Professional
Association of
CISOs
theciso.org

# CISO Attestation Leadership Portfolio

Document Owner: Heather Hinton

Document Authors: Heather Hinton, Steve Zalewski, Tyson Kopczynski

2/10/2025 V.99

# Introduction

We expect that this will take (at least) 10-20 hours to complete as you will need to think and reflect on the prompts and take the time to clearly describe how you handled this. This will require you to be vulnerable in ways that you have not previously had to do – at the end of the day it is your choice how open you wish to be in this exercise. We will say that from our experience, the more you lean into this process, the more impactful it will be to your overall leadership development.

We strongly recommend that you have a mentor or coach (or other independent party) read your package before submission, to make sure that it is clearly documented and helps make the case that you have earned CISO Attestation.

## What is Attestation / What is it not

Attestation, and then Accreditation, is a demonstration of an individual's practice and mastery of both the technical skills and leadership competencies needed to succeed as a senior leader and the seniormost accountable cybersecurity leader within an organization.

The purpose of the CISO Attestation package and process is to provide you with the ability to reflect on your practice of the PAC identified leadership competencies. That is, we are looking to understand how you apply and demonstrate these competencies.

If we look at how we become good at something, the process is

Learn – Practice – Mastery

Within the journey of a cybersecurity professional, you probably spent the most time in the "Learn" phase – this is what we will evaluate with the Associate CISO (formerly referred to as "CISO Ready"). Now that you have been in a CISO or deputy CISO role, you should be focused on "Practice"

## 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.

Even more importantly, we are asking you to be vulnerable as part of your leadership portfolio, identifying areas where you didn't do as well as you would have liked, and how you learned and grew as a leader as a result of the experience.

For these reasons, we will make every effort to ensure the confidentiality of your package including

1. Ensuring the secure storage of your package,

THIS ITERATION

2. Limiting access to only those who need to know:
    a. Heather Hinton, Steve Zalewski, Tyson Kopczynski, Renee Guttman.
    b. You may choose to share the details of this portfolio with your references to help them support your application for CISO Attestation. Obviously, this is not something we can control and so we will not make any statements on confidentiality in this regard.
3. Deleting within three (3) months of the general availability launch of the CISO Accreditation process or by March 31, 2026, whichever is sooner.

FUTURE ITERATIONS:

4. Limiting access to only those who need to know, including
    a. The assigned Shepherd,
    b. The assigned CISO Attestation review panel,
    c. The Chair and Vice Chair of the Accreditation and Professionalism Board, and
    d. If you go forward for CISO Accreditation, those named individuals involved in the Accreditation process.
5. Deleting in accordance with our retention policy.

The Professional Association of CISOs, including the (future) Accreditation and Professionalism Board will make a reasonable effort to keep confidential the contents of a Leadership Portfolio package, including the outcomes and recommendations. The A&PB may be required to divulge details regarding a member's Leadership Portfolio, by court order or other legal process in some circumstances. The Association and the Accreditation and Professionalism Board will comply with all legally valid requests.

## Leadership Portfolio Goals

The leadership portfolio is a multi-purpose document. It is intended to allow the PAC accreditation reviewers to evaluate your skills, knowledge and competencies in support of your 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

We are looking for both self-awareness of how others view your leadership styles, as well as how you have responded to this awareness by adapting and changing how you work with others.

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

We are also looking for self-awareness of how others view you and how you have continued to learn and grow and adapt based on your 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.

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 a CISOs career, a CISO (or any leader for that matter) will find themselves in a crisis situation, including cybersecurity incidents. Arguably, this is the fundamental reason why organizations have a CISO: to help them prepare for, respond to and recover from a cybersecurity incident. 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.

While "core CISO leadership" includes crisis and incident response leadership, and risk leadership, succeeding in these leadership competencies also 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 relationship, including peers, colleagues, stakeholders, executive leadership and (if appropriate) the Board of Directors.

## 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 leadership. This means that 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).

## Mapping Prompts to Expertise and Competencies

The prompts included in the Leadership Portfolio are intended to be broad enough to give the candidate multiple opportunities to describe how they have practiced and demonstrated the domain expertise and leadership competencies that are part of their success as a cybersecurity leader and CISO.

| | Prompt | | | | | | |
|---|---|---|---|---|---|---|---|
| | P1 | P2 | P3 | P4 | P5 | P6 | P7 |
| Domain Expertise | | | | | | | |
| Regulatory & Legal Expertise | | | | | | | |
| Crisis / Incident Response Expertise | | | | | | | |
| Cybersecurity Risk Leadership | | | | | | | |
| Technical Expertise | | | | | | | |

| Leadership Competencies | | | | | | | |
|---|---|---|---|---|---|---|---|
| General Leadership | | | | | | | |
| Business Acumen | | | | | | | |
| Communications | | | | | | | |
| Collaboration, Relationship Building | | | | | | | |
| Build/Maintain High Functioning Teams | | | | | | | |
| Strategic Thinking | | | | | | | |

# Leadership Portfolio Prompts

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.

