & Legal Expertise |  |  |  | X |  |  |  |
| **Core CISO Leadership** |  |  |  |  |  |  |  |
| Crisis / Incident Response |  |  |  | X |  | X |  |
| Cybersecurity Risk Leadership |  |  |  |  | X |  |  |
| **Business Leadership** |  |  |  |  |  |  |  |
| Business Acumen |  |  |  |  |  |  |  |
| Collaboration, Relationship Building |  |  |  |  |  |  |  |
| Build/Maintain High Functioning Teams |  |  |  |  |  |  |  |
| Strategic Thinking |  |  |  |  |  |  |  |

# P1. Your Management Style(s)

How would you like people to describe both your leadership and your management style(s)? How would you describe your leadership style, both when things are going well as well as when you are under stress? What about when you are receiving or giving bad news? What do you think are your greatest strengths as a leader? What would you like to do better as a leader?

A key part of your management style is how you communicate. How do you (do you?) change your method, style, content of communication when dealing with different members of your organization (your team, your manager, your peers, the executive leadership, and so)?

If we were to ask one of your direct reports, how would they describe your management style?

### Your Answer

Answer here.

# P2. Technical Leadership

Describe a situation in which “the business” (members of your team, IT, Engineering, HR, other) wanted to deploy a program (technology, vendor specific solution) to address a security outcome but the program, as defined, would not and could not provide effective controls to mitigate the threats to the business.

1. For example, the technology/vendor was not going to be able to deliver on the promise made because of gaps in coverage, applicability to your environment or technical fit.
2. For example, a technical project for the rollout of DLP for company workstations did not include in the scope the BYOD devices held by the senior executive leaders.

As part of your scenario / answer, please include

* What was the problem / disconnect with the technology and its intended use
* What role did you play in the “cause/creation” of the situation, or did you inherit the situation?
* How did you explain the problem to the impacted stakeholders
* How did you address this situation and restore, or at least begin to move, towards a repaired relationship with negatively impacted individuals or teams?
* How did you help manage the situation to its resolution?
* What would you do differently next time, how would you have changed your reactions and responses if you could go back in time?

### Your Answer

Answer here.

# P3. Budgets for (technical) security projects

Answer one of the two prompts below, clearly indicating which prompt you have chosen to answer. (deleting the prompt that you are not answering is an acceptable way to handle this).

1. Option 1: (Net new/net add budget items) Describe a situation where you had an approved budget, and mid budget cycle something happens that creates the opportunity (demand) for an urgent, unplanned security project. Describe how you made the case that the new/additional spend was urgent, “non-negotiable”, and had to be done. Did you offer up other parts of your budget, did you require a different group to fund (and did they have the budget available), or did you require “new” funds from the CFO? How did you make the case to your not-security-technical stakeholders that this had to be spent “now” rather than worked into the next budget cycle? How did you explain this technical project and how it supported the company’s business goals? Were you successful? What would you do differently next time?
   1. For example, a near-miss related to a phishing email with your CFO highlights that your EDR solution is not universally installed or properly configured. The Board/Executive Leadership Team directs you to “fill the gaps” in your EDR solution company-wide within three (3) months.
2. Option 2: (Project in the red) Describe a situation where you had (whether you defined or you inherited) an approved budget where in your assessment at least one of the projects was not going to deliver on its promises because of the combination of stated project outcomes, the technology (or vendor implementation of a “technology”) selected and the nuances of your organization’s environment. What did you do? Did you allow the project to continue and reset the organization’s expectations? Did you pause the project (and spend) to reevaluate the project’s goals? How did you explain the situation and the required reset to your non-technical business stakeholders? Were you successful? What would you do differently next time?
   1. For example, your CIO selected a vendor to provide an MFA solution for your company to support a Board mandate/contractual obligation for MFA, but the MFA solution was sized, tested and planned to address only applications covered by your zero-trust solution and so does not cover your development and production environments.

### Your Answer

Answer here.

# P4. Regulatory & Legal Considerations

Describe a situation where you have had to address tension between regulatory or legal requirements and the business’s operations. How did you evaluate the situation, what were the competing concerns, how did you assess the appropriate alternatives and actions? How did you help your organization come to a resolution?

Examples of this situation may include

* Your head of sales has determined that you must have FedRAMP ATO to close a major 3Q deal (it is now 1Q). How did you work with all stakeholders to understand the implications for the business and build the appropriate plan of action.
* Your IAM and SOX-related (\*) policies require that all applications in scope for financial data management are reviewed at least quarterly for continued business need, and all members of the finance team as well as any privileged users with administrative rights to these applications have their access removed within 24 hours of termination of employment (regardless of the reason for termination). You discover that the previous controller, who has left the company as a full-time employee but has remained as a part time consultant to help on-board the new controller, has retained their employee level account and access rights instead of being given a new, contractor-level account and access rights.

