في إطار جهود المركز الوطني للأمن السيبراني في حوكمة الأمن السيبراني على المستوى الوطني وبموجب المادة (6-أ / 6-ب) من قانون الأمن السيبراني رقم 16 لعام 2019 ، قام المركز بتطوير إطار تنظيمي (الإطار الوطني الأردني للأمن السيبراني) متطوّر وفعال يواكب الممارسات العالمية الفضلى لتطوير المنظومة الدفاعية للأمن السيبراني على المستوى الوطني لجميع المؤسسات العامة والخاصة ولمواجهة التهديدات السيبرانية بكفاءة وفاعلية وتخفيف الأثر الناتج من تحقق المخاطر السيبرانية المختلفة من خلال تطوير القدرات الفنية والبشرية والإدارية في المؤسسات.

حيث يتكون الإطار التنظيمي من مجموعة من السياسات والإجراءات والآليات والضوابط التي يجب على المؤسسات العامة والخاصة اعتمادها وتنفيذها لتعزيز أمان أنظمتها السيبرانية لتحقيق الحماية التكاملية على المستوى الوطني. ويهدف الإطار التنظيمي إلى الارتقاء بالأردن ليكون من الدول الرائدة في الأمن السيبراني من خلال دفع نمو عجلة الاقتصاد الوطني وتعزيز القدرة والرشاقة المؤسسية والبشرية على التعامل مع التهديدات والمخاطر السيبرانية المحتملة وتقليل تأثيرها السلبي على المؤسسة وعلى المملكة ككل.

ومن المبادئ الرئيسية التي يعتمد عليها الإطار التنظيمي:

- توفير القدرة التنظيمية: يهدف الإطار التنظيمي إلى توفير الهيكلية التنظيمية اللازمة للمؤسسات لتنفيذ استراتيجيات الأمن السيبراني وتنفيذ السياسات والإجراءات ذات الصلة.
- تعزيز الوعي والتدريب: يركز الإطار التنظيمي على زيادة الوعي بالتهديدات السيبرانية وتعزيز قدرة المؤسسات على التعامل معها من خلال تدريب الموظفين وتوفير الموارد التعليمية اللازمة.
- تطوير السياسات والإجراءات: يساعد الإطار التنظيمي على تطوير وتحسين السياسات والإجراءات المتعلقة بالأمن السيبراني في المؤسسات، بما في ذلك إدارة المخاطر والتعامل مع الحوادث والاستجابة السريعة للتهديدات.
- تعزيز التعاون: يشجع الإطار التنظيمي على التعاون بين المؤسسات المختلفة والجهات المعنية لتبادل المعلومات والخبرات وتعزيز قدرة الاستجابة الجماعية للتهديدات السيبرانية.
- التقييم والمراجعة المستمرة: يتضمن الإطار التنظيمي آليات لتقييم ومراجعة المنهجيات المتبعة في تحقيق مستويات النضوج المستهدفة.

وبموجب المادة (8-ب-1) من قانون الأمن السيبراني رقم 16 لعام 2019 تلتزم الوزارات والدوائر الحكومية والمؤسسات الرسمية والخاصة والأهلية باتباع السياسات والمعايير والضوابط الصادرة عن المركز لكل قطاع وذلك لمواجهة التهديدات السيبرانية المتزايدة التي من شأنها تقويض البنية التحتية التقنية.

المركز الوطني للأمن السيبراني
National Cyber Security Center

Cybersecurity Framework Booklet

Jordan National Cybersecurity Framework Philosophy and Main Capabilities

The National Cybersecurity Framework of the Hashemite Kingdom of Jordan

Table of Contents

As part of the efforts of the National Cyber Security Center of Jordan in regulating cybersecurity at the national level and in accordance with Article (6-A / 6-B) of Cyber Security Law No. 16 of 2019, the center has developed an advanced and effective regulatory framework (Jordan's National Cyber Security Framework - JNCSF) that aligns with global best practices for developing the national cybersecurity defense system for all public and private institutions. The framework aims to address cyber threats and mitigate the impact of potential cyber risks by enhancing technical, human, and administrative capabilities within institutions efficiently and effectively.

The regulatory framework consists of a set of policies, procedures, mechanisms, and controls that public and private institutions must adopt and implement to enhance the security of their cyber systems and achieve comprehensive protection at the national level.

The objective of the regulatory framework is to position Jordan as a leading country in cybersecurity, promoting the rapid growth of the national economy, and enhancing institutional and human capacity to deal with cyber threats and potential risks, while minimizing their negative impact on the organization and the kingdom.

Management Framework
Complementing
Enabling
Empowering

The key principles on which the regulatory framework relies are as follows:

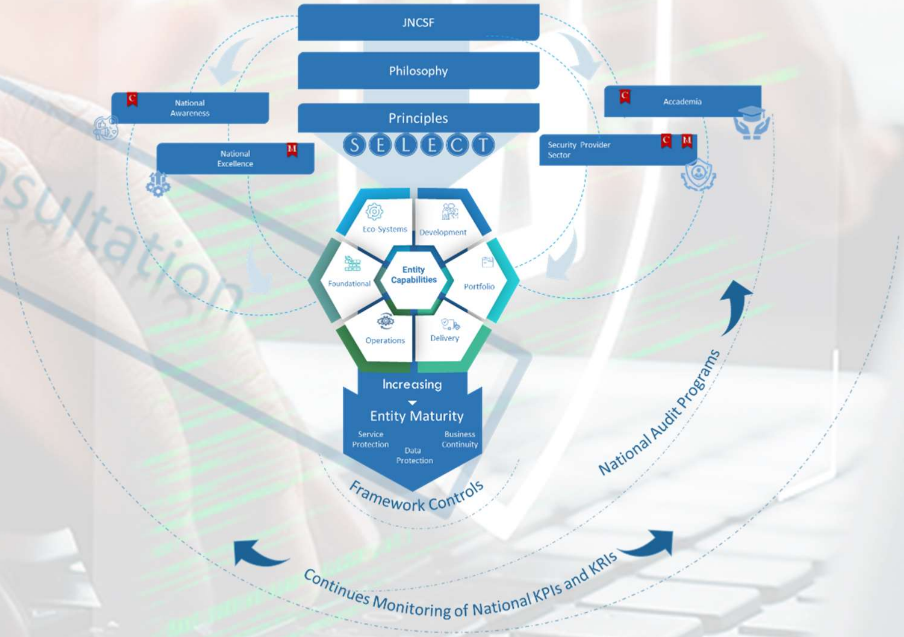
Organizational Capability: The regulatory framework aims to provide the necessary organizational structure for institutions to implement cybersecurity strategies and enforce relevant policies and procedures.

Awareness and Training: The regulatory framework focuses on increasing awareness of cyber threats and enhancing the capacity of institutions to deal with them through employee training and providing necessary educational resources.

Policy and Procedure Development: The regulatory framework helps develop and improve policies and procedures related to cybersecurity in institutions, including risk management, incident handling, and rapid response to threats.

Collaboration Enhancement: The regulatory framework encourages collaboration among different institutions and stakeholders to exchange information, expertise, and enhance collective response capabilities to cyber threats.

Continuous Assessment and Review: The regulatory framework includes mechanisms for continuous assessment and review.



In accordance with Article (8-B-1) of Cyber Security Law No. 16 of 2019, ministries, government departments, official, private, and civil institutions are committed to following the policies, standards, and controls issued by the center for each sector to address the increasing cyber threats that can undermine the technical infrastructure.

Jordan National Cybersecurity Framework Philosophy

Cyber Threats threaten every element of our presence, including personal finance and identities, the national economy, critical infrastructure, and even public safety, and since Information and Technologies became tightly integrated with almost every service offered or consumed by Jordanian citizens, all Jordanian citizens will assume a different level of responsibility and or accountability to protect the nation from what it might be called a cyberattack or cyber threat, where maintaining national cyber security against cyber threats would be a comprehensive obligation for both individuals and entities.

Therefore, the service provider for a Jordanian citizen or those with the right to live in the Hashemite Kingdom of Jordan, regardless of the type of the service provider, if he comes from the local or foreign community, or If he works in the private or public sector, they must all be fully aware of the risk of cyberattacks and submit all the necessary and available services to improve cybersecurity and thwart all potential threats on the national level.

The phrase "For want of a nail the kingdom was lost" highlights the idea that small actions or oversights can have significant consequences. It is often used to illustrate the importance of paying attention to even the smallest details, as they can have a significant impact on the outcome of a situation, so, we highlight here that the protection is for all data and services types that could be invested to be an asset for entities, that might be related to Jordanian citizens or national resources are treated as national assets and need to be highly protected, where Everything is connected in the digital age, and even the simplest things can have a big impact on our lives. To ensure the effectiveness of the protection procedure and avoid electronic security breaches, it is vital to ensure the security of all tiny information, data and services before the large one In order to avoid any outlet for an attack, cyber, or security breach

The Jordanian National Cybersecurity Philosophy is based on this idea, the idea of losing the nail topples a kingdom, not because it is a nail, but because it is part of a whole, and its loss makes a loophole (a gap), if its place is filled with a threat that spreads and moves from one place to another, corrupting the whole, then this empty gab for this lost nail becomes the gateway to the danger that toppled in the Kingdom.

The approach used in The Jordanian National Cybersecurity Freamwork is the national security approach, which will be addressed below.

National Security

The kingdom, which faces political, economic, topographical, and even climatic obstacles, prides itself on being safe and secure, it even adopted the " Country of Safety and Security " as its main slogan.

The Hashmi kingdom of Jordan proudly complies with all national and international safety regulations, both traditional and electronic, which has enhanced the credibility of its slogan. And based on its concern for national security that affects all facets of life and ensures the protection of its citizens, lands, and interests from internal and external threats, regardless of the nature of the resource of these threats, national security policies and practices are designed to safeguard a country's citizens and ensure the sovereignty and stability of the nation.

National security encompasses a broad range of areas, including military, diplomatic, economic, and intelligence activities. It involves not only protecting against threats but also promoting stability and peace through strategic alliances and partnerships. Effective national security strategies require a coordinated effort from multiple government agencies, as well as input from private entities and citizens.

Defense policy and military strategy, intelligence gathering and analysis, border and transportation security, emergency management, and cybersecurity are a few of the important sectors of national security, which justifies considering that national security is an ongoing concern for every nation, this requires ensuring the development of policies and strategies used to achieve national security, as well as ensuring that these policies and strategies are adapted to face evolving threats and challenges.

National cybersecurity programs

National Cybersecurity Programs refer to the comprehensive initiatives and strategies that a country adopts to protect its digital assets, infrastructure, and citizens from cyber threats. These programs may include various activities such as developing cybersecurity policies, establishing legal frameworks and regulations, conducting awareness campaigns, creating a cybersecurity workforce, building cyber-defense capabilities, and collaborating with international entities.

These national cybersecurity programs are essential in today's digital age as they provide the necessary protection and resources to defend against cyber threats.

Cybersecurity in Digital Age

Digital transformation enables businesses to provide better customer experiences using digital channels, such as websites, social media, and mobile applications. This can lead to increased citizen and customer satisfaction, loyalty, and retention, contributing to the growth of the national digital business index.

