Mercer

Cyber Security Assessment Sample Report

June 2024

A business of Marsh McLennan

Sample Overview

37

Participants

UP TO

10 YEARS

Tenure with Organisation

5

COUNTRIES

4 COMPETENCIES

- Compliance and Process
- Interpersonal Relationships
- Positive Attitude
- Taking Responsibility

2

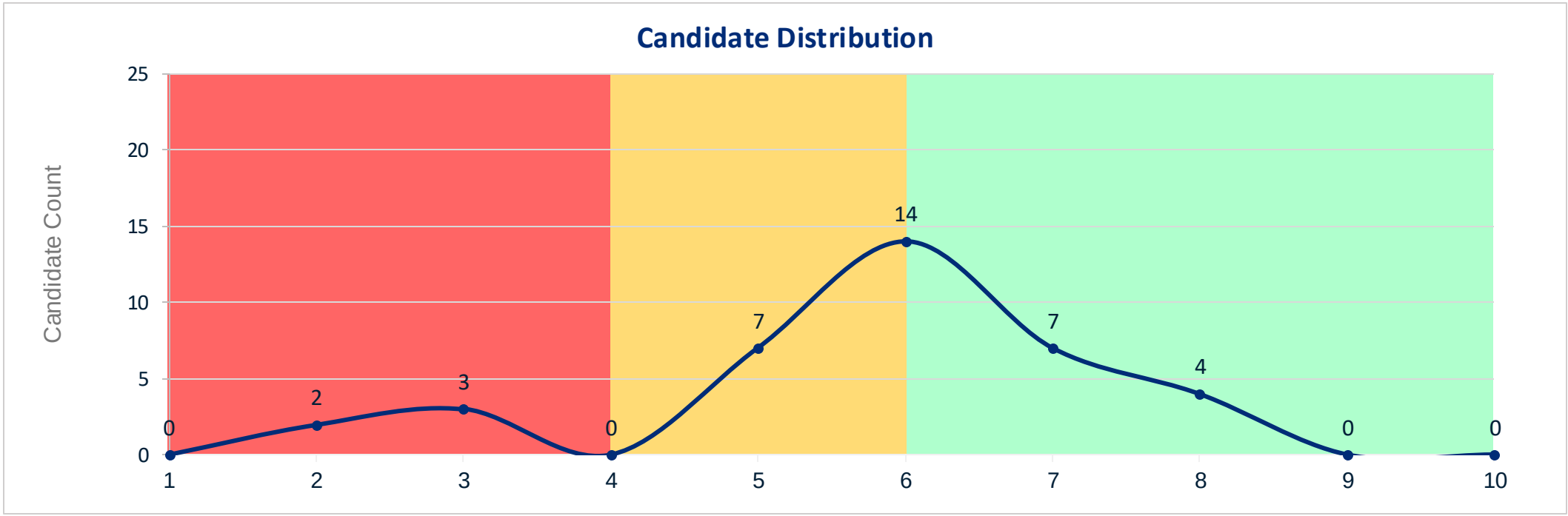
Departments

4

JOB ROLES

Candidate distribution – Security Index (Overall Score)

This report session aims to provide you with a quantitative measurement of your team's security status in context of cybersecurity domain(**Security index**) along with a qualitative description of your team's profile. By understanding the team's security profile, we can identify the strengths and potential areas of improvement and develop targeted strategies to enhance their effectiveness in addressing cybersecurity challenges.