## 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 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.*

### *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?

### *Why are we asking this?*

*We believe that a key input to your overall continued improvement is to understand your management and communication styles, and your flexibility in adopting these styles and how they play to your strengths, and where and how you might want to adapt as part of your leadership journey. We have found that including this prompt helps us and you understand and evaluate your scenario response prompts below.*

## Technical 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: Describe a situation (if possible, within the last 36 months) where you have identified a disconnect with a (technology related) project and its promised outcomes.
   a. *For example, the technology/vendor was not going to be able to deliver on the promised made because of gaps in coverage, applicability to your environment or technical fit.*
2. Option 2: Describe a cross-organizational technical program that you have implemented (you managed the program) to reduce cybersecurity risks.  Who defined the criteria for success for the program? If not you, how did you ensure that they addressed the reality of your environment and further that the criteria were included in the technology/vendor selection process?  What was the business case and ROI for the program? Was the technology selected sufficient to address all use cases.
   a. *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.*

### *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?

### *Why are we asking this?*

All CISOs need to 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. Even if you rely on your teams, you need to be able to understand what they are proposing, guide them if they are incorrect, and ultimately, own the outcome of the technology project.

We want to see if you understand how to evaluate control effectiveness of technology solutions & architecture in the context of risk reduction. We are looking to see if you have sufficient technical depth to be able to both call "technical BS" when needed and to help your teams understand how to build a successful security program.

## 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?
    a. *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?

a. *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.*

### *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?

### *Why are we asking this?*

*Influencing budgets is a key to a CISOs success – without budget, you cannot implement the projects that you believe the organization needs. The budget process is in many ways the single situation that demonstrates all of your leadership competencies and is a key indicator of your success.*

While managing budgets is not a "leadership competency" (in our definitions at least), managing the security budget, including CapEx, OpEx for the security team as well as the understanding and influencing the implications of security-related projects run by other teams, is a skill that requires both business leadership and technical leadership. The hardest part of the budget cycle is making the case for the security projects that you know are needed, keeping as many of them as possible "above the line," while acting within a constrained budget scenario. While acting as a business leader, you need to be able to make the case for a technical project that is required in support of the business, knowing that there are other projects, also in support of the business, that will have to be "cut" if your project is to stay.

## Regulatory & Legal Tradeoffs

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.*

### *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.

### *Why are we asking this?*

*We believe that a key indicator to your overall success as a cybersecurity-focused business leader is to be able to guide your organization as it navigates regulatory and legal concerns and their impact on your cybersecurity posture and programs, in addition to helping you to make sure that your security programs are in compliance with and in support of relevant laws and regulations.*

*Note we do not expect you to understand laws to the level of detail of your company's attorneys, but you should be working and collaborating with the attorneys to understand and advise on the cybersecurity implications of laws and regulations.  As an example, when you buy a house, you must be able to understand the language of the contract, either on your own or when working with an attorney who can walk you through.*

## 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.*

*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?

*Why are we asking this?*

*Ultimately the role of the CISO is to help the business by managing cybersecurity risks that may negatively impact the business and its goals. We are trying to understand how you balance partnering with the business and managing the required cybersecurity risk posture.*

## Crisis & Incident Leadership

Crises come in many shapes and forms. In fact, most are not data breach or ransomware related. Regardless of their shape, form, origin or resolution, organizations should prepare for them so that they are in a position to respond and recover in a timely manner.

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"

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 all 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.

Examples of scenarios that may have exercised your crisis leadership skills include (note that while these, if handled properly, may not be elevated beyond a cybersecurity event, however, if mishandled could easily become "extinction level" events):

- 0-day vulnerability in a critical component (such as a firewall or critical open-source software – think log4j) that is "in the news".
- Cybersecurity incident at a third-party vendor on whom you have a critical dependency (such as Okta, Snowflake, CircleCI, GitLab) that is "in the news"
- Disgruntled former employee after a major corporate layoff event, where employee may be former or may still be employee

### *Your Answer*

*Answer here.*

### *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?

### *Why are we asking this?*

*As CISOs, we ultimately live or die by the 1% situation – how well we have prepared an organization, or have we been able to prepare, for a cybersecurity incident response. This effectiveness of this preparation is demonstrated in the leading of the response, independent of the maturity and discipline within the organization, including controls, processes, metrics and visibility we have brought to the security organization. It is easy to forget this, and so we explicitly call this out as something that CISOs must be diligent about working with their organization to practice and prepare.*

## 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.*

### *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?

### *Why are we asking this?*

*All great leaders are continually self-reflecting and improving. We all have situations where we did not respond as well as we would have liked because we are distracted, misunderstood the situation, having a bad day, or didn't have enough coffee – it doesn't really matter. What matters is how we respond – do we use this as an opportunity to self-reflect, learn and grow.*

# Appendix: More Scenarios

This appendix includes scenarios that we have considered as part of refining the individual prompts. They are included here to provide a reference in case you need additional context. If you find any of these scenarios to be more helpful than those documented, or if you want to add scenarios based on your experience that we have missed, please let us know and we will add them to this section.