The ability to collect and analyze large amounts of data is made possible by digital transformation, which improves work efficiency and decision-making. Entities that use data in decision-making and implement digital transformation in this area also experience higher levels of profitability and growth.

Digital transformation has a significant impact on the digital business indicator, which measures the performance of digital businesses in a particular industry or region. Digital transformation involves the integration of digital technologies into all aspects of business operations, leading to increased efficiency, innovation, and agility.

Digital business has had a significant impact on the national business indicators which measure the performance of the overall economy of a country, and since digital business is becoming more prevalent, it has had a significant impact on a number of factors that influence the national business indicators, including:

Economic Growth
Innovation
Decision-making Based on Data
Globalization

Factors That Influence the National Business Indicators

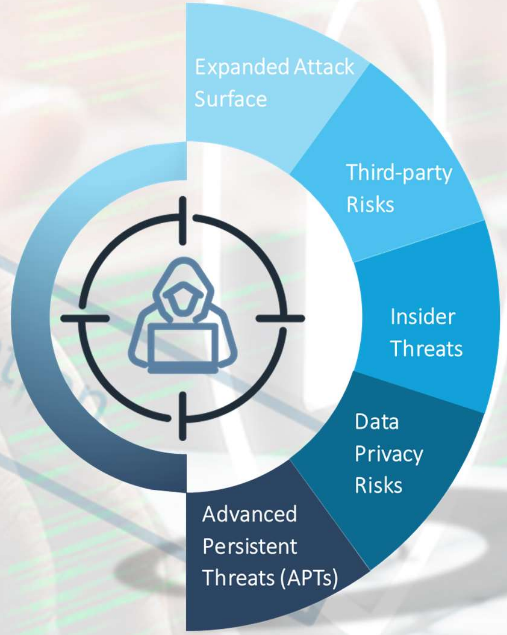
1. **Economic Growth:** Digital business has the potential to increase economic growth by providing opportunities for businesses to expand their reach and connect with new customers.

2. **Innovation:** Digital business has also led to increased innovation, with government and companies developing new products and services to meet changing customer demands. This can lead to higher levels of research and development, which can contribute to increased competitiveness and a stronger economy.

3. **Globalization**: Digital business has made it easier for businesses to connect with customers and partners in other countries, contributing to increased globalization. This can increase trade, investment, and cross-border collaborations, all of which can have a positive impact on the national business indicator.

4. **Decision-making Based on Data**: Digital business has simplified the way for entities to gather and analyze data, which can guide tactical decision-making. As a result, any entity processes may become more effective and efficient, which would promote overall economic growth and competitiveness.

In abbreviation, business indicators at the national level have been significantly impacted by digital business, which has also boosted innovation, internationalization, and data-driven decision-making. The influence of digital business on national business indicators, however, may differ based on variables like the extent of a nation's digital adoption, the regulatory climate, and the accessibility of digital infrastructure, In addition to awareness of digital threats and how to address them, due to the increased use of automation in all procedures involving sensitive and important data and information, the prospect of national cybersecurity threats was also arising, as there were many factors supporting the exacerbation of this kind of threats, we highlight the following:



1. **Expanded Attack Surface**: As firms adopt new technologies like cloud computing and the Internet of Things (IoT), the attack surface grows, giving cybercriminals more opportunities to conduct assaults.

2. **Third-party Risks**: Working with third-party suppliers and vendors is a common aspect of the digital transformation process. Nevertheless, because cybercriminals might exploit them to obtain illegal access to a

goverment and company's networks and data, these third-party connections could create additional cybersecurity vulnerabilities.

3. **Insider Threats**: Digital transformation can also increase the risk of insider threats, as employees may have access to more data and systems than ever before. Insider threats can occur intentionally or unintentionally and can be difficult to detect and prevent.

4. **Data Privacy Risks**: As entities collect and store more data, they become more vulnerable to data breaches, which can result in the loss or theft of sensitive information. Data privacy regulations, also increase the risk of non-compliance and the associated legal and financial penalties.

5. **Advanced Persistent Threats (APTs)**: APTs are sophisticated and targeted attacks that can go undetected for long periods of time. Digital transformation can make it easier for APTs to infiltrate an entities network, as they often exploit vulnerabilities in outdated or poorly secured.

Highlights of Jordan National Cyber Security Philosophy

1. Institutionalize Cybersecurity Risk Management across the Nation.

2. Transforming from COE as Center of Excellence to COE as Center of Enablement, where the National Cyber Security Center will develop programs to help Every Organization to become Cyber Security Center of Excellence.

3. Empower National Sector Regulators to Elevate the Sector Cyber Security Maturity Index

4. Cyber Security is Not a Technology Issue, Technology is One Third Only.

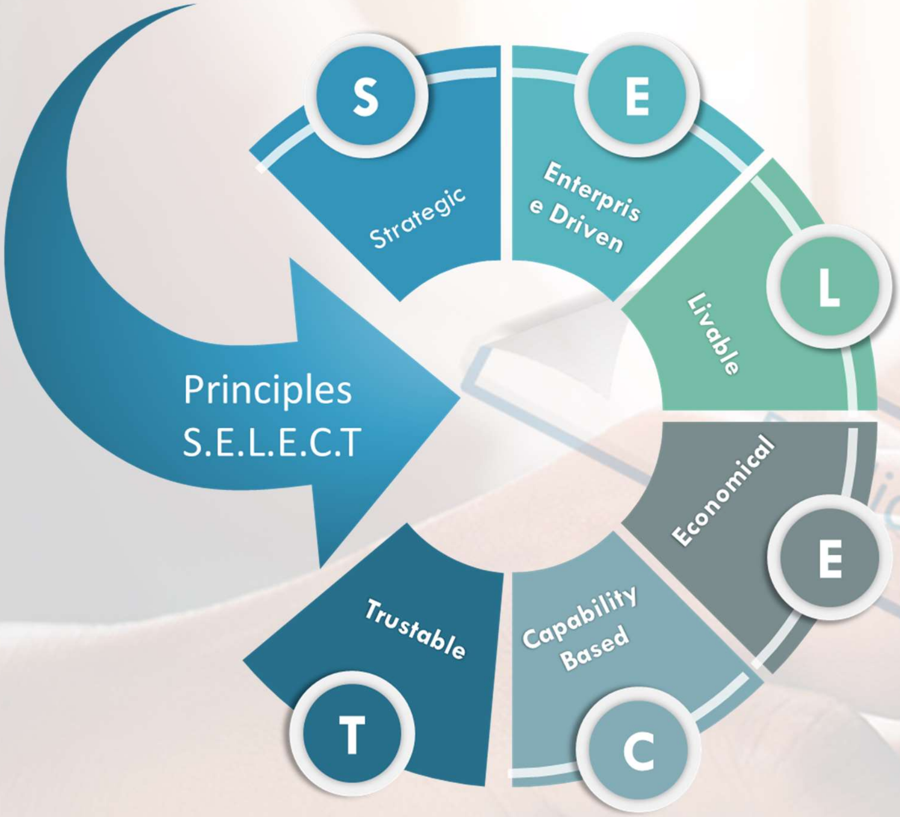
5. Promote the concept of Cyber Security Economics to help every organization develope a sophisticated, economically driven and cyber risk measurements that blends into their business plan.

6. Build the National Cyber Security Defender spirit in every Jordanian Citizen.

7. Build and Sustain National Capabilities through Accademia.

8. Promote, direct and enable building National Cybersecurity Products and Solutions to Minimize Third Party Risks.

Principles S.E.L.E.C.T



Strategic

Strategic

- Cyber Security as Strategic Objective
- National Concern, Every One is Responsible and Accountable
- Protecting Data and Services
- Business Problem Not Technology Problem
- Protecting Data and Services
- Information and Data are assets
- Integrated in Digital Strategy
- Protecting the Eco System

Cyber Security as Strategic Objective

Driving business without strategy and strategic objective is disorientation, cybersecurity without strategy and strategic objectives is a nightmare, disconnected strategies is a killer.

Having a clear strategy and set of strategic objectives is essential for any business or organization, including those working in the field of cybersecurity. A strategy is a long-term plan for achieving specific goals, while strategic objectives are specific, measurable targets that help an organization move towards its overall strategy. Without a strategy and strategic objectives, a business or organization can become disoriented and may struggle to achieve its goals. In the field of cybersecurity, this can be particularly problematic, as the risks and threats faced by organizations are constantly evolving and can be very complex. Without a clear strategy and set of objectives to guide their actions, organizations may struggle to effectively protect themselves and their customers from cyber threats. Disconnected strategies, or strategies that are not aligned with one another, can also be a major problem, as they can lead to confusion and

inefficiencies. It is important for organizations to carefully consider their goals and objectives and to develop a cohesive, well-defined strategy that can help them effectively navigate the challenges they face.

Here are a few more points to consider when it comes to the importance of having a strategy and strategic objectives:

- A strategy helps to define the overall direction of an organization and provides a framework for decision making. It allows an organization to focus its resources and efforts on the most important goals and to allocate its resources effectively.
- Strategic objectives provide specific, measurable targets that help an organization track its progress and stay on course. They also help to ensure that everyone in the organization is working towards the same goals and can be held accountable for their contributions.
- Without a clear strategy, an organization may struggle to effectively navigate the challenges it faces and may end up reacting to problems rather than proactively addressing them. This can lead to inefficiencies and missed opportunities.
- In the field of cybersecurity, having a clear strategy and set of objectives is particularly important because of the constantly evolving nature of the threats faced by organizations. A well-defined strategy can help an organization stay ahead of potential threats and be better prepared to respond to them when they do arise.
- Disconnected strategies can be a major problem, as they can lead to confusion and inefficiencies. It is important for an organization to ensure that all of its strategies are aligned and working towards the same goals.

National Concern, Every One Is Responsible and Accountable

Cybersecurity is a national concern; everyone is responsible and accountable

Cybersecurity is a national concern because it affects the overall security and stability of a country. The increasing reliance on technology and the internet has made it easier for cyber criminals to gain access to sensitive information and disrupt critical systems and services. This can lead to financial losses, damage to reputation, and even physical harm in certain cases. It is therefore essential that everyone takes responsibility for their own cybersecurity and works to protect their own systems and data. At the same time, everyone must also be accountable for their actions and take care not to expose others to cyber risks. This requires a collective effort from individuals, organizations, and government entities to educate and raise awareness about cybersecurity, implement effective security measures, and work together to respond to and prevent cyber-attacks.

In today's digital age, cybersecurity is a major concern for everyone, not just those working in the field of technology. With the increasing amount of personal and sensitive information stored online and offline, and the reliance on technology for everything from banking and shopping to communication and entertainment, it is more important than ever to ensure that our systems and data are secure which are critical for individuals and organizations from various sectors

The entity also has a responsibility to protect their citizens data, as well as their own systems and operations. This includes implementing strong security measures, training employees on how to identify and prevent cyber threats, and having a plan in place to respond to and recover from any attacks that do occur. However, cybersecurity is not just the responsibility of IT professionals, every individual within the entity has a role to play in protecting themselves and their information

Overall, cybersecurity is a national concern because it affects everyone and requires a collective effort to address. By being responsible and accountable, we can work together to protect ourselves and our communities from cyber threats.

Business Problem Not Technology Problem

Cybersecurity is a business problem, it is not a technology problem.