Security Index

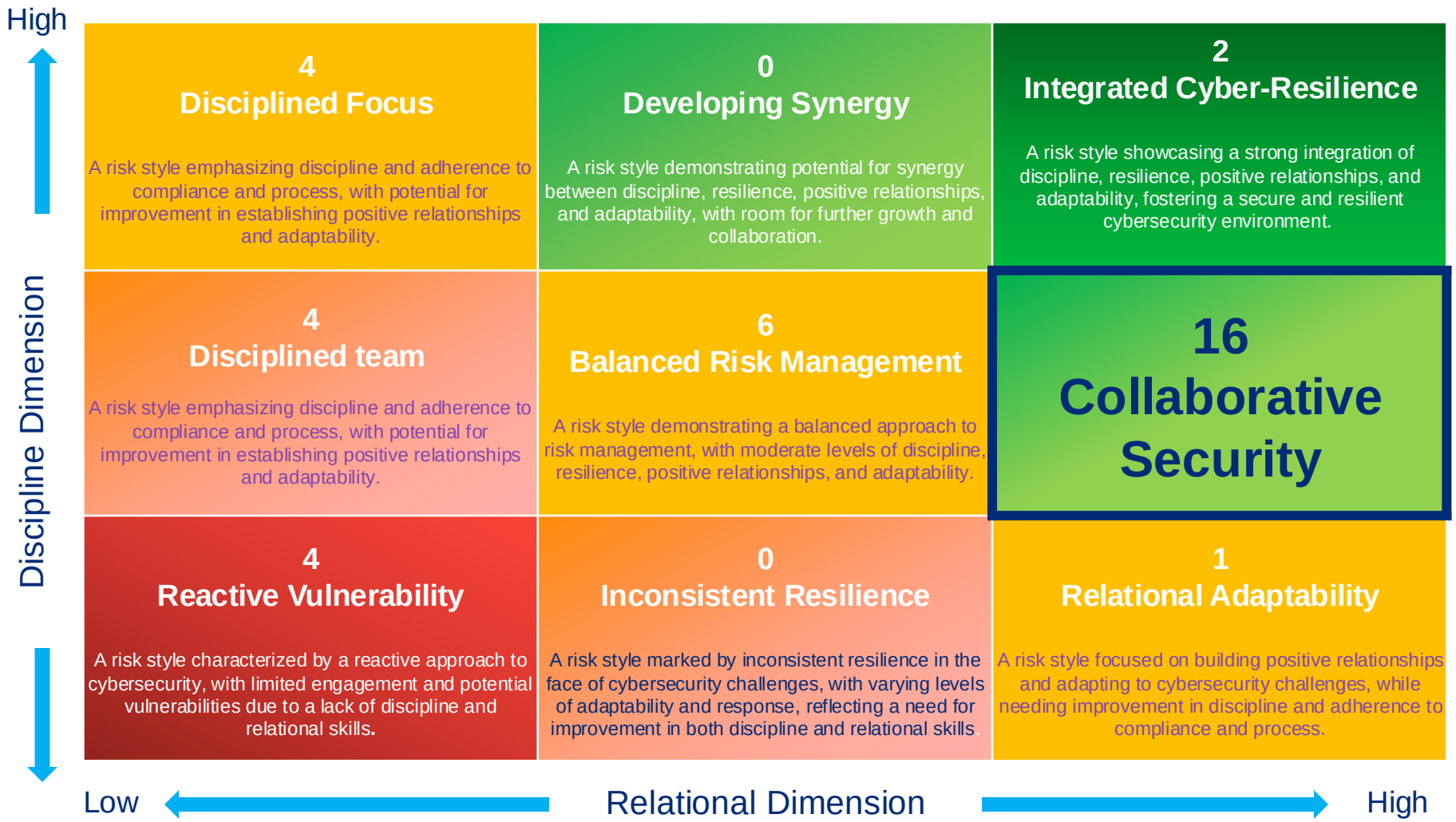
Low Security (1-4) (High Risk) — 05

Moderate Security (5-6) (Moderate Risk) — 21

High Security (7-8) (Low risk) — 11

Security Index is a measure of the level of cybersecurity a team possess. It consists of 3 bands ranging from low security, moderate security and high security. The present data reflects that 5 members of the team lie in the low security zone indicating high risk which means, members are likely to be vulnerable to cyber incidents. 11 members lie in the high security-low risk zone and **majority** of the team members lie in the moderate security-moderate risk zone.