## Technical Leadership Prompts

Examples of situations that you may have encountered that may be worth discussing include:

- 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.
- You (or your predecessors) purchased a security technology that it turned out you could not easily deploy causing your project timeline and budget to need a hard reset and causing you to miss your committed goals
- You (or your predecessors) purchased a security technology and kicked off a project to deploy that technology, even though the expected outcome / controls to be implemented by the program did not address high priority controls.
- You (or your predecessors) purchased a security technology that it turned out you could not easily deploy / conflicted with other tools / did not actually solve the proposed problem
- A situation where your technical guidance turned out to be incorrect, but it was not discovered until teams had invested (significant) amounts of work in your preferred approach
- A "not engineering" team (think sales, marketing, finance) purchased – or attempted to purchase – a SaaS solution that was not compliant with your defined risk posture and had not completed a security review
- A situation where you were trying to establish security best practice (e.g. hard drive encryption, blocking USB write on workstations, physical badging for building access) and you met with significant resistance from the business as this was "getting in our way" and "slowing us down"
- Mid-cycle budget adds may result from a crisis (never let a crisis go to waste), where the crisis may include cybersecurity incident, public (inflammatory) statements by your CEO, a merger or acquisition, or other.
- Your head of sales and CEO made the statement – publicly – that your organization uses phishing-resistant MFA even though your solution is SMS Push based (and your proposed budgetary line item from last budget cycle was rejected as not needed given current MFA and additional spend to upgrade). Your existing provider does provide a "phishing resistant" MFA-solution but all of your previous investigations highlighted serious technical gaps, including a lack of coverage for the full set of mobile devices used within your organization.
- A project to roll out a new agentless vulnerability scanning tool, with the published goal and outcome of complete coverage of vulnerabilities in the organization's "Engineering" organization, not recognizing that the organization's inviolate approach to network segmentation would not allow the same source to punch holes into network segments of differing classification (such as development classed as "classified" but production classed as "secret")
- (The same scenario from above): 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.

## Risk Leadership

- Timeline to patch a particular vulnerability, including refusal to patch a critical vulnerability
- Migration from owned and managed data centers to cloud hosted assets
- Assessment of a business application's mission critical status and the required resiliency of operations to support the business
- Physical badging and access control for the organization's (head) office space
- Roles and privileges retained by former employees who stay on as consultants after the termination of their full-time employment status.

## Crisis & Incident Leadership

- Sudden resignation or other incapacitation of a key member of the executive leadership team.
- Misdirected email with large numbers of records with confidential information pertaining to one of your strategic customers sent to another entity (customer, vendor, member of the media, etc.).
- Availability outage of your organization's SaaS style services, caused by a vulnerability in the SaaS application, a configuration error, the failure of a security tool such as a firewall or similar.
- Confirmed material data breach (published).
- Confirmed cybersecurity incident including malware, APT, and so on.
- Availability outage of one of your organization's mission critical vendors (such as your third-party Customer Relationship Management tools at your quarter end).

# Appendix: Archived Prompts

## New In Role Relationships

Describe your peers/stakeholders: who were your most important partners in the understanding and improvement of your organization's security posture. What role did they play and why were they important to your success / the security of your organization?

Were you successful in establishing the relationships you wanted to have in place across the organization? If not, what was the impact and how did you try to repair / move forward? How did you continue to build and then maintain these relationships?

## High Functioning Teams Getting To Know You

If you had a team: How did you approach the initial "getting to know you" phase of being a new leader with your direct reports? What did you do that was effective, and what could have been improved? If you didn't have a direct team, how did you find people across the organization that you needed to influence to ensure security discipline is in place and effective? What did you do to establish yourself as a security leader and SME within the organization?
Rest of the organization: How did you go about establishing relationships and preferred working styles with the rest of the organization, especially the teams managed by your key stakeholders? How did you help them understand your role and goals? How did you set about understanding their roles and goals? Were you successful in establishing the relationships you wanted to have in place across your team? How did you continue to build and then maintain these relationships? How did you go about getting your team on board with your vision and goals?
High Functioning Teams

Almost everyone has a goal for a security assessment and strategy document to be completed within their first 90-days. How did you go about doing the research necessary to understand your team and your organization's security posture and risk tolerance? How did you evaluate your team's current projects, goals and deliverables? Did you end up (wanting to) change the team/their goals/structure/function as part of a new strategic document? How did you get buy-in from your team for this activity? How did you help establish psychological safety for your team, learn from them, understand the team's structure, function, deliverables, and so on?

## 90 DAY ASSESSMENT

New leaders are often tempted to put their "mark" on a team and an organization. Once you had completed your 90-day review and had an opinion on the organization's risk posture, how did you communicate this? Did you find that you had to make changes immediately (you were brought in to "clean up on aisle 6") or were you able to take time to introduce changes including new projects, goals and objectives? How did you make sure that you were calling out the positives as well as the areas of improvement? How did you communicate your results and what did you do to minimize the likelihood of being seen as throwing stones, how did you leverage the relationships you had built, how did you get buy-in for your recommendations? How did you make the case for changes, additions, drops in security projects based on your assessment