This is a statement that is becoming increasingly recognized by government entities around the world. While it is true that technology plays a crucial role in maintaining the security of an organization's systems and data, it is ultimately the business practices and policies that determine the effectiveness of those technological safeguards.

One of the primary reasons that cybersecurity is a business problem is because it is closely tied to an entity's risk management strategy. Cyber threats are constantly evolving and can come in many different forms. It is the responsibility of the business leaders to measure the potential risks and implement measures to mitigate them. This includes not only the use of technology, but also the development and enforcement of policies and procedures to ensure that employees are aware of and follow best practices for cybersecurity.

Another reason that cybersecurity is a business problem is that it affects the bottom line. The cost of a data breach can be significant, This can include the cost of repairing the damage done, as well as the cost of lost business due to the disruption caused by the breach. All of these costs can have a significant impact on a entity's financial performance.

Protecting Data and Services

Cybersecurity is concerned with protecting the known services and data, and protecting the value of data which is not yet known.

Cybersecurity is concerned with protecting the known data and services that are essential to individuals, businesses, and entities. This includes sensitive information such as personal financial data, intellectual property, and confidential entity information.

However, cybersecurity also plays a role in protecting the value of data that is not yet known. As new technologies and innovations emerge, data and information that was previously unknown or undiscovered may become valuable. By ensuring that this data is secure and protected, cybersecurity helps to preserve its value and prevent it from being exploited or misused.

Protecting the value of data that is not yet known is a complex and multifaceted challenge, as it requires anticipating the potential value of data and taking steps to protect it before it becomes valuable. This can involve a range of measures, such as implementing strong security measures to prevent unauthorized access or tampering, establishing clear policies and guidelines for the use and handling of data, and if needed investing in technologies and systems that enable the secure storage and management of data.

One key element of protecting the value of unknown data is ensuring that it is properly collected, processed, and stored. In addition, it is important to have a clear understanding of the legal and regulatory frameworks that govern the use and handling of data. This can help to ensure that data is used in a responsible and ethical manner, and to prevent violations of laws or regulations that could compromise the value of the data.

Protecting the data, services and the value of unknown data requires a proactive and comprehensive approach that combines technical, legal, and ethical considerations. By taking steps to ensure the security and integrity of data and services, entities and individuals can achieve their business goals

Information and Data are Assets

Information is asset like any national asset, if someone can measure it, steal it, benefit from it, we have to protect it

Information has value and can be used to benefit entities and countries. Just like physical assets, it is important to protect information from being stolen or misused. This is especially true in the digital world where information can be easily accessed and shared. It is important for individuals and entities to take steps to secure their information and prevent unauthorized access or use.

In addition, it is important to recognize that information is a valuable resource that can be used to make informed decisions and drive progress. This is true for goverment and companies as well as entities. For example, businesses rely on information about their customers, competitors, and market conditions to make

strategic decisions and stay competitive. Governments also rely on information to make policy decisions and allocate resources. In short, information is a powerful tool that can be used to drive success and progress.

However, this also means that information can be used for malicious purposes if it falls into the wrong hands. This is why it is so important to protect information and prevent it from being accessed or used without permission.

Overall, it is clear that information is an asset that must be protected in order to maintain privacy and security. By taking steps to secure information and prevent unauthorized access or use, entities can ensure that this valuable resource is used responsibly and to the benefit of all.

Integrated in Digital Strategy

Automation and Digital Transformation is innovation focusing on disruption, cybersecurity and digital transformation are 2 faces of the same coin, no one should overcome the other.

Automation and digital transformation are two key trends that are driving innovation in today's business world. Both are focused on disruption and are leading to significant changes in how organizations operate and compete. However, these two trends also have an important relationship with cybersecurity. In fact, automation and digital transformation and cybersecurity are two sides of the same coin, and neither should be prioritized over the other.

Automation and digital transformation are about making processes and systems more efficient, more effective, and more responsive to the needs of the business. This can be achieved through the use of technologies such as artificial intelligence, machine learning, cloud services and the Internet of Things. Automation is helping to reduce human error, improve accuracy, and increase productivity, while digital transformation is enabling organizations to create new business models and revenue streams.

Cybersecurity, on the other hand, is about protecting the organization's assets, data, and reputation. With more and more information and systems moving online, cybersecurity is becoming more important than ever. Cyber threats such as malware, phishing, and ransomware are on the rise, and organizations must be prepared to defend against these threats. This includes implementing security controls, such as firewalls and antivirus software, as well as educating employees about the risks and how to spot and avoid them.

The key to successfully balancing automation, digital transformation, and cybersecurity is to ensure that security is built into the design and implementation of new business systems and processes. This means that security should be considered at every stage of the process, from the initial planning and design stages, to the testing and deployment phases. Additionally, regular security assessments and penetration testing should be performed to identify vulnerabilities and ensure that the organization's defenses are robust and up-to-date.

Protecting the Eco System

Protecting our organization is not enough, we need to protect or help others to protect themselves to protect ourselfs.

Cybersecurity is no longer just about protecting our own organization's assets and data, it's about protecting the broader ecosystem that your organization operates in. This means that in order to truly protect yourself, you must also help others protect themselves.

When it comes to cybersecurity, the weakest link can often be the one that causes a data breach or cyber attack. This can include third-party vendors and suppliers, customers, or even employees. If a vendor or supplier's network is compromised, it can provide a gateway for attackers to access our organization's data. Similarly, employees who fall for a phishing attack or use weak passwords can provide a point of entry for attackers. And customers who don't properly protect their own data can make it vulnerable to attack, potentially leading to a data breach or loss of sensitive information.

Therefore, it's essential that organizations take a proactive approach to cybersecurity and not only focus on protecting their own assets, but also help others protect themselves. This includes educating employees and customers about cyber threats, best practices for staying safe online, and warning signs of an attack.

One way to help others protect themselves is to share information about threats and vulnerabilities. This can be done through regular communication with other organizations, including suppliers and partners, as well as through participation in information-sharing organizations and initiatives. By sharing information about known threats and vulnerabilities, organizations can help each other identify and mitigate risks.

Another way to help others protect themselves is to provide training and education. Many cyber attacks are successful because employees are not aware of the risks or do not know how to protect themselves. By providing training and education on cybersecurity best practices, organizations can help employees understand the risks and take steps to protect themselves.

By protecting others and making sure that our vendors, partners, and customers are also secure, you can also lower the risk of an attack happening to us. When other companies are more secure, they are less likely to be compromised and fall victim to an attack, which means the attackers will have a much harder time using that compromised company to reach our organization. By assisting with the security of our partners and vendors, we are not only protecting them, but also creating a secure environment for our business as well.

Enterprise Driven

- Cybersecurity Architecture
- Organizational DNA Analysis
- Security in Depth and Security by Design
- Granular and Multi-Tier Risk Management Responsibilities
- Cybersecurity Policies as Hierarchy

Enterprise Driven

Cybersecurity Architecture

Architecting security need fundamental architecting change, design and redesign of current organizational architecture, security by design is fundamental, cosmetics surface can be scratched easily.

"Architecting security" refers to the process of designing and implementing a comprehensive security plan for an organization. This often involves making fundamental changes to the organization's current architecture, including its systems, processes, and policies. In order to effectively architect security, it is important to adopt a "security by design" approach, which means incorporating security considerations into the design and development of all systems and processes from the outset. This is often referred to as "security by design" or "security by default."

One of the key challenges in architecting security is the need to balance security with other important considerations such as usability, cost, and flexibility. It is important to find the right balance so that security measures do not unduly burden users or inhibit the organization's ability to achieve its goals.

Another important aspect of architecting security is the need to be proactive and to anticipate potential threats and vulnerabilities. Simply "scratching the surface" with cosmetic security measures is not sufficient. Instead, it is important to design systems and processes with security in mind from the ground up, in order to provide the most robust and effective protection possible.

Here are a few more points to consider when it comes to architecting security:

- Security needs to be integrated into all aspects of an organization's systems and processes, not just added on as an afterthought. This means that security needs to be considered at every stage of the design process, from planning and development to testing and deployment.

- It is important to adopt a risk-based approach to security, in which the level of protection is tailored to the specific risks faced by the organization. This allows an organization to prioritize its efforts and allocate its resources most effectively.

- In order to be effective, security measures need to be regularly reviewed and updated to ensure that they are still relevant and effective. This is particularly important in the fast-changing world of cybersecurity, where new threats and vulnerabilities are constantly emerging.

- It is also important to educate and train employees on the importance of security and to ensure that they understand their role in helping to protect the organization. This can include providing training on topics such as secure password management, phishing scams, and how to spot and report potential threats.

- Finally, it is essential to have a clear and well-communicated security policy that outlines the organization's approach to security and sets out the responsibilities of all employees in relation to security. This can help to ensure that everyone in the organization is working towards the same goals and is aware of their role in helping to protect the organization.

Organizational DNA Analysis

Because only those who are doing the specific job know deeply what they are doing, only those can better measure the risk, Applying the concept : for the want of a nail the Kingdom fall down.

The old adage "for want of a nail" is often used to emphasize the importance of small details in larger systems, and it is especially relevant in the realm of cybersecurity. The security of a system is only as strong as its weakest link, and it is often the small, seemingly insignificant details that can leave it vulnerable to attack.

One of the key challenges in cybersecurity is accurately assessing risk. When it comes to protecting a system, it is important to be able to identify potential vulnerabilities and understand the potential impact of a successful attack. However, because the threat landscape is constantly evolving and the methods used by attackers are constantly changing, it can be difficult to predict the likelihood of a given vulnerability being exploited.

One way to better measure risk is by having a deep understanding of the systems and processes that we are responsible for protecting. This means taking the time to familiarize ourself with the technical details of the systems in question, including how they are configured and how they are used. It also means being aware of the ways in which different systems and processes interact, and understanding how changes to one system might impact the security of others.

Furthermore, security experts should always be up-to-date with the latest threats, trends, and techniques used by attackers. This helps them to identify the risk and take necessary preventive measures. In addition, they should conduct regular security assessments, testing the systems and identifying potential vulnerabilities that might have been missed.

In conclusion, Accurately measuring risk is an essential part of cybersecurity, and one of the keys to success is having a deep understanding of the systems and processes that we are responsible for protecting. Because only us know deeply what we are doing, only us can better measure the risk. Regular security assessments, knowledge of the latest threats and techniques and having a comprehensive incident response plan are important steps in achieving this understanding and improving the overall security posture. "For want of a nail" illustrates the point that small details can have a big impact, by paying attention to those small details, we can help to ensure that our systems and processes are as secure as possible.

Security in Depth and Security by Design

Bad guys do systematic microscopic analysis of our organization, process, and activities, to be able to race with them we should do the same, analyzing the organization is critical and mandatory, but it is not an easy job, it should be done continuously, systematically, deeply, granularly and always to be governed.

The process of conducting a thorough analysis of an organization in order to identify potential vulnerabilities or weaknesses that could be exploited by "bad guys." This process may involve examining various aspects of the organization, including its goals, processes, activities, roles and responsibilities, location and geographics, triggers and events as well as things, materials and systems. By conducting a systematic, microscopic analysis of the organization, it may be possible to identify potential vulnerabilities or areas for improvement, and take steps to address them.

