# CISO Self Attestation Scenario

[CISO Self Attestation Scenario 1](#_Toc184659256)

[Introduction 2](#_Toc184659257)

[Scenario: 2](#_Toc184659258)

[Prompt Identification 2](#_Toc184659259)

[Scenario Description 2](#_Toc184659260)

[Leadership Competencies 4](#_Toc184659261)

[General Leadership 4](#_Toc184659262)

[Business Acumen 5](#_Toc184659263)

[Change Leadership 6](#_Toc184659264)

[Collaboration & Relationship Building 7](#_Toc184659265)

[Communication 8](#_Toc184659266)

[(Build & Maintain) High Functioning Teams 9](#_Toc184659267)

[Regulatory Landscape Acumen 10](#_Toc184659268)

[Risk Management 11](#_Toc184659269)

[Strategic Thinking 12](#_Toc184659270)

[Appendix: Prompts 13](#_Toc184659271)

[Prompt 1: New CISO Role 13](#_Toc184659272)

[BEFORE: 13](#_Toc184659273)

[DURING: 13](#_Toc184659274)

[AHA MOMENTS 13](#_Toc184659275)

[AFTER 13](#_Toc184659276)

[Prompt #2: A Cybersecurity Event or Incident 14](#_Toc184659277)

[BEFORE 14](#_Toc184659278)

[AHA 14](#_Toc184659279)

[DURING 14](#_Toc184659280)

[AFTER 14](#_Toc184659281)

[Prompt #3: A Material Change in Risk Evaluation 15](#_Toc184659282)

[BEFORE 15](#_Toc184659283)

[AHA MOMENT 15](#_Toc184659284)

[DURING 15](#_Toc184659285)

[AFTER 15](#_Toc184659286)

[Leadership Competencies Self Evaluation 17](#_Toc184659287)

[Grading / Things we look for 18](#_Toc184659288)

# Introduction

This self-reflection is just that: a self-assessment of how you handled a situation that you have found yourself in as part of your CISO responsibilities and how you demonstrated and practiced leadership competencies. This may be abstracted to the hypothetical to protect the innocent, but it is not to be abstracted to the point that you are making things up, or embellishing the situation, or otherwise inserting hypothetical “here’s what I would do” explanations. We want to understand what you did do, what worked, what didn’t work, and perhaps most importantly, what did you learn, how did you grow and overall, how did the experience help you become a better cybersecurity leader?

While this is a self-reflection and self-assessment, you are to describe a scenario that aligns with one of the prompts below.

# Scenario:

## Prompt Identification

Identify the prompt your scenario is aligned with:

* Prompt 1: New CISO Role
* Prompt 2: Cybersecurity Event or Incident
* Prompt 3: Material Change in Risk Evaluation
* Prompt 4: (Details not yet available) 30% Reduction in Team Size
* Other: FILL IN THE BLANK

## Scenario Description

Describe the situation, following the guidance of the prompt. *We expect that the answer to this will be somewhere between 1500-2500 words. We will stop reading at 7500 words.*

*Answer goes here, up to 2500 words:*

This page left blank

## Leadership Competencies

### General Leadership

#### Self-Assessment:

* Not (Yet) Demonstrated / Limited Practical Experience
* Needs Work
* Meets Expectations

#### Rational and Justification

*Answer here, up to 1000 words*

### Business Acumen

#### Self-Assessment:

* Not (Yet) Demonstrated / Limited Practical Experience
* Needs Work
* Meets Expectations

#### Rational and Justification

*Answer here, up to 1000 words*

### Change Leadership

#### Self-Assessment:

* Not (Yet) Demonstrated / Limited Practical Experience
* Needs Work
* Meets Expectations

#### Rational and Justification

*Answer here, up to 1000 words*

### Collaboration & Relationship Building

#### Self-Assessment:

* Not (Yet) Demonstrated / Limited Practical Experience
* Needs Work
* Meets Expectations

#### Rational and Justification

*Answer here, up to 1000 words*

### Communication

#### Self-Assessment:

* Not (Yet) Demonstrated / Limited Practical Experience
* Needs Work
* Meets Expectations

#### Rational and Justification

*Answer here, up to 1000 words*

### (Build & Maintain) High Functioning Teams

#### Self-Assessment:

* Not (Yet) Demonstrated / Limited Practical Experience
* Needs Work
* Meets Expectations

