Mercer Cyber Security Assessment (Italian)

Maximiliano | 03 Jun 2024

You are viewing the report in a different language and test is in other language

Test Taker Details

Overall Status: Completed Detailed Status: Test-taker Completed

Test Finish Time: June 03, 2024 01:48:56 PM BST

M

Maximiliano

Indirizzo email: maxpapagna@gmail.com

Test-Taker ID: - 132701903

Table of Contents

Introduction and Background

Mercer Mettl's Cyber Security risk framework identifies competencies and personality traits that are relevant to Cyber Security risk-taking behavior. The framework and assessment aim to help individuals understand how their personality may influence their approach to Cyber Security risks. Individual behavior plays a critical role in the Cyber Security of organizations. By exhibiting good Cyber Security behaviors, individuals can reduce vulnerability to security breaches, enhance data security, and safeguard both themselves and their organizations from cyber incidents.

The Mercer Mettl Cyber Security risk framework comprises four competencies: Compliance and Process, Taking Responsibility, Interpersonal Relationships, and Positive Attitude. These competencies can be further broken down into specific personality traits, which provide a more detailed understanding of how individuals are likely to comply with Cyber Security measures or take risks in this domain.

The illustration below shows the four competencies and the personality traits that underpin them.

- **Compliance and Process**

  Compliance and Process refers to an individual's tendency to adhere to Cyber Security rules, regulations, and protocols, as well as their understanding of the processes involved in maintaining a secure environment.

  Individuals who score high on Compliance and Process competency tend to demonstrate a high level of rule adherence, follow established Cyber Security protocols, and comply with relevant regulations and standards. They tend to exhibit traits such as Rule Adherence, Proactivity, Self-Efficacy, and Ethics. They tend to understand the importance of Cyber Security processes and actively contribute to maintaining a secure environment. They tend to possess a strong sense of ethics, ensuring that their actions align with ethical principles in Cyber Security practices.

- **Positive Attitude**

  Positive Attitude refers to an individual's tendency to have a mindset and outlook towards Cyber Security that encompasses resilience, positivity, openness to change, and persistence in overcoming challenges.

  Individuals who score high on Positive Attitude competency tend to approach Cyber Security challenges with resilience and a positive mindset. They tend to exhibit traits such as Resilience, Positivity, Openness to Change, and Persistence. They tend to embrace changes in security practices, technologies, and threats, demonstrating a tendency to adapt and learn. They tend to maintain a positive attitude towards security measures and processes, persisting in their efforts to overcome obstacles and achieve Cyber Security goals. They tend to exhibit trust in security systems, processes, and the reliability of Cyber Security measures, fostering a positive and secure Cyber Security environment.

- **Interpersonal Relationships**

  Interpersonal Relationships refer to an individual's ability to establish and maintain positive relationships with others in the context of Cyber Security, fostering collaboration, empathy, and effective communication.

  Individuals who score high on Interpersonal Relationships competency tend to excel in building relationships characterized by openness to diversity with colleagues, stakeholders, and other relevant parties involved in Cyber Security. They tend to exhibit traits such as Openness to Diversity, Empathy, Sociability, and Altruism. They tend to actively engage in collaborative efforts, effectively communicate security-related information, and demonstrate empathy towards others' security concerns. They tend to foster a supportive and collaborative Cyber Security culture by exhibiting sociability and altruistic behavior.

- **Taking Responsibility**

  Taking Responsibility refers to an individual's tendency to have a sense of ownership, assertiveness, ability to take charge, and effective planning in the context of Cyber Security.

  Individuals who score high on Taking Responsibility competency tend to take ownership of their Cyber Security responsibilities and demonstrate a proactive approach. They tend to exhibit traits such as Ownership, Assertiveness, Take Charge, and Planning. They tend to assertively address security issues, communicate concerns, and advocate for necessary security measures. They have a tendency to take charge of security initiatives when required and effectively plan and organize Cyber Security actions. They exhibit accountability and demonstrate a strong sense of responsibility towards maintaining a secure environment.

How to Interpret the Report?

This report is divided into several sections:

1. Profile Summary

2. Strengths and Risk Hotspots

3. Cyber Security Competencies

4. Individual Development Plan

1. The Profile Summary

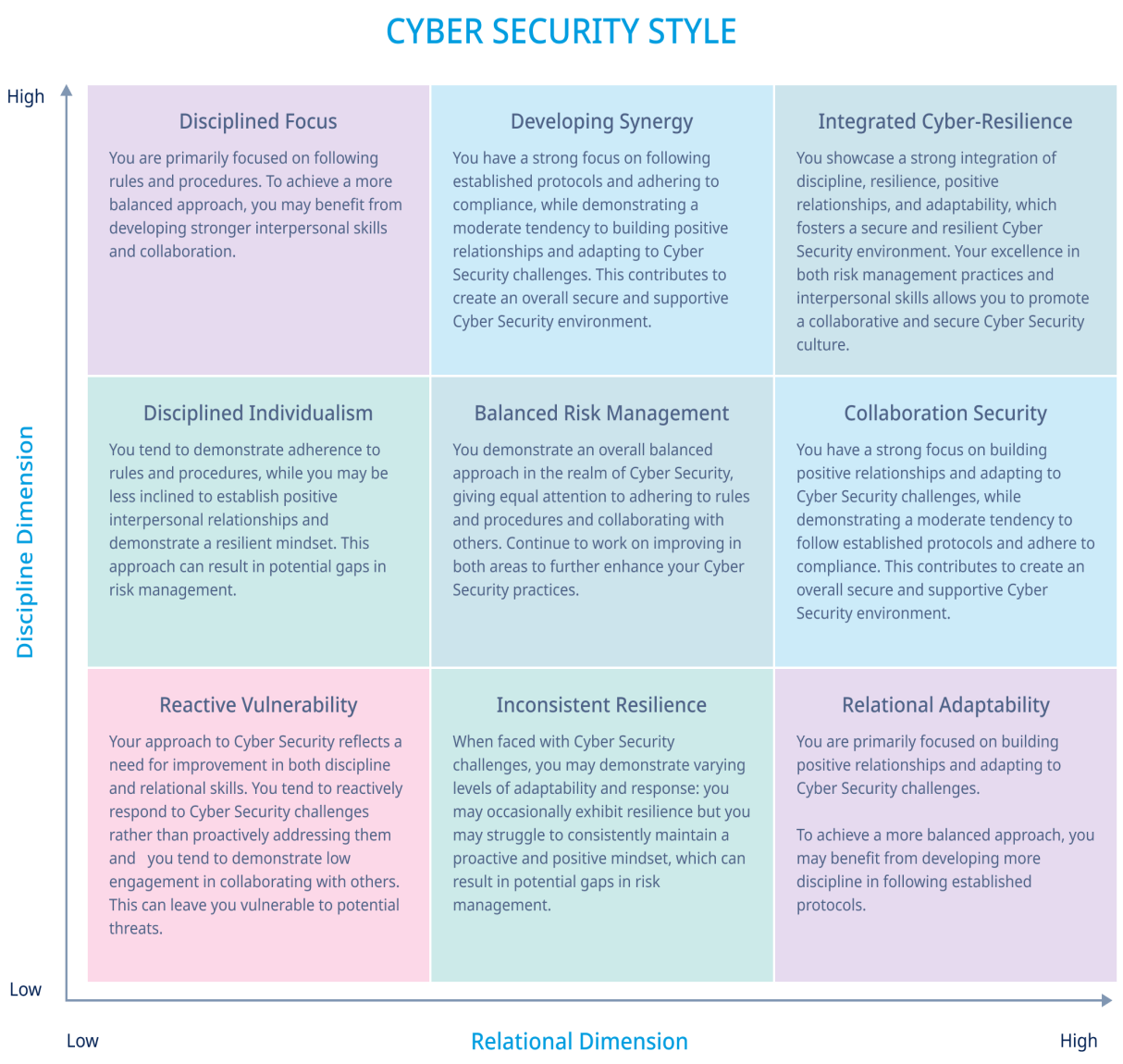
This section offers the overall profile of the candidate. It provides insights into the individual's likelihood to adhere to Cyber Security practices and suggests their overall Cyber Security style.

The individual's Cyber Security style is determined by the interaction between two key dimensions: Discipline and Relationship.

The Discipline dimension comprises the Compliance and Process, as well as Taking Responsibility competencies. These competencies shed light on an individual's inclination to adhere to Cyber Security Discipline, their commitment to following established protocols, and their sense of accountability towards their work.

On the other hand, **the Relational dimension** encompasses the Positive Attitude and Interpersonal Relationships competencies. These competencies predict how an individual interacts with others and their propensity to demonstrate a positive attitude in the context of Cyber Security.

By categorizing the meta-competency scores into low, medium, and high, the two dimensions form a 9-box matrix that provides a clear and intuitive summary of the individual's overall Cyber Security style. Subsequent sections will delve into a more detailed explanation of the individual competencies and traits.



2. Strengths and Risk Hotspots

The Strengths and Risk Hotspots section begins by presenting a graphical summary of all scores for the individual's personality traits that are relevant to Cyber Security. Subsequent pages provide a detailed breakdown of an individual's strongest traits and highest risk hotspots, accompanied by a deeper interpretation of each.