It is important to note that this type of analysis is not an easy task and requires a significant amount of time, resources, and expertise. It is also important to conduct the analysis continuously, as the organization and its environment may change over time, potentially introducing new risks or vulnerabilities. Additionally, it may be necessary to approach the analysis in a granular, detailed manner in order to identify all potential risks and vulnerabilities.

Overall, the process of analyzing an organization is critical and mandatory in order to identify potential vulnerabilities and take steps to protect the organization from potential threats. However, it is a complex and ongoing process that requires significant resources and expertise to be done effectively.

One key aspect of the analysis may be to identify potential vulnerabilities or weaknesses within the organization. These may include inefficiencies in processes, gaps in security measures, or inadequate policies or procedures. By identifying these vulnerabilities, the organization can take steps to address them and reduce the risk of harm or loss.

It is also important to consider the organization's external environment when conducting this type of analysis. This may include factors such as the competitive landscape, regulatory environment, and economic conditions. By understanding these external factors, the organization can better anticipate and prepare for potential risks or challenges.

Overall, the process of analyzing an organization is complex and requires significant resources and expertise. It is also an ongoing process, as the organization and its environment are likely to change over time, potentially introducing new risks or vulnerabilities. By continuously and systematically examining the organization, it is possible to identify potential vulnerabilities and take steps to mitigate them, reducing the risk of harm or loss.

Granular and Multi-Tier Risk Management Responsibilities

Organization is a sophisticated multidimensional structure, but it is decomposable.

An organization is a complex entity that is made up of many different parts or components. These components may include people, processes, systems, structures, and culture, among others. An organization may also operate in multiple dimensions, such as geographic regions, business units, or functional areas.

Despite this complexity, it is possible to decompose an organization into its various components and dimensions in order to study and understand it more effectively. Decomposing an organization means breaking it down into smaller, more manageable parts in order to more easily analyze and understand it. This may involve examining specific aspects of the organization, such as its processes, systems, or structures, in order to understand how they fit together and contribute to the overall functioning of the organization.

By decomposing an organization in this way, it is possible to gain a deeper understanding of how it operates and identify potential vulnerabilities or areas for improvement. However, it is important to recognize that an organization is a complex, interconnected system, and any changes or improvements made to one part of the organization may have ripple effects throughout the rest of the organization. Therefore, it is important to approach the analysis and decomposition of an organization with a holistic, systems-level perspective in order to truly understand its functioning and identify opportunities for improvement.

When decomposing an organization, it may be helpful to use various tools and techniques to analyze its various components and dimensions. This may include using data analysis techniques to examine financial or operational performance, conducting interviews or surveys with employees or stakeholders, or using process mapping or flowcharting techniques to understand how work is carried out within the organization.

It is also important to consider the context in which the organization operates when conducting this type of analysis. This may include factors such as the competitive landscape, regulatory environment, and economic conditions. By understanding the external factors that may influence the organization, it is possible to identify potential risks or opportunities and develop strategies to address them.

Overall, the process of decomposing an organization is a complex and multifaceted task that requires a thorough understanding of the organization and its environment. By breaking down the organization into its various components and dimensions and examining them in detail, it is possible to gain a deeper understanding of how the organization operates and identify potential vulnerabilities or areas for improvement. However, it is important to approach this process with a holistic, systems-level perspective in order to truly understand the organization and its functioning.

Cybersecurity is an enterprise risk, cybersecurity without proper Risk management is disorientation.

Effective cybersecurity requires a comprehensive risk management approach, in which potential threats are identified and evaluated, and appropriate measures are put in place to mitigate or eliminate those risks.

Without proper risk management, an organization's cybersecurity efforts can become disoriented, as it may struggle to effectively identify and prioritize the most significant threats it faces. This can leave the organization vulnerable to attacks and potentially costly breaches.

It is important for organizations to regularly measure their cybersecurity risks and to implement appropriate controls to manage those risks. This may involve working with a cybersecurity specialist or consulting firm to help identify, evaluate and measure risks and to develop a risk management plan.

Here are a few additional points to consider when it comes to the importance of risk management in cybersecurity:

- Risk management is a proactive approach to identifying and mitigating potential threats, rather than simply reacting to problems as they arise. This allows an organization to be more proactive and to take a more strategic approach to cybersecurity.

- By identifying and prioritizing the most significant risks, an organization can allocate its resources more effectively and focus on the areas that are most critical to its operations and objectives.

- Risk management involves not only identifying and mitigating risks, but also monitoring and reviewing the effectiveness of the measures in place. This helps to ensure that an organization's cybersecurity efforts remain relevant and effective over time.

- An effective risk management plan should be integrated into all aspects of an organization's operations and should be regularly reviewed and updated to ensure that it remains effective.

- Finally, it is important to have clear policies and procedures in place to guide the organization's risk management efforts and to ensure that all employees understand their role in helping to protect the organization.

Risk is uncertainty, the major cause of uncertainty is ignorance

Risk is the potential for harm or loss resulting from a given action or inaction. In financial terms, risk is often associated with the possibility of losing money. However, risk can also refer to the possibility of other negative outcomes, such as accidents, injuries, or damage to property.

Uncertainty refers to the state of being unsure or unknowing about something. There are many different sources of uncertainty, including lack of information, unpredictability, and lack of control.

Ignorance is a lack of knowledge or understanding about something. It can be a source of uncertainty because when we are ignorant about something, we are unable to predict or control what may happen. Ignorance can also lead to risk taking behaviors, as people may not be aware of the potential consequences of their actions.

In the context of risk, ignorance can be a major source of uncertainty because it can prevent us from being able to accurately measure and mitigate risk. For example, if we are ignorant about the potential risks associated with a particular activity, we may not take the necessary precautions to avoid those risks. This can lead to unexpected outcomes, such as accidents or financial losses.

Ignorance can also lead to risk-seeking behavior, as people may not be aware of the potential consequences of their actions.

To mitigate the effects of ignorance and reduce uncertainty, it is important to seek out and acquire knowledge about the risks associated with a particular activity or decision. This may involve researching and gathering information, consulting with experts, or seeking advice from others. By increasing our knowledge and understanding of the risks involved, we can make more informed decisions and take appropriate precautions to mitigate potential harm or loss.

Cybersecurity Policies as Hierarchy

Cybersecurity Risk is hierarchy of sub-risks, cybersecurity policy need to be developed as hierarchy

The idea behind a risk hierarchy is that it allows organizations to prioritize their efforts and resources based on the most significant threats they face.

At the highest level, organizations must identify and understand their overall cybersecurity risk posture. This includes assessing the risks to the organization as a whole, as well as the specific risks to individual assets, systems, data and services. Once the overall risk posture has been established, organizations can then begin to identify and prioritize specific sub-risks.

One way to approach this is to organize sub-risks into different categories, such as external threats, internal threats, and operational risks. External threats, for example, might include attacks from cybercriminals or nation-state actors, while internal threats might include malicious insiders or accidental data breaches. Operational risks might include issues such as inadequate security controls or a lack of incident response capabilities.

After the sub-risks have been identified and categorized, organizations can then prioritize them based on their potential impact and likelihood. This will allow them to focus their efforts on the most critical risks first, while still addressing lower-priority risks as resources permit.

By developing cybersecurity policies as a hierarchy of sub-risks, organizations can ensure that they are addressing the most significant threats they face while still being able to respond quickly and effectively to new or emerging threats. This approach will allow organizations to stay ahead of the constantly evolving threat landscape and protect their assets, systems, data and services from cyber attacks.

Livable

- Operational Cybersecurity Excellence
- Systematic Continues Analysis
- Continues Monitoring and live business dashboard

Livable

Operational Cybersecurity Excellence

Running cybersecurity operation is like all other types of operation, organizations should strive for efficiency and effectiveness throughout the organization processes.

Operational Cybersecurity Excellence requires, leadership continuous commitment, ensuring clear goals and targets and the institutionalization of cybersecurity defender spirit across the entire organization, which can be achieved through continuous and frequent awareness and training programs, identifying the gaps and issues and fixing them proactively.

Systematic Continues Analysis

Cybersecurity is not a project, there is no end point, it is always a race with bad and neglecting people, defenders will not achieve the first place.

Cybersecurity is an ongoing process, not a one-time project. There is no final destination or end point to reach, as the threat landscape is constantly evolving. As a result, it is a constant race to stay ahead of those who wish to cause harm or exploit vulnerabilities. Unfortunately, the "bad guys" are often more agile and able to adapt quickly, while government as well as most of the private entities and defenders may struggle to keep pace.

This is why it is so important for government as well as private entities to prioritize cybersecurity and allocate sufficient resources towards it. It is not a matter of if a cyber attack will occur, but when and what are the consequences . By being proactive and constantly working to strengthen their defenses, government as well as private entities can better protect themselves and their citizens and customers from the consequences of a cyber attack.

It is also important to recognize that achieving "first place" in this race may not be realistic. The nature of cybersecurity means that there will always be some level of risk present. However, by staying vigilant and continuously improving their defenses, government and private entities can minimize this risk and better protect themselves and their constituents and customers.

Continues Monitoring and live business dashboard

Cybersecurity risks are live and living, as attack surface are continuously extended, and the threat capabilities are increasing. The more digital services are introduced the more uncertainty will increase.

Continues Monitoring of Risks is critical principle, and every organization should develop business driven cybersecurity dashboard which maps the organizational Key Performance Indicators (KPIs) to the Organizational Key Risk Indicators (KRIs).

The Business Driven Cybersecurity Dashboard should be simple and straightforward helping business leaders to continuously monitor the organizational cybersecurity risks allowing them to enforce and enable responsible as well as accountable stakeholders to respond effectively and efficiently on timely based manner.

Economical

- Economical Effective Controls
- Cyber Risk Quantification

Economical

Economical Effective Controls

Controls are everywhere, no one can implement all controls, selecting the controls is art.

Controls are measures or procedures that organizations put in place to manage risks and ensure the security and integrity of their assets. They come in many forms, including administrative, physical, and technical controls. Examples of controls include firewalls, intrusion detection systems, security awareness training, background checks, and access controls.

Controls are everywhere, in the sense that they are present in every aspect of an organization's operations. They are used to protect assets such as services and data, systems, and infrastructure, as well as to ensure compliance with regulations and industry standards. However, it is not possible for an organization to implement all controls, as the number and variety of controls available are vast, and the cost and resources required to implement them all would be prohibitive.

Selecting the appropriate controls to implement is an art, as it requires a balance of technical expertise, business acumen, and risk management knowledge. The selection process starts with identifying the assets that need protection and the risks that they face. This information is then used to determine the controls that are most effective at mitigating those risks.

When selecting controls, organizations should consider factors such as the cost of implementation, the potential impact on business operations, and the likelihood of the risk occurring. It is also important to evaluate the level of protection provided by each control and consider the overall security posture of the organization, furthermore, it's important to remember that the controls needs to be aligned with the organization's risk appetite and overall goals. Although some organizations may place a high priority on compliance for their specific international relationships.

Cyber Risk Quantification

Most qualitative risk assessments do not rely on precise and consistent definitions of risk, instead measuring it in terms of high-medium-low, red-yellow-green, or ordinal scales such as 1-5.