#### Rational and Justification

*Answer here, up to 1000 words*

### Regulatory Landscape Acumen

#### Self-Assessment:

* Not (Yet) Demonstrated / Limited Practical Experience
* Needs Work
* Meets Expectations

#### Rational and Justification

*Answer here, up to 1000 words*

### Risk Management

#### Self-Assessment:

* Not (Yet) Demonstrated / Limited Practical Experience
* Needs Work
* Meets Expectations

#### Rational and Justification

*Answer here, up to 1000 words*

### Strategic Thinking

#### Self-Assessment:

* Not (Yet) Demonstrated / Limited Practical Experience
* Needs Work
* Meets Expectations

#### Rational and Justification

*Answer here, up to 1000 words*

# Appendix: Prompts

## Prompt 1: New CISO Role

At some point, every CISO was a new CISO, both a first time CISO and a new-to-this-role CISO. With this prompt, we are focused on your first 90 (120-, 180-, whatever your grace period was) days, how you approached the activities in this timeline, what you did and how you communicated your findings. Things to think about as you are thinking of this scenario, and how to use it to demonstrate and describe your leadership competencies.

### BEFORE:

1. How did you prepare for this situation?
2. What were your goals for your first 90-days?
3. What expectations did you have going into this situation?

### DURING:

1. What did you do, accomplish, learn during your first 90-days?
2. What was your overall assessment of the company, its security posture and security maturity and the projects required to bring the organization to an organizationally defined, business appropriate risk posture.

### AHA MOMENTS

Some of the AHA moments typically discovered by CISOs during their break in period include:

* Need to reset the expectations on you as the CISO
* Mismatch in stated and practiced organizational approach to and tolerance of risk
* Reality of your organization’s expectations for security (Is it a checkbox? A business enabler? A necessary evil?)
* Mismatch in maturity/skills of team from what was advertised to reality
* Find/create a RACI for the security team’s role in overall business and strategy
* Reality of your team’s experience and maturity with respect to Incident Response

### AFTER

* How did you communicate your findings to your executive stakeholders, peers, colleagues and team members.
* How did that impact your relationships with these teams and individuals?
* With the benefit of time, were you able to accomplish what you initially set out to do during your first 90-days?
* Describe the major / important work items and learnings from your first 90 days

## Prompt #2: A Cybersecurity Event or Incident

While not every cybersecurity leader has dealt with a material cybersecurity incident at the level of a data breach, ransomware, or bad actors moving through the infrastructure, every cybersecurity leader has dealt with 0-Day vulnerabilities of some sort. Even if you had to do an investigation to confirm that you are not impacted, you had to do an investigation, you had to involve legal, communications, inform the executive leadership team (activating your corporate Incident Response plan).

For this prompt, your scenario is a cybersecurity event or incident that you have led. Cybersecurity incidents that are not public should probably not be used for this prompt, but 0-Day investigations and responses should not violate confidentiality requirements and make a great case study for this assessment.

Describe this scenario (abstracted to remove any personal or sensitive details) and how you handled it. Make sure that you address the following items below:

### BEFORE

* Describe the parts of your people, process and technology that played a role in the AHA and AFTER actions

### AHA

* What happened to trigger the cybersecurity event?
* How did you learn of the event?
* Who made the decision to elevate to incident (if required)?
* How did you communicate it to your executive stakeholders?

### DURING

* How did you manage the response process?
* How did you/Did you leverage your Incident Response playbook?
* How did you communicate and engage stakeholders from inside and outside the organization?

### AFTER

* With the benefit of hindsight, what would you have done differently, either before or during this situation?
* How did you learn/grow from this experience and how has this made you a better leader and business partner for your company?

## Prompt #3: A Material Change in Risk Evaluation

For the purposes of this prompt, we are explicitly considering a change in the risk evaluation (impact and or likelihood) of a given event, such that you must change your plans, strategies, and may require an out-of-cycle communication to the executive leadership and potentially even Board of Directors. This may be part of your ongoing CISO role, or it may be something that you “discovered” during your first 90 days.

Respond to this prompt with a scenario where you have identified and communicated a risk posture and the corresponding projects and controls to manage/remediate the risk and the business has chosen to accept the risk as it stands. In this scenario, something happened to fundamentally change your risk assessment (for the worse) such that the decision to accept the risk is no longer correct – the risk is now stated at Critical (or High) and steps must be taken to remediate the risk.