3. Cyber Security Competencies

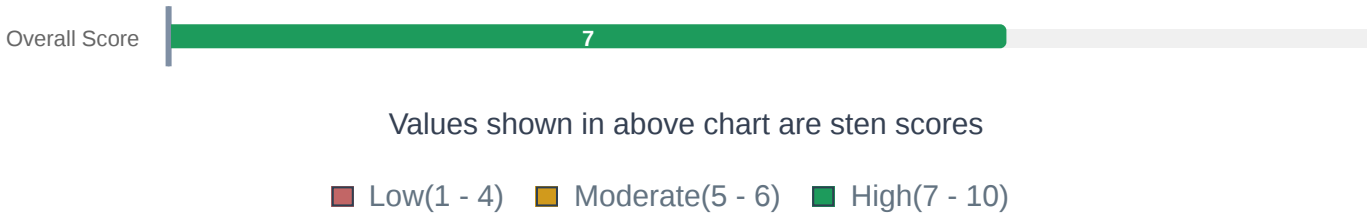
This section gives greater detail on each of the four Cyber Security competencies.

4. Individual Development Plan

This section provides personalized recommendations to address specific areas of concern (hotspots) and capitalize on strengths.

PROFILE SUMMARY

Overall Risk Score:



1. Overall Risk Score:

7

Of 10.0

Overall Score: High

Your overall Cyber Security score is high, indicating you follow the cyber security protocols laid down in the organization, are aware of the cyber threats, and prepare yourself well to prevent cyber incidents that could pose a danger to your digital assets. Your skills, knowledge of the Cyber Security domain, and cyber hygiene practices could be beneficial for others, and your peers could learn and adopt similar cyber-secure behaviors from you.

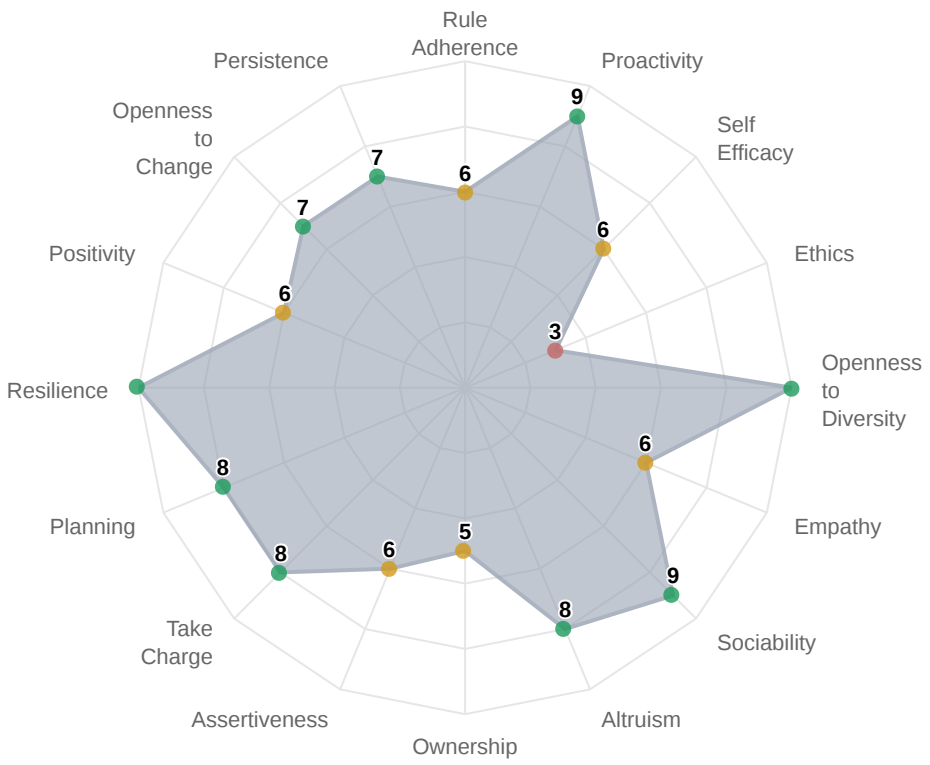
CYBER SECURITY STYLE

Collaborative Security: A risk style characterized by a strong focus on collaboration, resilience, discipline, and adherence to compliance and process, fostering a secure and supportive Cyber Security environment.

Strengths and Risk Hotspots

The spider chart below serves as a visual representation of your scores across relevant personality traits in the realm of cybersecurity.

Your scores are presented on a scale of 1 to 10 for each personality trait. The closer a data point is to the center of the chart, the lower the corresponding score, while data points closer to the outer edges indicate higher scores.



Values shown in above chart are sten scores

Low(1 - 4) Moderate(5 - 6) High(7 - 10)

Strengths

–

Strengths refer to those traits that may contribute positively to Cyber Security practices and are to be leveraged.

- Openness to Diversity
- Resilience
- Proactivity

Risk Hotspot

–

Risk Hotspots refer to those traits that may pose challenges or increase the likelihood of engaging in risky behaviors.

- Ethics
- Ownership
- Rule Adherence

Strengths

–

Openness to Diversity

Overall Description

You tend to be more open to working with people from a diverse set of backgrounds. This is likely to help you build strong relationships with others and to benefit from a range of diverse perspectives about how to implement, maintain and defend Cyber Security.