Risk management and decision making based on qualitative risk assessments are fundamentally incorrect and erroneous because they are vulnerable to subjectivity, depending on an individual's conscious experience, among other concerns. Range compression is another issue which might impact the effectiveness of the qualitative risk approach as using discrete numbers can result in two scenarios scoring the same but indicating vastly different levels of risks.

Qualitative risk management may also introduce Inability to represent uncertainty, the use of discrete numbers results in a failure to express the possible range of outcomes, which should be central to risk analysis.

The consequence of using qualitative risk assessments is that the wrong prioritization decisions might be made as they are based on inaccurate risk estimates and that investment decisions continue to be made on a highly subjective basis, with little quantifiable data and economical rationale.

Although Qualitative Risk Management approach might be helpful at certain stages but every organization should adopt the Quantitative Risk Management approach.

Quantitative risk measurements help organizations prioritize risks and risk mitigation investments by quantifying the impact a risk presents to an organization's operations, assets, and mission. Data and estimates are used to inform risk factors such as event frequency (likelihood) and event magnitude (impact), to obtain a range of probable loss exposure.

Articulating cybersecurity risk in financial and quantitative terms helps better meet the requirements of assessing the adequacy of cybersecurity investments in the face of the specific risks an organization faces and bridges the communication gap between the cybersecurity team and the Business Leaders.

- **Organizational Capabilities**
- **Sustainable National Skills and Qualifications**
- **National Cybersecurity Products and Technologies**

Capability Based

Organizational Capabilities

Building Organizational Capabilities is sustainable, controls are compliance.

Building organizational capabilities is a sustainable approach to managing risks and achieving long-term success. It involves investing in the skills, knowledge, and resources of an organization in order to improve performance and achieve its goals. This can include training and development for employees, implementing effective systems and processes, and investing in technology and other resources.

While controls are an important part of managing risk and ensuring compliance with laws and regulations, they are only one aspect of building organizational capabilities. Effective controls help to prevent and mitigate risks, but they are reactive in nature and do not necessarily address the root causes of those risks.

In contrast, building organizational capabilities involves proactively addressing the underlying issues that contribute to risk and weakness. This can include improving processes, investing in technology and training, and developing a culture of continuous improvement. By taking a sustainable approach to building organizational capabilities, an organization can better manage risks and achieve long-term success.

Investing in organizational capabilities can help to create a strong foundation for long-term success. This includes developing the skills and knowledge of employees, implementing effective systems and processes, and investing in technology and other resources. By building these capabilities, an organization can improve performance, increase efficiency, and better adapt to changing circumstances.

In addition to improving operational effectiveness, building organizational capabilities can also help to manage risk and ensure compliance with laws and regulations. For example, by investing in employee training and development, an organization can reduce the risk of errors and accidents. Similarly, implementing effective systems and processes can help to prevent errors and ensure compliance with regulations.

However, it is important to recognize that controls, while important, are only one aspect of managing risk and ensuring compliance. Relying solely on controls can create a compliance-oriented culture that is reactive rather than proactive in managing risk. By focusing on building organizational capabilities, an organization can take a more proactive approach to managing risk and achieving long-term success.

Cybersecurity requires wide range of skills, qualifications and professionals, it is a global concern, it is a puzzle all pieces need to be fulfilled to close the gap.

One of the most important things to understand about cybersecurity is that it is not a one-size-fits-all solution. A wide range of different skills and qualifications are needed to effectively address the various threats and vulnerabilities that exist in the digital landscape. For example, professionals with technical expertise in areas such as network security, encryption, and artificial intelligence are needed to protect against cyberattacks, while those with backgrounds in strategy management, business analysis, business modeling, data analysis, law,

policy, and communications are needed to develop and implement effective cybersecurity policies.

Furthermore, Cybersecurity is not only a technical concern, but also a legal, ethical, and policy one. Cybersecurity experts should be familiar with legal and regulatory framework, to ensure that their solutions are compliant with laws and regulations. Moreover, cybersecurity professionals should have ethical considerations in their approach, not only to protect their own organization and clients but also the overall well-being of the society.

Another important aspect of cybersecurity is that it is a global concern. Cyberattacks can originate from anywhere in the world and can target individuals, organizations, or entire nations. To truly be effective, cybersecurity efforts must be coordinated at the national, regional, and international levels. This requires cooperation and collaboration between governments, private sector, and academic institutions from around the world.

Moreover, in the age of digitization, cybersecurity is not only limited to IT professionals but also it is a cross-functional concern, it is a responsibility for every employee, regardless of their role. Employees should be trained on cyber hygiene and security best practices, as well as to be familiar with the organization's security policies and procedures.

In conclusion, Cybersecurity is a puzzle, all pieces need to be fulfilled to close the gap. Achieving robust cybersecurity requires a wide range of skills, qualifications, and professionals. Business leaders, Cybersecurity experts, legal, ethical and policy expertise should be working together in a coordinated effort at the national, regional, and international levels. In addition, cybersecurity should not be the responsibility of IT professionals only, but also cross-functionally, every employee should be aware of cyber hygiene and security best practices, which will help to create a culture of safety and security in the digital age.

Sustainable National Skills and Qualifications

Sustainable cybersecurity starts very early, schools and academia is critical for sustainability

Sustainable cybersecurity is a crucial aspect of protecting our digital lives and ensuring the continued growth and development of technology. The most important aspect of sustainable cybersecurity is that it must be a continuous process, one that begins very early and is constantly evolving to keep pace with new threats and challenges.

One of the key players in this process is education, specifically schools and academia. These institutions are critical for the development of sustainable cybersecurity because they are where the next generation of cybersecurity professionals are trained and educated.

Cybersecurity is a constantly evolving field, and it is essential that schools and universities stay up to date with the latest trends and technologies. This includes not just teaching traditional cybersecurity concepts, such as encryption and network security, but also more recent developments such as artificial intelligence and machine learning and on top of that the critical skills of business analysis, business modeling and threat modeling.

In addition to providing formal education, schools and universities also have an important role to play in raising awareness about cybersecurity among the general population. This includes educating students, staff, and faculty about the risks and threats they may encounter online and how to protect themselves. This can be done through workshops, seminars, and other educational resources.

Moreover, In order to build a sustainable cybersecurity ecosystem, there is a need to encourage collaboration and information sharing between academic institutions, the private sector, and government organizations. This allows for the sharing of knowledge and resources, and enables the development of new solutions to emerging cybersecurity challenges.

One example of such collaboration is the National Cyber League competitions, where high school and college students compete against each other in simulated real-world cybersecurity challenges. This not only educate the students but also improve the talent pool for the future, as these competitions help to identify talented students and connect them with potential employers.

Furthermore, In order for sustainable cybersecurity to truly take root, it is important that it be integrated into all aspects of life, not just in the workplace. This means that schools and universities must work to ensure that their students are equipped with the knowledge and skills they need to stay safe online and to be responsible digital citizens.

National Cybersecurity Products and Technologies

Technology is one of the fundamental components of automation and digital transformation, investment on building national technologies for transformation and neglecting the investment of building national security technologies is third-party risk

Technology is a driving force behind automation and digital transformation. It enables businesses to streamline their processes, increase efficiency, and improve productivity. However, with the increasing reliance on technology comes the need to invest in the development of national technologies. This is important because relying on third-party technologies can create security risks.

When a company or government entities relies on third-party technologies, it is essentially outsourcing a critical component of its operations to an external entity. This means that the entity is vulnerable to the actions of that third party. If the third party experiences any issues, such as a data breach or disruption of service, it can have serious consequences for the entity that is relying on their technology.

On the other hand, investing in the development of national technologies allows the entity to have more control over the technology it uses. It reduces the reliance on external entities and the associated risks. It also has the potential to stimulate economic growth by creating jobs and fostering innovation within the country.

In addition to the risks associated with relying on third-party technologies, investing in the development of national technologies can also bring other benefits. For example, it can help a country to become more self-sufficient and less reliant on external sources for technology. This can be especially important in times of crisis, when access to external technology may be disrupted or restricted.

Investing in national technologies can also lead to the development of a strong domestic technology industry. This can create new job opportunities and stimulate economic growth within the country. It can also make it easier for companies and government entities within the country to access the technology they need, as they will not have to rely on external sources.

Furthermore, investing in national technologies can help to foster innovation and technological advancement within the country. This can lead to the development of new and improved products and services, which can help to drive economic growth and competitiveness.

Trustable

- Trust is Vulnerability
- Defensible Program
- Risk based audit

Trustable

Trust is Vulnerability

Trust is vulnerability, zero trust concept is not applicable for technology level only, it starts in trusting the business process towards the business objectives

Trust is a vital component of any business or organizational relationship. It is the foundation upon which all other elements, such as communication and collaboration, are built. However, trust is not always easy to come by, and it is often viewed as a vulnerability. This is particularly true in today's increasingly digital landscape, where cyber threats are a constant concern and data breaches are all too common.

The concept of zero trust is one that has gained traction in recent years as a way to mitigate these risks and protect against threats. But what exactly is zero trust, and how does it relate to trust and vulnerability?

At its core, zero trust is a security model that assumes that every interconnected goals, process, user, location, event, trigger, device, and application is untrusted until proven otherwise. This means that instead of trusting anything within an organization, a comprehensive process and analysis need to be practiced to continuously examine the interconnected business artifacts.

While zero trust is often associated with technology, it is important to understand that it is not just a technical solution. It starts with trust in the business process and its alignment towards the business objectives. It is about building a culture of security, where everyone understands that they have a role to play applying the zero trust concept in their daily jop protecting the organization's assets as security is not just the responsibility of the IT department.

For example, A business process that requires sensitive data to be shared with third parties should have a clear process in place for verifying the identity of those third parties, ensuring that the data is transmitted securely, and that there are controls in place to detect any breaches or unauthorized access.

To be effective, zero trust must be a holistic approach that involves all areas of the organization, not just IT. It must also be flexible enough to adapt to new risks and threats as they arise. This means that organizations must be willing to invest in the necessary processes, technologies, training, and resources to implement and maintain a zero trust model.

Defensible Program

Most of the Cybersecurity programs fail due to many factors like invisible systemic risk management, lack of transparency, broken accountability, throwing money on problem and many others.

Leveraging cybersecurity control frameworks — or multiple if required — aids organizations to develop a more mature approach to security. Cybersecurity frameworks serve to underpin security and risk management leaders to build a defensible security program by:

- Instilling confidence in internal and external stakeholders that the organization is aligning with industry best practices.

- Making it more measurable in terms of being able to assess maturity levels over time to a consistent set of control objectives.
- Increasing the likelihood that the security program is rightsized for the organization.

Building a defensible program requires deep understanding of the characteristics of what “good” looks like and build a continuous security program that is defensible and ensures a balance between protection and the need to run the business. Implementing a program to only meet a compliance requirement or “tick the boxes” is not an effective approach. Creating all the requisite documentation and implementing technology is not enough.

Defensible program should provide confidence to business leaders that controls are consistent and work the same way over time, adequate and provide satisfaction in line with business needs, reasonable and appropriate, effective to produce the desired or intended results.

Risk based audit

A "risk-based audit" is an approach to auditing where the auditor focuses on the areas of the organization that present the greatest risk on Business Objectives.

The main advantage of a risk-based audit is that it allows the auditor to more effectively use their time and resources by focusing on the areas of the organization that are most likely to be affected by errors or threats. By focusing on these areas, the auditor is better able to identify and report on significant risks that could impact the business objectives.