Describe this scenario (abstracted to remove any personal or sensitive details) and how you handled it. Make sure that you address the following items below:

### BEFORE

1. How did you communicate the initial risk posture to your stakeholders (the “before” the bad things happened)?
2. Did you recommend a project(s) (with people and budget) to manage or remediate the risk, and,
3. Did the business decide to accept the risk (not fund the projects needed to remediate the risk)?

### AHA MOMENT

1. What happened to change the risk assessment such that the previous recommendation needed to be updated?

### DURING

* How did you manage the situation?
* How did you communicate the changes and their impact to your stakeholders?
* How did you communicate the changes and their impact to your executive leadership and Board of Directors?
* If you needed additional budget or headcount to address, how did you make the case? If you were successful, what did you do? If you were not successful, what did you do?

### AFTER

* With the benefit of hindsight, what would you have done differently, either before or during this situation?
* How did you learn/grow from this experience and how has this made you a better leader and business partner for your company?

# Leadership Competencies Self Evaluation

For each of the competencies, evaluate your attainment and demonstration of the competency as part of working through your identified prompt. The allows competency levels are:

* Not (Yet) Demonstrated / Limited Practical Experience
  1. Candidate has not had the opportunity to demonstrate the identified competency or has had limited experience demonstrating their experience; evaluation not possible.
* Opportunity for Improvement
  1. Candidate has had opportunities to demonstrate the competency but needs work (time, practice) to perform at the level expected
* Meets Expectations
  1. Candidate has had opportunities to demonstrate and has met expectations of the level of competency as described; confirmed by at least one reference and by (where possible) observation

Throughout these scenarios (any of them), how did you leverage and demonstrate leadership competencies?

If you did not leverage any of the competencies to the extent that you would have liked, or if you feel that you need to improve in a given area but require time to improve, describe your before and desired after competency level and what you are doing as part of continuous improvement.

*Complete the “how you will leverage your competencies” chart to describe how you continue to improve your overall leadership competencies as part of the rest of your (at least) first year in role.*

You may also wish to refer to general skills that you have called upon in this scenario, including:

1. **General Skills**
   1. Problem Solving
   2. Project & Program Management
   3. Decision Making
   4. Change Management
   5. Executive posture and maturity

# Grading / Things we look for

|  |  |
| --- | --- |
| Competency |  |
| General Leadership |  |
| Business Acumen | Did the candidate’s proposed solutions (or learning from the situation) demonstrate business acumen? How was business acumen used as part of the overall identification of problem, proposed solution? |
| Change Leadership | Did the candidate understand the magnitude of the change and apply change management thinking and discipline? Did they take steps to successfully lead people through the situation acting as a positive leader, resource and change agent? |
| Collaboration & Relationship Building | Did the candidate have collaborative / relations in place to help address this scenario? How did they leverage them? If they weren’t already in place, how did they build them on-the-fly? |
| Communication | How did the candidate communicate all of this to their stakeholders? Did they tailor their communications to the intended audience?  How well is the assessment written (does their answer demonstrate strong written communication skills)? |
| Crisis Management | Arguably this is a crisis situation, even if it is not an all-hands on deck IR crisis – how well did the candidate manage the situation? |
| (Build & Maintain) High Functioning Teams | Did the candidate have a high functioning team to rely on? Were they hostage to a few star performers? How did they leverage their team to address the situation? Did they use this to help uplift / move their team towards high functioning team characteristics? |
| Regulatory Landscape Acumen | Did the candidate understand and include regulatory implications (if applicable) in their solution? |
| Risk Management | How did the candidate address risk management before, during and after? |
| Strategic Thinking | Did the candidate demonstrate strategic thinking in their assessment and proposed solution? |
| GENERAL SKILLS |  |
| Problem Solving | There must have been a problem somewhere (its hard to have an AHA moment without one). How did the candidate describe the problem, its identification, its resolution? How did their technical expertise support this problem solving? |
| Project & Program Management, Change Management | How did the candidate demonstrate and leverage project and/or program management skills? Did they ensure the situation was managed according to some level of PM like discipline?  How did the candidate leverage change management disciplines as part of remediation / new project? |
| Decision Making | Did the candidate display effective decision making? How was this highlighted as part of leadership competencies? |
| Executive posture & maturity | Does the candidate’s written response and presentation demonstrate executive posture & maturity (esp in how they worked with stakeholders to address and remediate)? |
| Technical Expertise | How did the candidate leverage their technical expertise (and that of their teams) to understand the situation and identify alternatives? |