Advantages

- Individuals with high openness to diversity bring various perspectives and experiences to the table. This diversity of thought can lead to more innovative and effective problem-solving in Cyber Security.
- Individuals with this trait actively seek input from diverse stakeholders and can make informed decisions. It can contribute to building trust and satisfaction.
- When individuals are accepting of diverse backgrounds, this can lead to increased trust, engagement, and compliance with security protocols.

Possible Derailers

- Individuals open to diversity tend to be more accommodating towards others, making them vulnerable to cyber security risks.
- Embracing diversity in Cyber Security can introduce additional complexity in the implementation of security measures.

Resilience

Overall Description

You are likely to cope well and recover quickly when faced with difficult and stressful situations in the workplace. This is likely to help you tend to stick with the ongoing need for often uninteresting IT updates and protective behaviors, but also to react with strength during high-pressure situations such as cyber-incidents.

Advantages

- Resilient individuals tend to have the ability to bounce back quickly from setbacks, such as security breaches or failures; this allows them to maintain a strong security posture and minimize the impact of cyber threats.
- Resilient individuals tend to adapt quickly; it helps them stay one step ahead of cybercriminals and effectively protect systems and data.
- Some Cyber Security activities, such as password updating, can feel repetitive and boring; more resilient people may be more inclined to keep doing it and to do it across multiple websites.

Possible Derailers

- Individuals scoring high on resilience may assume that they can easily recover from any incident. This may create blind spots and leave systems vulnerable to new and emerging threats.

Proactivity

Overall Description

You tend to engage in self-starting, future-oriented behavior to enact positive change rather than waiting for direction. As a result, you are likely to follow Cyber Security rules and respond to potential threats without needing to be prompted.

Advantages

- Proactive people tend to act without waiting for direction from others. They are likely to prepare themselves in advance to safeguard against any potential cyber threats.
- Proactive individuals are likely to actively secure devices (e.g., locking computers/laptops/phones); they may go beyond minimum security requirements (e.g., using longer passwords); proactivity often helps keep software up-to-date and look out for new versions.
- Proactive individuals may actively search for vulnerabilities in systems, networks, or applications with the intention of identifying and addressing them before they can be exploited by malicious actors.

Possible Derailers

- As proactive people may act without waiting for direction from others, there is some chance of their actions diverging from official protocol when it comes to Cyber Security; when unsure of how to tackle novel threats to security, it is important to be ready to take action, but also consult Cyber Security and privacy experts.

Risk Hotspot

–

Ethics

Overall Description

You may either prefer not to follow conventional ethical standards or may follow your own individual view of ethics. This may mean that you disregard guidelines for Cyber Security or feel that you can judge for yourself what will work best.

Possible Derailers

- Low compliance with accepted behaviors within an organization can erode trust between you and your team members, hindering effective collaborations. This can lead to slow responses to threats, making teams vulnerable to cyber-security risks.
- Individuals with low scores in ethics may be unmotivated to handle data responsibly, for example, by obtaining proper consent, securely storing and transmitting data, and respecting user privacy. This increases the risk of data breaches and unauthorized access to sensitive information.

Ownership

Overall Description

You tend to avoid taking responsibility for your actions and decisions. It is unlikely that you feel responsible for your actions or the security of your digital assets, leading to a relaxed attitude towards implementing necessary security measures.

Possible Derailers

- Individuals scoring low on ownership may neglect important security practices, such as regularly updating software, using strong passwords, or implementing multi-factor authentication.
- Individuals are less likely to stay informed about the latest security trends, best practices, or emerging threats, making them more susceptible to social engineering incidents or other forms of cyber incidents.
- Individuals tend to lack preparedness for Cyber Security incidents and have a relaxed approach, they may not try to learn the latest security practices.

Rule Adherence

Overall Description

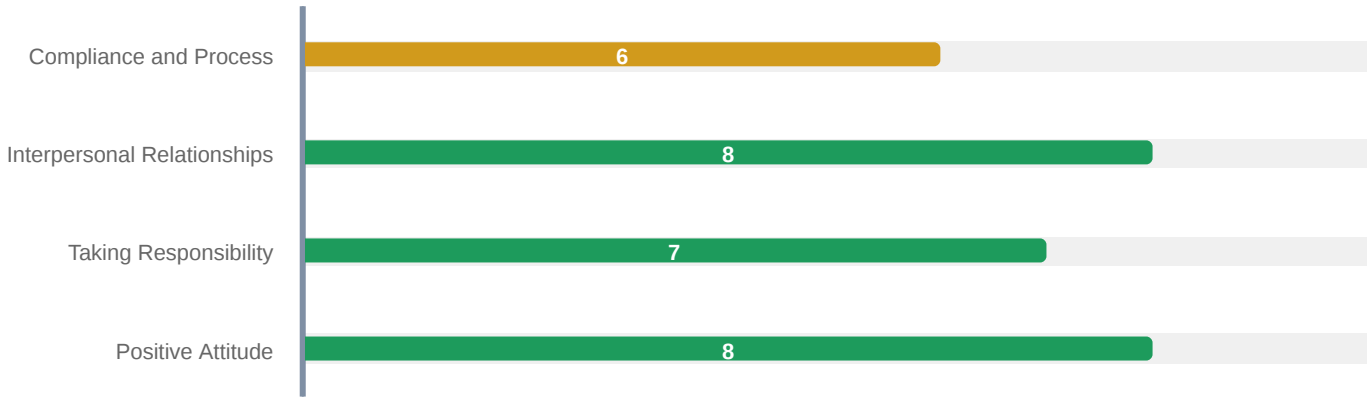
You tend not to follow rules, procedures and conventions at work. This may mean that you have less motivation than most to follow the many best practices and regulations set by your organization for secure online behavior.