9 Box Model Distribution over Team Profile

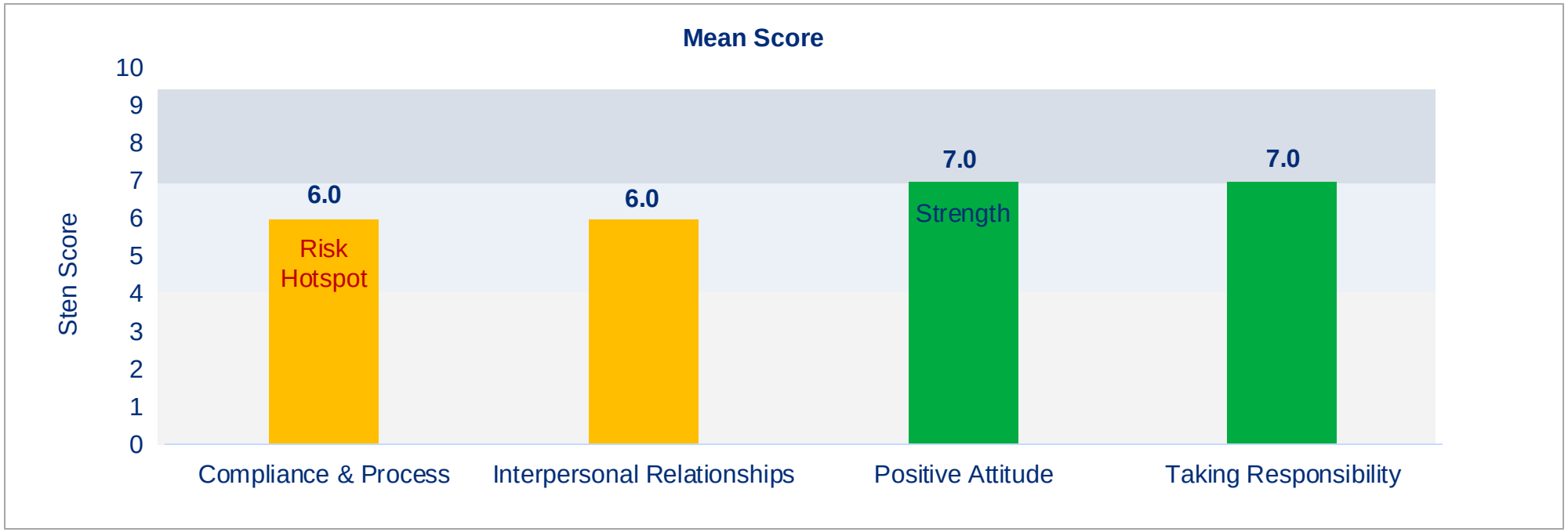


Majority of the candidates are falling in “**Collaborative Security**” box indicating team’s strong focus on collaboration, resilience, discipline, and adherence to compliance and process, fostering a secure and supportive cybersecurity environment.
Team excel in both interpersonal skills and risk management practices, promoting a collaborative and secure cybersecurity culture.

Competency Wise Mean Score

Low Security (1-4) (High Risk) | Moderate Security (5-6) (Moderate Risk) | High Security (7-8) (Low risk)