It is important to note that a risk-based audit is not limited to financial audits, it can be applied in any domain or field where the potential loss or damage is a concern. For example, in Information security, a risk-based audit approach can be applied to identify vulnerabilities and potential threats to the organization, prioritizing the most critical areas that need to be addressed.

A risk-based audit approach can also help organizations identify and manage emerging risks. As part of their assessment, auditors can evaluate the organization's ability to identify and respond to new or emerging risks, such as those arising from new technologies or changing business models. By identifying these risks early on, organizations can take steps to mitigate or manage them before they become a significant problem.

Risk-based auditing also requires auditors to have a deep understanding of the organization and its operations. Auditors must be familiar with the organization's business processes, internal controls, and systems in order to effectively identify and assess risks. This requires a collaborative approach between the auditor and the organization, with regular communication and information sharing.

Another key aspect of risk-based auditing is testing and validation. Once the areas of highest risk have been identified, auditors will need to test and validate the controls and processes in place to ensure that they are working effectively. This can include reviewing documents, testing systems and applications, and observing and interviewing employees.

The end goal of a risk-based audit is to provide value to the organization by identifying and reporting on risks that could have a significant impact on its operations financial aspects and business objectives. It should not be only to meet regulatory compliance, but also to enhance the organization's overall risk management and governance.

It's also worth mentioning that with the increasing trend of digitalization, risk-based auditing is also moving towards using data analytics and technology to make the audit process more efficient and effective. Auditors use various tools and techniques to extract and analyze large amount of data, which helps them to identify risks and patterns that could be missed with traditional audit methods.

Highlights of Jordan National Cyber Security Principles each organization need to understad and practice:

1. Organization understands and practice Cybersecurity as strategic business objective.

2. Organization is committed, capable and enabled to play its critical role as First Level of Defense

3. Organization understands and practice Cyber Security Accountability.

4. Organization understands that Cyber Security is Not a Technology Issue.

5. Organization practices decomposition and classification of the Goals, Business Processes, Roles and Responsibilities, Things and Materials, location and Geography, Events and Triggers, to the level ensures ignorance reduction, uncertainty reduction and reducing cyber security risks.

6. Organization practices data, information and services decomposition and classification to the level ensures ignorance reduction, uncertainty reduction and reducing cyber security risks.

7. Organization understands and practice discovering the Technology (IT, OT, ET, IOT, IIOT and any other emerging technologies) positioning in their Critical Service Operation.

8. Organization maintains a view of all systems and interfaces and provides guidelines and recommendations for stakeholders across the organization.

9. Organization deeply practices Cybersecurity Quantitative Risk Management for both Data and Services.

10. Organization evaluates the potential impact of risks (e.g., impact, likelihood, velocity) to business objectives.

11. Organization understands and practice Third Party Risk Management.

12. Organization tracks operational metrics to provide view of accepted operational objectives.

13. Organization tracks levels of risk exposure and ensures that risk exposures are within risk appetite.

14. Organization identifies, implements, and monitors the processes and controls necessary to support the organization's legal compliance initiatives.

15. Organization understands and facilitates fundamental audit principles and processes.

16. Organization identifies the roles, responsibilities and competencies needed For Effective cyber security practices.

17. Organization develops critical skills and competencies in the security staff.

18. Organization facilitates employee awareness and culture as it relates to secure behavior.

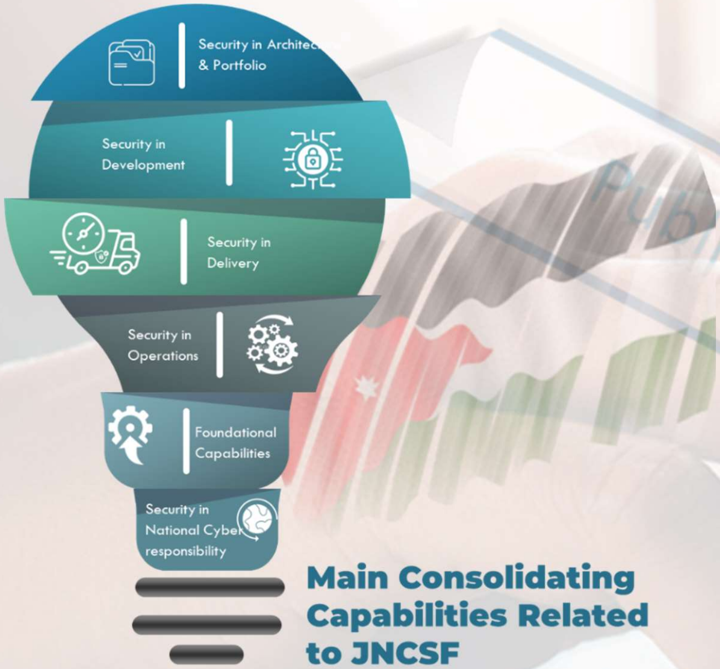
19. Organization enables and facilitates building national capabilities by supporting universities, schools and other academia students.

20. Organization promotes "where possible" the national cybersecurity solutions providers to help building national cyber security products.

Jordan National Cybersecurity Framework Capabilities

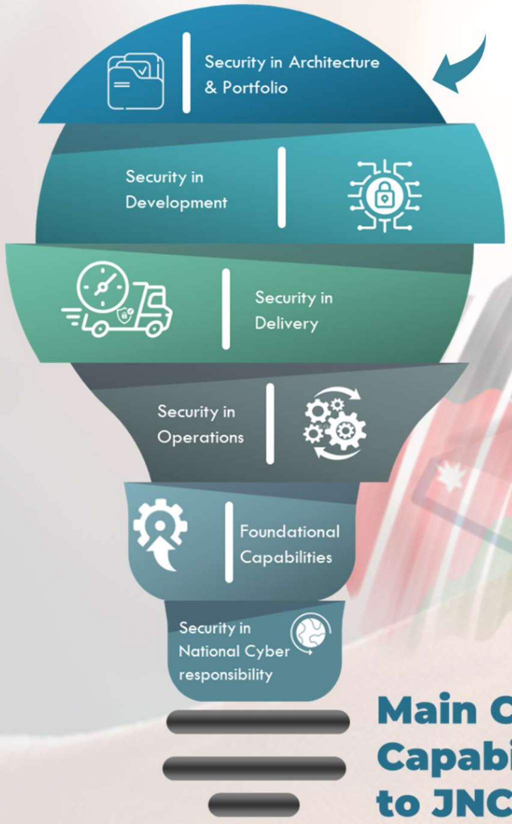
The Jordan National Cybersecurity Framework requires all organizations private and government to build and develop organizational capabilities that will insure the optimal utilization of the national as well as promoting digital transformation strategy and resources to elevate the cybersecurity maturity index, these capabilities, along with their related capabilities and sub capabilities have all put to integrate with the aim of ensuring cybersecurity.

These main capabilities are listed below:



Main Consolidating Capabilities Related to JNCSF

1. **Security in Architecture & Portfolio:** Security in Architecture is the first capability in Jordan's National Cyber framework, and it is considered one of the most important capabilities, given its precedence in application and importance in integration with the rest of the capabilities to maintain security and maximum protection for entities, as it is one of the most critical planning features of any project or producer's planning stage, enabling effective prioritization of proposed investments, initiatives, and projects.
2. **Security in Development:** The measures and techniques used during the services development process to ensure that the resulting system is secure and protected against potential threats and. This includes practices such as vulnerability assessments, security testing, and adherence to industry-standard security protocols and guidelines.
3. **Security in Delivery:** Security in Delivery refers to the measures taken to protect data and services during transformation and delivery. Such measures include secure encryption, tracking and monitoring systems, and personnel background checks. The goal of delivery security is to ensure that service/data are delivered to the intended recipient safely and securely, without being lost, stolen, or tampered with during transit.
4. **Security in Operations:** Security in operations refers to the practices and processes that aim to protect an entity's services and information systems, networks, and data from unauthorized access, use, disclosure, disruption, modification, or destruction. These operations encompass a wide range of activities such as incident response, threat intelligence, vulnerability management, and so on.
5. **Foundational Capabilities:** Fundamental capabilities in cybersecurity are the foundational skills and knowledge that entities and individuals must have in order to effectively protect their services, systems, networks, and data from unauthorized access, misuse, and malicious attacks. These capabilities are essential for ensuring the service resiliancy and confidentiality, integrity, and availability of information, which are the three main pillars of information security.
6. **Security in National Cyber Responsibility:** Cybersecurity is a collective responsibility, shared between countries, businesses, accademia and individuals. Countries worldwide are increasingly realizing cybersecurity's importance in protecting national security and its significant impact on economic growth.


Security in Architecture & Portfolio
Security in Development
Security in Delivery
Security in Operations
Foundational Capabilities
Security in National Cyber responsibility

Main Consolidating Capabilities Related to JNCSF

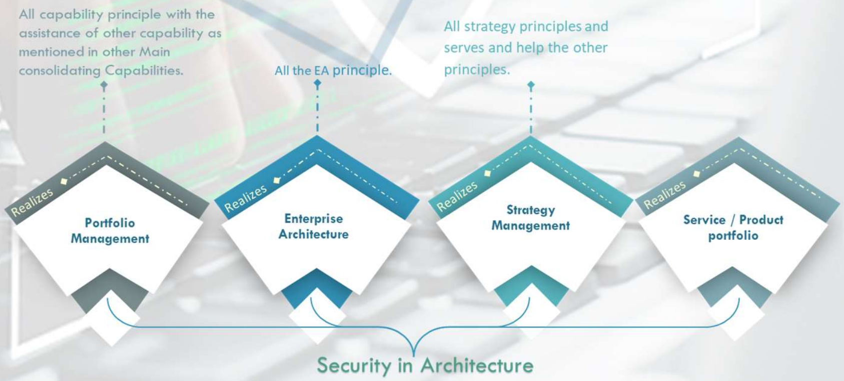
Security in Architecture

Security in Architecture is the first capability in Jordan's National Cyber framework, and it is considered one of the most important capabilities, given its precedence in application and importance in integration with the rest of the capabilities to maintain security and maximum protection for entities, as it is one of the most critical planning features of any project or producer's planning stage, enabling effective prioritization of proposed investments, initiatives, and projects.

It is intended to improve security by designing strategically and comprehensively. It is the Strategy to Portfolio functions that allow for the efficient design, creation, traceability, and management of secure-strategy-aligned products/services or enhancements. Starting from a strategic standpoint, develop a security and cybersecurity strategy that is aligned with the overall business strategy. Assuring the practice of articulating and modeling cybersecurity within enterprise architectures. As a result, optimize the required security among products/services by managing portfolio security and cyber security aspects.