Possible Derailers

- By not adhering to rules and guidelines, individuals are less likely to follow established security protocols and tend to overlook critical security measures, such as regular software updates, strong password policies, or encryption protocols, making it easier for cybercriminals to exploit vulnerabilities.
- Scoring low on rule adherence can result in non-compliance with legal and regulatory requirements, such as data protection laws or industry-specific guidelines.
- Individuals tend to be inconsistent in their security practices, making it easier for cybercriminals to exploit vulnerabilities and launch successful incidents.

Cyber Security Risk Competencies

Each personality trait related to risk falls under one of the four below competencies



Values shown in above chart are sten scores

Low(1 - 4) Moderate(5 - 6) High(7 - 10)

2. Cyber Security Risk Competencies:

6

Of 10.0

Compliance and Process: Moderate

You possess a balanced level of rule adherence and proactivity in the context of Cyber Security risk. You demonstrate self-efficacy and ethical behavior, but there is room for further development. By enhancing your skills in rule adherence, proactive risk identification, and ethical decision-making, you can strengthen your ability to effectively manage Cyber Security risks. Strive to be more proactive in identifying potential risks and consistently adhere to established procedures to ensure a secure Cyber Security environment. This can enhance your ability to effectively manage Cyber Security risks and navigate uncertainties. It is important to work on developing traits such as resilience, positivity, openness to change, and persistence. By cultivating these qualities, you can enhance your ability to navigate challenges, embrace change, and maintain a positive and proactive approach to risk management. Building resilience, fostering a positive mindset, and embracing change will contribute to a more effective management of Cyber Security risks. Additionally, by enhancing your ownership, assertiveness and planning skills, you can strengthen your effectiveness in managing Cyber Security risks.

8

Of 10.0

Interpersonal Relationships: High

You may contribute to a positive and collaborative Cyber Security culture within the organization. You are likely to actively seek opportunities to collaborate with others on Cyber Security initiatives. You may value input from colleagues and understand the importance of diversity in opinions, actively contributing to team efforts. It may be clear to you that Cyber Security is a collective effort, and you are likely to actively work towards building strong relationships and fostering a collaborative environment. You may demonstrate altruism in your behavior towards others and are likely to extend a helping hand in case of a Cyber Security crisis.

You are likely social and open to diverse opinions. Your reliability, consistency, and integrity in your actions likely foster trust and confidence in your ability to handle security matters. Others may feel comfortable approaching you with concerns or seeking your guidance. You are likely to demonstrate empathy and understanding towards the concerns and perspectives of others regarding Cyber Security. You may take the time to listen and consider different viewpoints and are likely able to tailor your communication and actions to address the needs and concerns of others.

You are likely able to evaluate the impact of your actions on colleagues and strive to create a supportive and inclusive environment. You understand the value of building a strong professional network and are likely to leverage these relationships to stay informed about emerging trends and best practices.

7

Of 10.0

Taking Responsibility: High

You may take initiatives to identify potential security risks and are likely to take appropriate actions to mitigate them. You are likely to actively seek out vulnerabilities, implement security controls, and make necessary improvements to protect the organization's assets. Additionally, you are likely to pay close attention to detail in Cyber Security practices and meticulously plan the way ahead. You are likely to take ownership of the responsibilities assigned to you to mitigate cyber risks and ensure data protection. You tend to understand the importance of your role in maintaining a strong Cyber Security posture for the organization. You tend to be confident and assertive in your approach to handling any Cyber Security issue. You are likely to invest in understanding procedures such as incident response steps, know how to escalate incidents when necessary, and take appropriate actions to mitigate the impact of incidents. Furthermore, you are likely to actively participate in post-incident analysis and contribute to lessons learned for future improvements.