(\*) If you are not US publicly traded organization, SOX may not apply. In this case, replace “SOX” with your region’s regulatory equivalent.

### Your Answer

Answer here.

# P5. Risk Leadership

Describe a situation where you have had a fundamental disagreement on the risk assessment (consequences, likelihood, impact) of some aspect of your organization’s cybersecurity operations. How did you work with your stakeholders and peers to help them understand the risk, the implications of the proposed options for handling (remediate, mitigate, transfer, accept), and the effectiveness of the business’s preferred approach of reducing the risk.

Examples that you may have encountered include:

* Security controls for personal mobile devices used for business purposes
* Adoption of a new technology (such as generative AI) without a proper understanding of the potential downsides of the technology

### Your Answer

Answer here.

# P6. Crisis & Incident Leadership

Answer one of the two prompts below, clearly indicating which prompt you have chosen to answer. (deleting the prompt that you are not answering is an acceptable way to handle this).

1. Option 1. If you have been through a cybersecurity event that had the potential to be elevated to a cybersecurity incident within the last 36 months:
   * How was this situation uncovered, what role did you play in its overall resolution? Describe the situation in sufficient detail so that the remaining answers can be put into context.
   * How did you involve the chain of command in your updates and communications? Did you meet the requirements stated your Incident Response policies, procedures and playbooks?
   * Did you have an IR plan and playbook? Did you follow it? How effective was your broader plan?
   * How did you lead and advise your team and members of the organization throughout the situation?
   * Did you have a post-mortem review? Did you ensure it was a blameless review?
   * What did you learn about your team’s readiness and response capabilities and what did you do to make sure that you were better prepared for “the next one”
2. Option 2. If you have **not** been through a cybersecurity event or incident within the last 36 months:
   * Describe how you help your prepare for incidents and crises
   * Do you hold exercises and tabletops? Do they include all the individuals who you worked with to resolve this situation? Why or why not?
   * Do you have an IR playbook and/or an IR plan to support your playbook? Do you practice following the playbook?
   * Do you have post-mortem reviews after each exercise? Do they follow a blameless review discipline?
   * What have you learned about your team’s readiness and response capabilities?
   * How do you ensure continuous improvement throughout this practice?
   * If you have had a non-public (non-material) events that have been treated as incidents, how has your discipline of practice reflected your ability to respond to these events?

NOTE: We understand that many situations will involve confidential information. These prompts are designed to allow you to answer without having to disclose confidential information. You may abstract your response to remove sensitive information (details of the crisis, names of individuals involved) but you should provide enough information that your response is meaningful and should report your actual actions and contributions (“this is what I did”) and not a hypothetical “this is what I would have done” response. This might mean, for example, that if you have recently experienced a non-public cybersecurity incident, that you focus on the preparation and practice option for this prompt so that you do not inadvertently disclose sensitive or confidential information.

### Your Answer

Answer here.

# P7. Self-Reflection Prompt

No leader is perfect; it is impossible to show up at your best in every single situation. Nor is it possible to anticipate (and therefore prepare for) every situation. We all have bad days. What separates good leaders from great leaders is how they respond, grow and learn from these situations.

Describe a situation where you “totally got it wrong”, you misjudged the situation, the people, the consequences, how and when you realized that you were wrong/had mishandled the situation, and how you set about to recover it? What did you learn and how did you change as a result?

#### Your Answer

Answer here.

# Appendix A: Questions for References & Referees

### P1. Sample questions for your referee/reference:

How do you know the candidate? Open ended…

Describe the candidate’s management style; does it align with how the candidate has described it in their portfolio (are they self-aware)?

Describe candidate’s communication style; do they communicate with the style and content expected by the senior and executive leaders within the company?

### P2. Sample questions for your referee/reference

Does the candidate have a strong enough technical background to be able to assess and report on the effectiveness of people, process and technology controls in support of an organization’s security posture?

### P3. Sample questions for your referee/reference:

Will be based in part on the professional relationship (peers, colleagues, managed the candidate). Candidate talked about (insert situation here). In your view, how effective was the candidate at making the case for the security project and budget?

### P4. Sample questions for your referee/reference:

Does the candidate have a strong enough grasp of the organization (its people, process, technology) to be able to articulate the cybersecurity implications of regulations and laws on the business as part of helping the business remain compliant?

How has the candidate helped the business balance non-negotiable regulatory and legal requirements with the “on the ground” business reality.

### P5. Sample questions for your referee/reference:

Describe a situation in which the candidate has helped business stakeholders understand the implications of a proposed course of action (or inaction) on the cybersecurity risk posture of the organization?

### P6. Sample questions for your referee/reference:

Describe how the candidate helps the organization prepare for and practice its readiness and response to a cybersecurity incident or response?

### P7. Sample questions for your referee/reference:

How has the candidate grown as a leader, including both a technical leader and a business leader, in the time that you have known them and worked with them? What are you the most proud of in the candidate’s growth in the time you have known and worked with them?