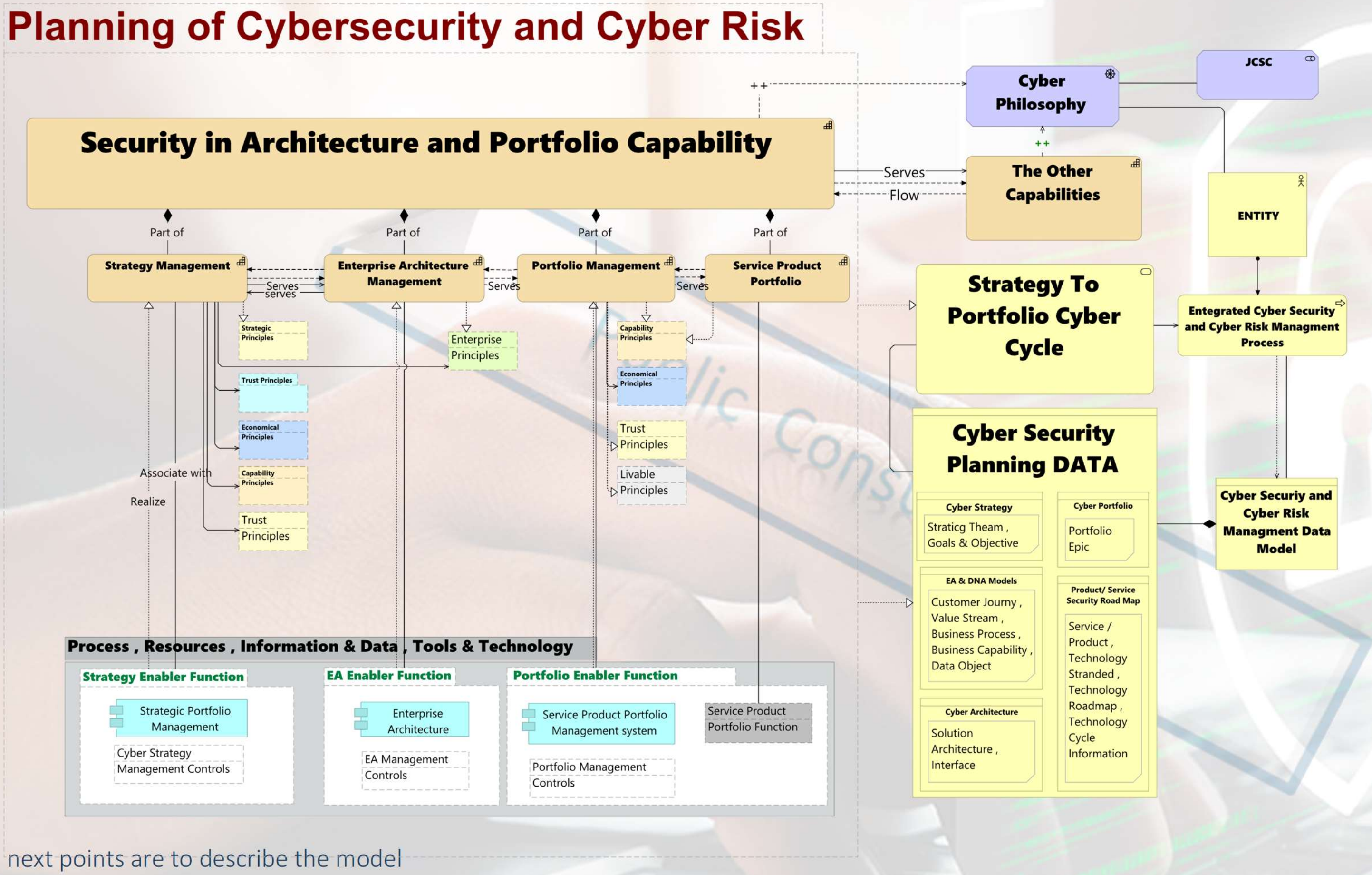
To have this consolidating capability, each entity must have the following underlying main capability developed, maintained, and activated at the appropriate maturity level:

- Strategy Management: This capability involves ensuring the strategic control and management of Cybersecurity and Cyber Risk across all Services and Information, from top management to everyone.
- Enterprise Architecture Management: This capability focuses on articulating and modeling the entire business from all angles to ensure proper, optimized-by-design, and effective security architectures.
- Portfolio Management: Portfolio management seeks to maximize returns while minimizing risk. As a result, the cyber risk would be considered at an early stage to ensure pro-action rather than reaction with cost optimization.
- Service Product Portfolio: This is a supplementary capability to the overall portfolio management capability, and it manages the level of detail for each product or service. To ensure that security by design is implemented in each service or product, as well as proper risk, technology, and resource classification, to achieve the required CIAS index.


All capability principle with the assistance of other capability as mentioned in other Main consolidating Capabilities.
All the EA principle.
All strategy principles and serves and help the other principles.
Realizes
Portfolio Management
Realizes
Enterprise Architecture
Realizes
Strategy Management
Realizes
Service / Product portfolio
Security in Architecture

Enterprise Architecture Module (EAM) Related to the Main Capability of Security in Architecture

The enterprise architecture module shown below summarizes the capabilities and sub-capabilities of this main capability


Planning of Cybersecurity and Cyber Risk
Security in Architecture and Portfolio Capability
Part of
Part of
Part of
Part of
Strategy Management
Serves
serves
Enterprise Architecture Management
Serves
Portfolio Management
Serves
Service Product Portfolio
Strategic Principles
Enterprise Principles
Capability Principles
Trust Principles
Economical Principles
Economical Principles
Trust Principles
Capability Principles
Livable Principles
Associate with
Realize
Trust Principles
Process , Resources , Information & Data , Tools & Technology
Strategy Enabler Function
Strategic Portfolio Management
Cyber Strategy Management Controls
EA Enabler Function
Enterprise Architecture
EA Management Controls
Portfolio Enabler Function
Service Product Portfolio Management system
Portfolio Management Controls
Service Product Portfolio Function
++
Cyber Philosophy
JCSC
++
Serves
Flow
The Other Capabilities
ENTITY
Strategy To Portfolio Cyber Cycle
Entegrated Cyber Security and Cyber Risk Managment Process
Cyber Security Planning DATA
Cyber Strategy
Straticg Theam , Goals & Objective
Cyber Portfolio
Portfolio Epic
EA & DNA Models
Customer Journy , Value Stream , Business Process , Business Capability , Data Object
Product/ Service Security Road Map
Service / Product , Technology Stranded , Technology Roadmap , Technology Cycle Information
Cyber Architecture
Solution Architecture , Interface
Cyber Securiy and Cyber Risk Managment Data Model

The next points are to describe the model

- The capabilities consist of the below main capabilities:
  - Strategy Management Capability
  - Enterprise Architecture Management Capability
  - Portfolio Management Capability
  - Product / Services Portfolio Capability

- The capability services as the planning phase or cycle regarding achieving an integrated cyber security and cyber risk management process, Where each entity is direct responsibility for ensuring the execution of the process.

- Each main capability realizes some main principles as below, where each realization may be associated with the other capability in a collaboration manner :
  - The Strategy Management Capability realizes all strategy principles and serves and helps the other principles.
  - The Enterprise Architecture capability realizes all the enterprise driven principle.
  - Portfolio management. And product/service portfolio realizes the all-capability principle with the assistance of other capabilities, as mentioned in other Main consolidating Capabilities.

- All the Sb-main capabilities are formed by utilizing, developing, and maintaining underlying functions that may consist of Tools, People, Technology, and information or data

- Each Main Sub Capability serves the other with the importance of the strategy and EA interrelation.

- The full capability is connected to the rest of the framework capabilities in terms of serving wise and flow of information.

- The Main Data output from the planning eco-cycle as part of the holistic cyber data models are :
  - Cybersecurity strategy
  - Cybersecurity Portfolio
  - EA & DNA models
  - Cybersecurity Architecture
  - Product/ Service Security Road Map

- The Capability is part for influencing the General Philosophy of Jordan National Cyber Security Center.

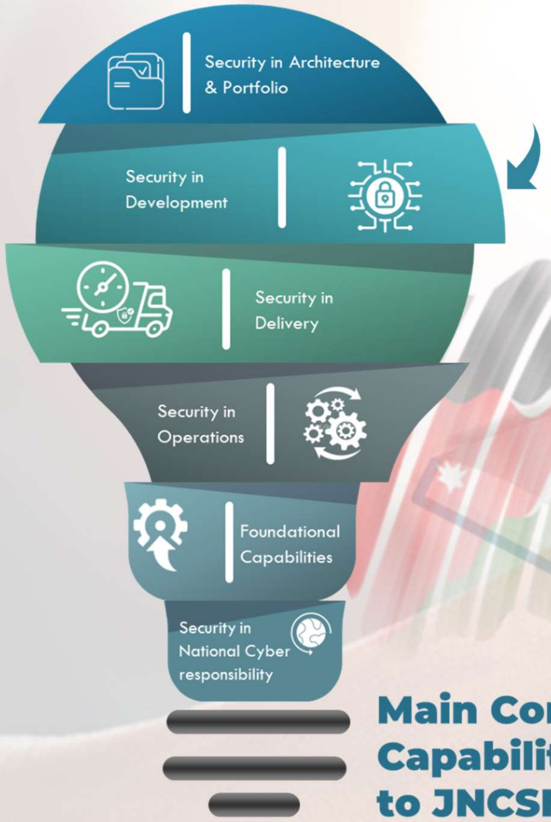
Benefits of the Capability of Security in Architecture

The strategy to portfolio functions describes a prescriptive framework of required functional components and information objects that entities can use to control better strategy alignment to the investment and product/services portfolio functional components.

The following are the primary advantages of utilizing the strategy to portfolio functions:

Business Benefits

- A holistic portfolio view encompassing the functional components of strategy, enterprise architecture, portfolio backlog, proposal, and product portfolio.
- Portfolio decisions made in accordance with business priorities.
- Tracking the lifecycle of a product across conceptual, logical, and physical domains.
- Rebalance investments in response to strategic and operational demand.
- Prioritized investment based on all portfolio aspects, such as cost/value analysis, architectural implications, product/service roadmap, business priorities, and feasibility.
- Effective communication with business stakeholders via scope agreements and roadmaps.


Security in Architecture & Portfolio
Security in Development
Security in Delivery
Security in Operations
Foundational Capabilities
Security in National Cyber responsibility

Main Consolidating Capabilities Related to JNCSF

Security in Development

The measure and technique used during the service development process to ensure that the resulting system is secure and protected against potential threats and vulnerabilities. This includes practices such as vulnerability assessments, security testing, and adherence to industry-standard security protocols and guidelines.

Furthermore, it entails involving security experts and stakeholders throughout the development process to ensure that security considerations are incorporated into each phase of service or software development. Security in development is critical for protecting sensitive information and maintaining system integrity.

To have this consolidating capability, the following nine capabilities -which are called Requirements to Deploy Functions- must be developed, maintained, and activated within the entity as an organization or an individual with the appropriate maturity level:

1. Requirements Management: the ability to gather, document, and manage the requirements of the software system, including gathering input from stakeholders and ensuring that the software system meets the needs of users.

2. Product & Team Backlog: The ability to maintain and prioritize a backlog of requirements, features, and user stories that need to be implemented, this helps to ensure that the software system is aligned with the needs of stakeholders.

3. Service/ product Design: The ability to design and plan the architecture, layout, and overall design of the software system, this includes creating detailed plans and specifications and ensuring that the software system is aligned with IT as well as cybersecurity governance best practices.

4. Secure Code Management: the ability to implement secure coding practices, such as input validation, error handling, and secure data storage, to help prevent common software vulnerabilities. This includes using secure coding standards, such as OWASP Top 10, and following best practices for software development.