8

Of 10.0

Positive Attitude: High

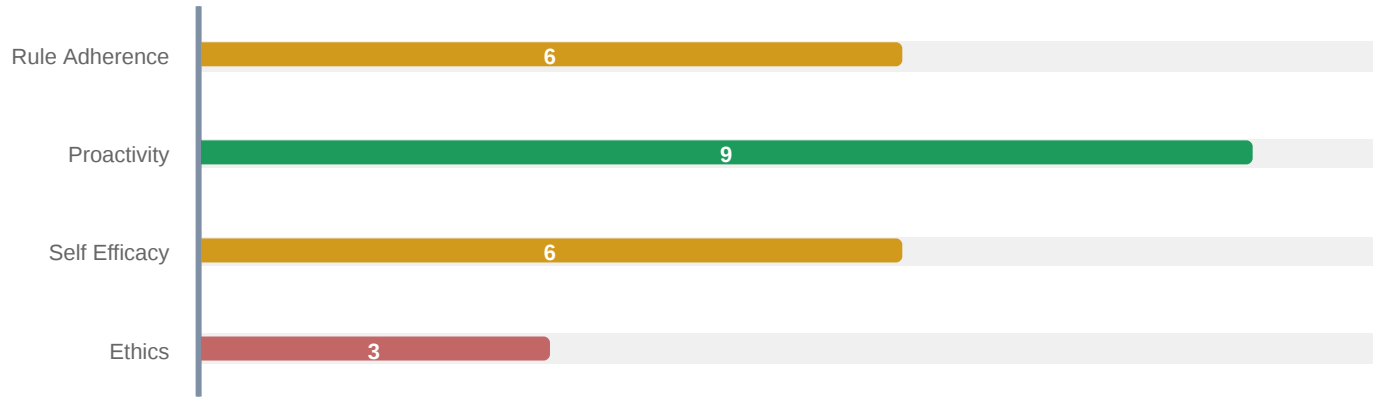
You may maintain a positive outlook and remain resilient in the face of Cyber Security challenges. You may approach problems with a can-do attitude and believe that solutions can be found with persistence. You may not easily get discouraged by setbacks and are motivated to find creative solutions.

You are likely to take a proactive approach to problem-solving in Cyber Security. You may actively identify potential security risks and vulnerabilities and take the initiative to address them. You are open to change and are not afraid to think outside the box and explore innovative solutions to Cyber Security challenges.

It is important to communicate with others in a positive and constructive manner when discussing Cyber Security matters. You may be resilient in your approach to overcoming Cyber Security challenges and inspire others with your positive attitude. You encourage a culture of security awareness and responsibility. People may take inspiration from your persistence, and you are able to influence them to adopt best practices and prioritize Cyber Security.

EVALUATION OF COMPETENCIES

Compliance and Process:



Values shown in above chart are sten scores

Low(1 - 4) Moderate(5 - 6) High(7 - 10)

3. Compliance and Process:

6

Of 10.0

Rule Adherence: Moderate

Rule Adherence is the inclination to strictly follow established rules and procedures in the context of Cyber Security risk, ensuring adherence to regulatory requirements and best practice.

You demonstrate some ability to follow established rules and procedures in the context of Cyber Security risk. While you may occasionally deviate from protocols, you generally understand the importance of compliance and make efforts to adhere to security measures. However, there may be room for improvement in your consistency and attention to detail in following Cyber Security protocols.

9

Of 10.0

Proactivity: High

Proactivity is the proactive engagement in future-oriented behaviors to enact positive change and mitigate Cyber Security risks, taking the initiative to identify and address potential vulnerabilities.

You tend to engage in self-starting, future-oriented behavior to enact positive change rather than waiting for direction. As a result, you are likely to follow Cyber Security rules and respond to potential threats without needing to be prompted.

6

Of 10.0

Self Efficacy: Moderate

Self-Efficacy is the confidence in one's ability to accomplish Cyber Security tasks effectively, demonstrating a belief in one's own competence and skills.

You demonstrate some confidence in your ability to accomplish Cyber Security tasks effectively. While you may occasionally experience self-doubt, you generally possess the necessary skills and knowledge to perform Cyber Security responsibilities. However, there is potential for further development to enhance your self-assurance and belief in your capabilities to effectively handle complex Cyber Security challenges.

3

Of 10.0

Ethics: Low

Ethics is the commitment to uphold a moral code of conduct and a belief in doing the right thing in the context of Cyber Security risk, ensuring ethical behavior and integrity.

You may either prefer not to follow conventional ethical standards or may adhere to your own personal ethical perspective. This can undermine your compliance or erode trust among your team members, hindering effective collaborations. This can lead to slow responses to threats, making teams vulnerable to cyber-security risks.

Interpersonal Relationships:

Values shown in above chart are sten scores

Low(1 - 4) Moderate(5 - 6) High(7 - 10)

4. Interpersonal Relationships:

10

Of 10.0

Openness to Diversity: High

Openness to Diversity refers to the acceptance and respect for individual differences in the context of Cyber Security risk, fostering an inclusive and diverse environment.

You tend to be more open to working with people from diverse set of backgrounds. This is likely to help you build strong relationships with others and benefit from a range of diverse perspectives about how to implement, maintain and defend Cyber Security.