Click here for Annexure

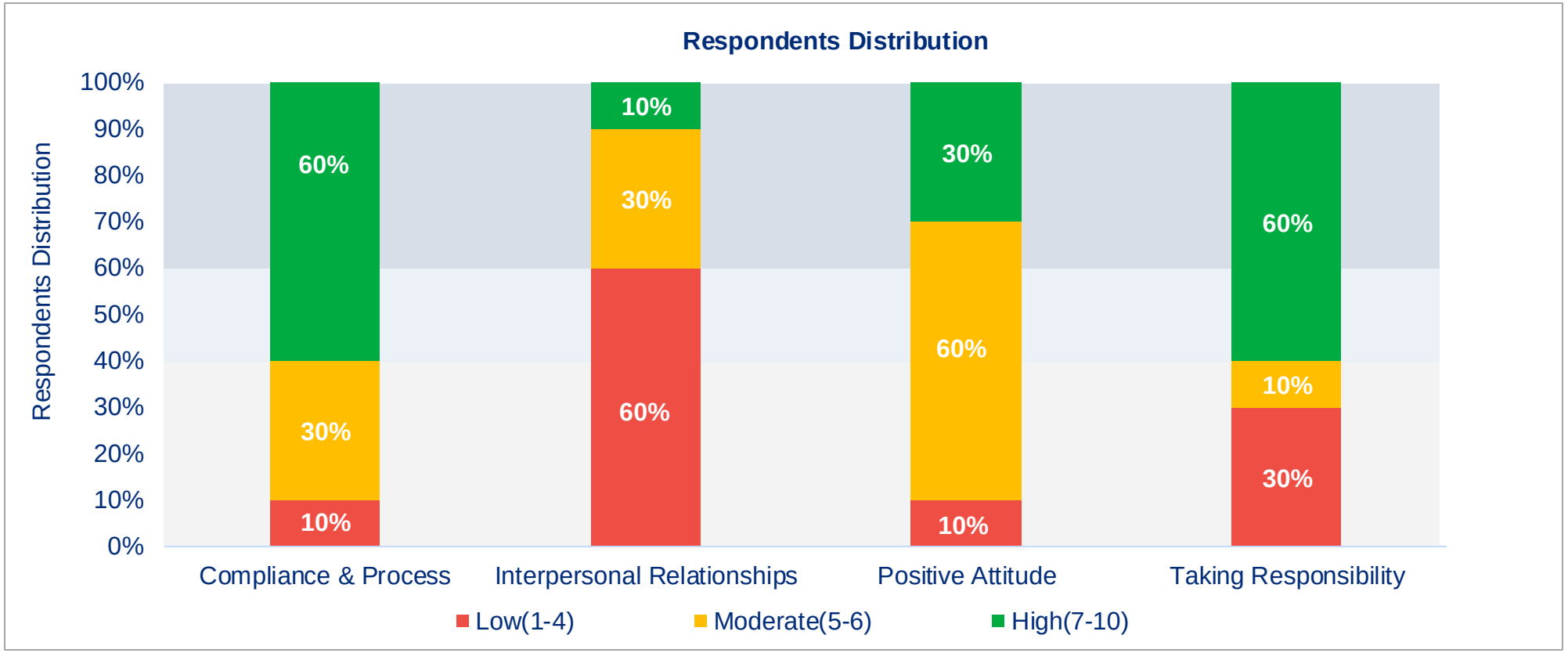


Description			
The team's adherence to established Cyber Security policies and ethical procedures is balanced, exhibiting moderate levels of self-efficacy and ethical behavior, with some room for further development.	The team is likely to be comfortable in establishing positive connections with others in the context of Cyber Security risk while occasionally being reluctant to seek input or assistance from colleagues.	The team is likely to maintain a positive outlook and remain resilient in the face of Cyber Security challenges, approaching problems with a can-do attitude.	When it comes to taking initiative and assuming ownership of Cyber Security responsibilities, the team is likely to adopt a proactive approach and take the appropriate actions to mitigate risks.

Out of 4 Competencies, 2 are falling in moderate scoring category and 2 are falling in high scoring category
Compliance & Process is coming out as a Risk Hotspot and Positive Attitude is coming out as a Strength of the cohort.

Candidate Distribution over Competencies

The Detailed Profile section of this report provides an in-depth analysis of the team's characteristics in the cybersecurity domain. By examining various dimensions and factors that contribute to the team's performance, this section offers a comprehensive understanding of their profile.



"WHILE MOST OF THE CANDIDATES SCORED HIGH IN COMPLIANCE AND TAKING RESPONSIBILITY, INTERPERSONAL RELATIONSHIPS REPRESENTS A RISK FOR THE 60% OF THE TEAM MEMBER.

Strengths:

Strengths refer to those Competencies that may contribute positively to cybersecurity practices and are to be leveraged.

Positive Attitude

Overall Description

In the realm of Cyber Security, the team proactive approach to problem-solving, positive outlook and resilience contributes to foster a positive Cyber Security culture, influencing others to adopt best practices and prioritize Cyber Security.

Advantages

Individuals who possess high positive attitude scores have the potential to significantly contribute to the cultivation of a positive cybersecurity environment. Often, employees only become aware of cybersecurity when they experience a negative incident, which can create a pessimistic perception. However, individuals with a positive attitude can play a crucial role in promoting a shift in mindset and fostering a culture of positivity and collaboration. By adopting positive communication strategies, utilizing encouraging and supportive language, and emphasizing solutions rather than dwelling on problems, these individuals can create an atmosphere where everyone feels comfortable reporting any suspicious activity they encounter.