6

Of 10.0

Empathy: Moderate

Empathy is the ability to understand and demonstrate concern for others' feelings, thoughts, and experiences in the context of Cyber Security risk, promoting a supportive and collaborative atmosphere.

You demonstrate concern and understanding for others' feelings, thoughts, and experiences in the context of Cyber Security risk. You may have put yourself in others' shoes, which helps in effective communication, collaboration, and support within the Cyber Security team.

9

Of 10.0

Sociability: High

Sociability is the enjoyment of social interactions and finding the company of others energizing and rewarding in the context of Cyber Security risk, facilitating effective communication and teamwork.

You tend to enjoy meeting new people and networking and tend to be more active in social situations. This is likely to help you work together with others to collectively strengthen Cyber Security practices.

8

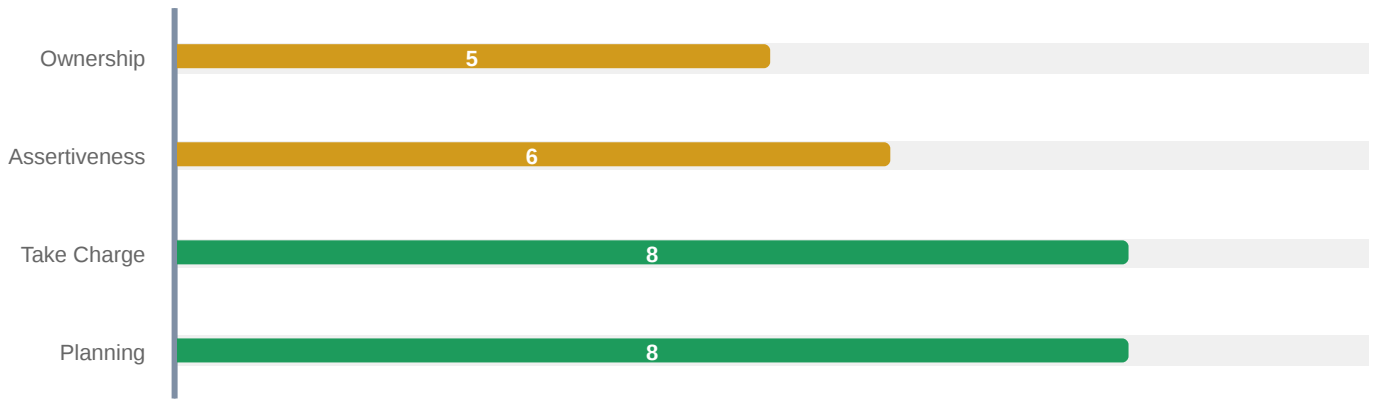
Of 10.0

Altruism: High

Altruism is the active concern for the well-being of others and willingness to help or support someone in need in the context of Cyber Security risk, promoting a culture of collaboration and assistance.

You tend to have an active concern for the well-being of others and a willingness to help or support someone in need. You are likely to help colleagues who have been affected by cyber threats and collaborate to enhance overall security.

Taking Responsibility:



Values shown in above chart are sten scores

Low(1 - 4) Moderate(5 - 6) High(7 - 10)

5. Taking Responsibility:

5
Of 10.0

Ownership: Moderate

Ownership refers to taking ownership of Cyber Security actions and decisions, demonstrating accountability and responsibility, and actively seeking opportunities to improve security measures.

You demonstrate some ability to take responsibility for your actions and decisions in the context of Cyber Security risk. While you may occasionally require guidance or direction, you generally understand the importance of accountability and make efforts to fulfill your Cyber Security responsibilities. However, there may be room for improvement in your consistency and proactive mindset in taking ownership of Cyber Security tasks.

6
Of 10.0

Assertiveness: Moderate

Assertiveness refers to the confident expression of ideas and feelings in a direct and appropriate manner in the context of Cyber Security risk, promoting effective communication and assertive decision-making.

You demonstrate some ability to confidently express your ideas and feelings in the context of Cyber Security risk. While you may occasionally encounter challenges in being assertive, you generally make efforts to communicate effectively and contribute to decision-making processes. However, there may be room for improvement in your assertiveness skills to ensure your Cyber Security perspectives are effectively conveyed.

8
Of 10.0

Take Charge: High

Take Charge refers to the natural inclination to lead in the context of Cyber Security risk, demonstrating initiative and the ability to guide others towards secure practices.

You express a natural tendency to lead. You tend to take control of things and situations and actively lead others to protect digital assets, systems, and information from cyber threats.

8
Of 10.0

Planning: High

Planning refers to the tendency to be well-organized and structured in one's approach to Cyber Security tasks, ensuring systematic and effective risk management.

You tend to keep yourself methodical and systematic with your work. When it comes to handling data and safeguarding it from any potential threats, you are likely to be organized and to plan ahead for them.

Positive Attitude:

Values shown in above chart are sten scores

Low(1 - 4) Moderate(5 - 6) High(7 - 10)

6. Positive Attitude:

10
Of 10.0

Resilience: High

Resilience is the unwavering ability to navigate and overcome Cyber Security challenges with a determined and adaptable mindset, ensuring the security and stability of systems and information.

You are likely to cope well and recover quickly when faced with difficult and stressful situations in the workplace. This is likely to help you to stick with the ongoing need for often uninteresting IT updates and protective behaviors and also to react with strength during high-pressure situations such as cyber incidents.

6
Of 10.0

Positivity: Moderate

Positivity is the inclination to maintain an optimistic outlook in the face of Cyber Security challenges, fostering a constructive and solution-oriented approach to risk management.

You tend to deal with cyber security challenges with a positive approach. You have a problem-solving attitude towards any data breach or cyber incident. This also helps you in effectively collaborating with others and finding innovative solutions to complex Cyber Security issues.

7
Of 10.0

Openness to Change: High

Openness to Change is the willingness to embrace and adapt to evolving Cyber Security practices, demonstrating flexibility and agility in response to emerging threats and technological advancements.

You tend to be open to major work-related changes and have a tendency to adjust appropriately to new work structures, processes, and requirements. IT and Cyber Security needs are constantly evolving, so your openness to change should help you to adapt.

7
Of 10.0

Persistence: High

Persistence is the unwavering commitment to consistently pursue Cyber Security tasks until successful completion, demonstrating resolute determination and unwavering dedication to maintaining a secure environment.

You have a tendency to work towards tasks in a diligent manner, persisting until they are completed, despite distractions or obstacles. You tend to keep yourself motivated until you fully implement cyber-security activities or find a solution to issues such as threats to data integrity.

–

This section provides personalized recommendations to address specific areas of concern (hotspots) and capitalize on strengths.

Ethics

- Gain a clear understanding of ethical principles and their importance in the field of Cyber Security. Familiarize yourself with professional codes of conduct, industry standards, and legal regulations that govern ethical behavior in Cyber Security.
- Develop a habit of documenting your work processes and procedures. This can help ensure that you are following the established rules and guidelines consistently. Keep records of your activities and any deviations from the rules, along with justifications and corrective actions taken.
- Respect and protect the confidentiality and privacy of sensitive information. Understand the importance of safeguarding personal and organizational data and ensure compliance with privacy regulations.
- Promote responsible use of technology by adhering to ethical guidelines and best practices. Avoid engaging in activities that may compromise the security or privacy of individuals or organizations.
- Encourage a culture of reporting and ensure that appropriate actions are taken to address ethical violations.

Ownership

- Take personal responsibility for Cyber Security risk management. Recognize that you play a crucial role in protecting your organization's systems, data, and networks. Understand the potential consequences of not taking ownership of Cyber Security risks.
- Clearly communicate roles, responsibilities, and expectations to ensure everyone understands their ownership in managing Cyber Security risks.
- Hold yourself accountable for your actions and decisions related to Cyber Security risk management.
- Report any identified risks, vulnerabilities, or incidents promptly and accurately. Take ownership of implementing corrective actions and ensuring their effectiveness.
- Set a positive example for others by demonstrating ownership in Cyber Security risk behavior. Encourage and support your colleagues in taking ownership of their responsibilities.
- Foster a culture of ownership by promoting awareness and understanding of the importance of Cyber Security risk management.
- Embrace a growth mindset and view mistakes as learning opportunities. Reflect on past experiences, identify areas for improvement, and learn from your mistakes. Use these lessons to enhance your ownership and risk management practices.

Rule Adherence

- Cyber Security training, awareness programs, and regular reminders about security practices. By emphasizing the importance of following established rules, organizations can enhance their overall security posture and reduce the likelihood of successful cyber incidents.
- Take the time to familiarize yourself with the Cyber Security policies, regulations, and best practices relevant to your organization and industry.
- Understand the specific rules and guidelines that govern your work and the consequences of non-compliance. Participate in regular audits and assessments of your organization's Cyber Security practices. This can help identify any gaps or areas of non-compliance.
- Use the findings to improve your adherence to the rules and address any identified weaknesses.
- Stay updated on the latest rules and regulations in the Cyber Security field.
- Engage in continuous learning to enhance your knowledge and understanding of rule adherence.
- Attend industry conferences, read relevant publications, and participate in online forums or communities to stay informed.

Test Log

3rd Jun 2024

01:25 PM Started the test with Inventario della Personalità

01:48 PM Finished the test

About the Report

This Report is generated electronically on the basis of the inputs received from the assessment takers. This Report including the AI flags that are generated in case of availing of proctoring services, should not be solely used/relied on for making any business, selection, entrance, or employment-related decisions. Mettl accepts no liability from the use of or any action taken or refrained from or for any and all business decisions taken as a result of or reliance upon anything, including, without limitation, information, advice, or AI flags contained in this Report or sources of information used or referred to in this Report.