Possible Derailers

- Overly positive teams may be less likely to question suspicious activities or potential threats, making them vulnerable to cyber attacks.
- A strong focus on positive outcomes may lead to neglecting proactive preparation for security incidents. "

Click here to go back

Risk Hotspot

Risk hotspots refer to those Competencies that may pose challenges or increase the likelihood of engaging in risky behaviours.

Compliance and Process

Overall Description

"The team's adherence to established Cyber Security policies and ethical procedures may not be consistent, potentially leading to the oversight or disregard of crucial security protocols. Consequently, the team may encounter difficulties in responding proactively to security incidents or experience delays in promptly reporting them. This, in turn, can create vulnerabilities and increase the risk of cyber threats. The situation can be exacerbated by a lack of the necessary knowledge or skills to handle incidents appropriately and a limited understanding of data protection regulations or industry-specific standards. These factors can result in self-doubt and further hinder incident response."

Possible Derailers

- ❑ Inconsistent adherence to cybersecurity policies and procedures can create vulnerabilities and increase the risk of cyber threats.
- ❑ Lack of awareness about common attack vectors, social engineering techniques, and emerging threats can make the team more susceptible to cyber incidents.
- ❑ Inefficiency and limited knowledge may result in delayed incident response and escalation of security incidents.

Click here to go back

Team Development Plan

Training and Education

Provide the team members with comprehensive training on cybersecurity best practices, industry standards, and relevant regulations. This can include courses, workshops, or online resources that cover topics such as data protection, risk management, incident response, and compliance requirements.

Policy Familiarization

Ensure that the team members are familiar with the organization's cybersecurity policies and procedures. Review these policies together and address any questions or concerns they may have. Emphasize the importance of compliance and the potential consequences of non-compliance.

Process Improvement

Help the team members understand the importance of following established processes and procedures in cybersecurity. Identify any gaps or weaknesses in their current approach and work together to develop more effective processes. This may involve creating checklists, implementing automation tools, or establishing clear communication channels for reporting and addressing security incidents.

Ongoing Monitoring and Feedback

Regularly assess the team member's progress and provide constructive feedback on their compliance and process adherence. This can be done through periodic evaluations, performance reviews, or mentoring sessions. Encourage open communication and address any challenges or concerns they may encounter.

Continuous Learning

Encourage the team members to stay updated on the latest cybersecurity trends, threats, and technologies. This can be achieved through participation in industry conferences, webinars, or subscribing to relevant newsletters and publications. Encourage them to join professional cybersecurity organizations or forums to network with peers and learn from their experiences.

Accountability and Recognition

Establish clear expectations for compliance and process adherence and hold the team members accountable for their actions. Recognize and reward their efforts when they demonstrate improvement and consistently follow cybersecurity protocols. This can help motivate them to continue their development journey.

Competency Description

Compliance & Process:

Moderate

- "The team's adherence to established cybersecurity policies and ethical procedures is balanced, exhibiting moderate levels of self-efficacy and ethical behavior, with some room for further development. It is important to encourage the team to stay up to date with the necessary knowledge and skills to handle incidents appropriately, in order to nurture self-confidence and strengthen incident response."

Competency Description

Interpersonal Relationships:

Moderate

- The team is likely to be comfortable in communicating and building relationships with colleagues or security teams regarding Cyber Security matters. They are able to moderate between the diverse opinions given by team members and act in favor of the organization's Cyber Security. However, occasionally, they may be reluctant to seek input or assistance from colleagues.

Competency Description

Taking Responsibility:

High

- "The team is likely to actively seek out vulnerabilities, implement security controls, and make necessary improvements to protect the organization's assets. They are likely to understand their role in maintaining a strong Cyber Security posture, take ownership of the responsibilities assigned to them and be committed to mitigating cyber risks."

Competency Description

Positive Attitude

High

- In the realm of Cyber Security, the team is likely to take a proactive approach to problem-solving, maintaining a positive outlook and not being easily discouraged by setbacks. Embracing change, they are unafraid to think outside the box and explore innovative solutions to overcome Cyber Security challenges. Through their positive attitude and persistence, they are likely to influence others to adopt best practices and prioritize Cyber Security.

Mercer

THANK YOU

A business of Marsh McLennan