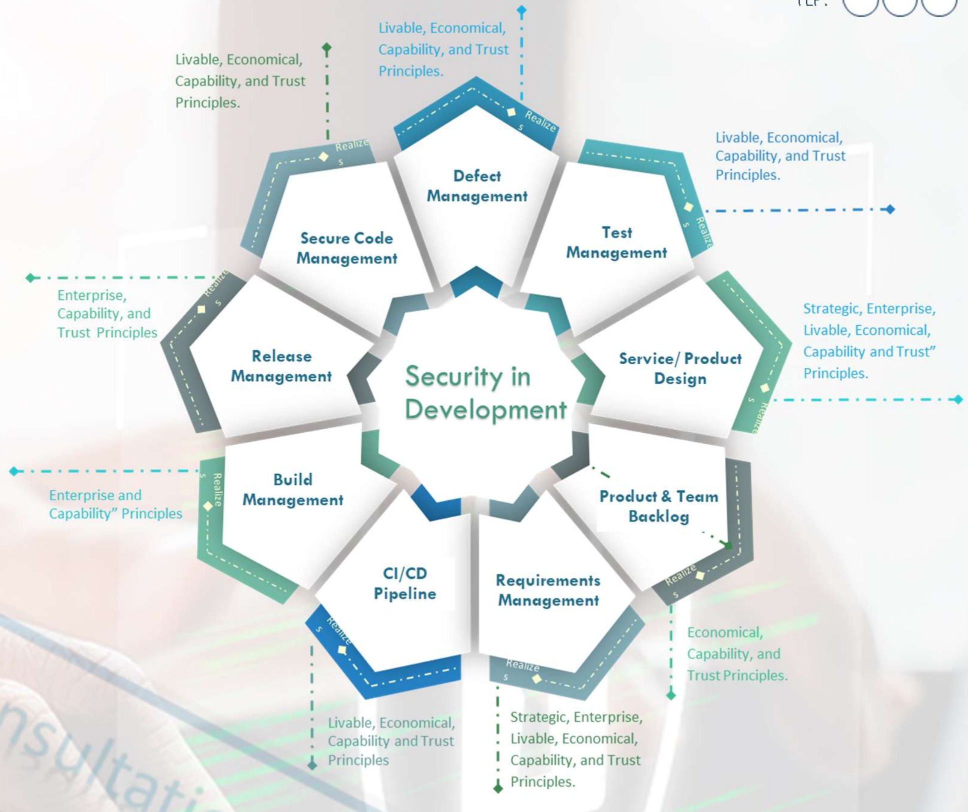
5. Test Management: the ability to use automated testing tools, such as unit tests, integration tests, and regression tests, to ensure that the software system is functioning correctly and is free of bugs or errors. This includes implementing automated testing and penetration testing as part of the CI/CD pipeline to ensure that the software system is secure and meets the requirements of stakeholders.

6. CI/CD Pipeline: the ability to implement a CI/CD pipeline to automate the software development process, including automated testing, building, and deployment. This includes integrating security testing into the CI/CD pipeline, to ensure that new code changes do not introduce any vulnerabilities or security issues.

7. Defect Management: security in development is the process of identifying, tracking, and resolving security-related defects in the software system. It includes capabilities such as security defect tracking, resolution, root cause analysis, reporting, and vulnerability management.

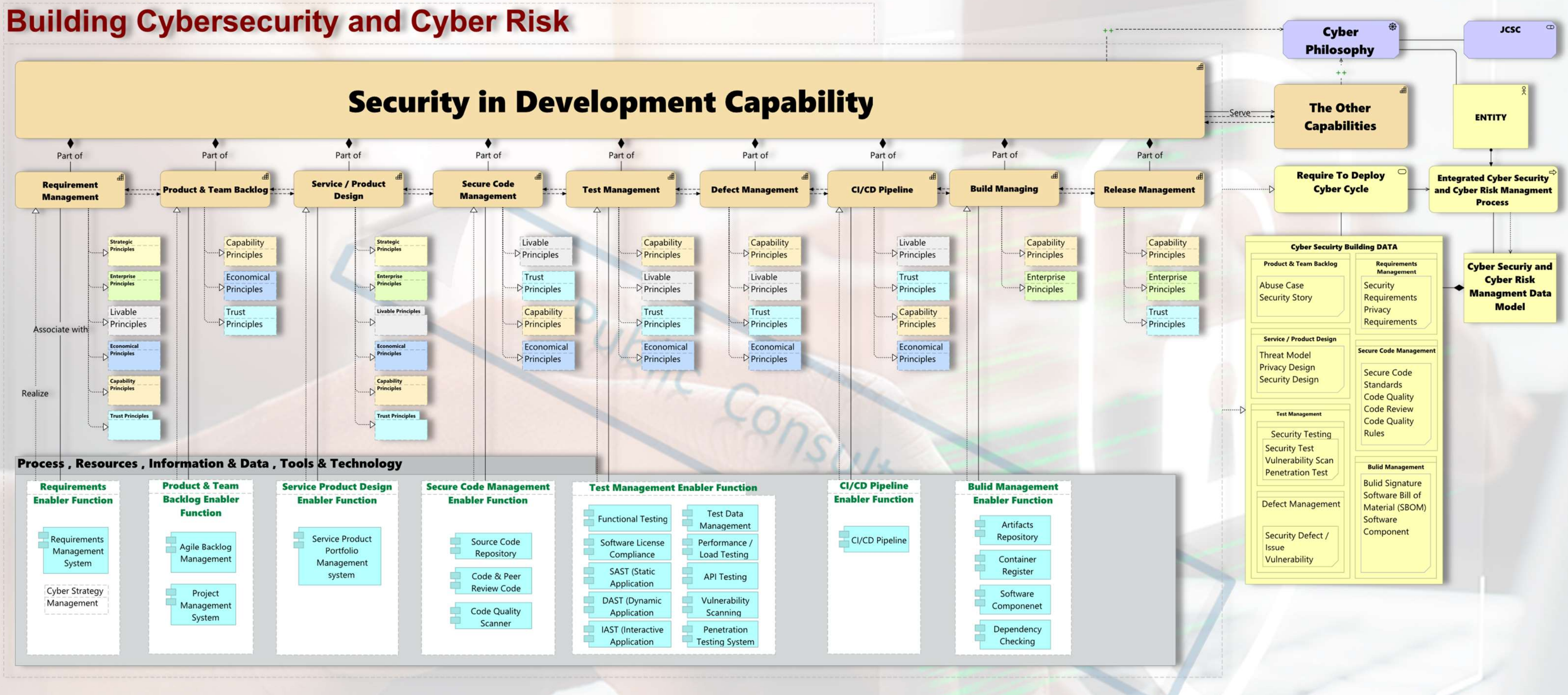
8. Build Management: the ability to manage the build process, including version control, testing, and packaging of software systems. This includes automating the build process, managing dependencies, and ensuring that the software system is ready for deployment.

9. Release Management: the ability to plan, organize, and manage the release of software systems, including testing, packaging, and deployment. This includes identifying the appropriate release schedule, determining the release criteria, and coordinating the release process with stakeholders.


Security in Development
Defect Management
Test Management
Service/ Product Design
Product & Team Backlog
Requirements Management
CI/CD Pipeline
Build Management
Release Management
Secure Code Management
Realizes
Livable, Economical, Capability, and Trust Principles.
Livable, Economical, Capability, and Trust Principles.
Livable, Economical, Capability, and Trust Principles.
Strategic, Enterprise, Livable, Economical, Capability and Trust" Principles.
Economical, Capability, and Trust Principles.
Strategic, Enterprise, Livable, Economical, Capability, and Trust Principles.
Livable, Economical, Capability and Trust Principles
Enterprise and Capability" Principles
Enterprise, Capability, and Trust Principles

Enterprise Architecture Module (EAM) Related to the Main Capability of Security in Development

The enterprise architecture module shown below summarizes the capabilities and sub-capabilities of the main capability of security in ddevelopment:



C

The next points are to describe the model

- This capability is made up of the nine previously mentioned capabilities, which are known as Requirements to Deploy Functions.
- The capability services serve as the foundation for achieving an integrated cyber security and cyber risk management process, with each entity directly responsible for ensuring the process's execution.
- Each main capability realizes some key principles, which are listed below, and each realization can be linked to the other capability in a collaborative manner:
  - The Requirements Management Capability realizes all "Strategic, Enterprise, Livable, Economical, Capability and Trust" Principles.
  - The Product & Team Backlog Capability realizes all "Economical, Capability, and Trust" Principles.
  - The Service/ Product Design Capability realizes all "Strategic, Enterprise, Livable, Economical, Capability and Trust" Principles.
  - The Secure Code Management Capability realizes all "Livable, Economical, Capability and Trust" Principles.
  - The Test Management Capability realizes all "Livable, Economical, Capability and Trust" Principles.
  - The CI/CD Pipeline Capability realizes all "Livable, Economical, Capability and Trust" Principles.
  - The Defect Management Capability realizes all "Livable, Economical, Capability and Trust" Principles.
  - The Build Management Capability realizes all "Enterprise and Capability" Principles.
  - The Release Management Capability realizes all "Enterprise, Capability and Trust" Principles.
- All the Sub main capabilities are formed by utilizing, developing, and maintaining underlying functions that may consist of Tools, People, Technology, and information or data.
- Each Main Sub Capability is serving the other.
- The whole capability is for sure connected to the rest of the framework capabilities in terms of serving wise and flow of information.
- The Main Data output from the building eco-cycle as part of the holistic cyber data models are:
  - Requirements Management
  - Service / Product Design
  - Test Management
  - Product & Team Backlog
  - Secure Code Management
  - Build Management
- The Capability is part of influencing the General Philosophy of the Jordan National Cyber Security Center.

Business Benefits of the Capability of Security in Development

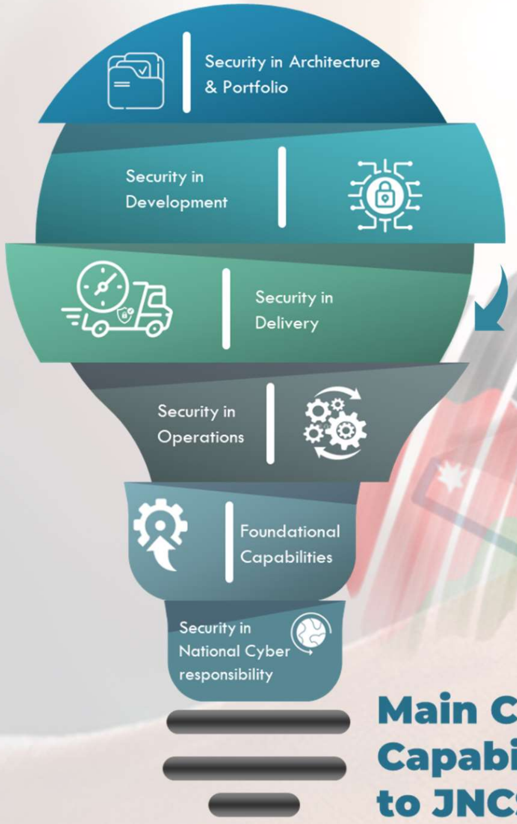
The requirement to deploy describes a prescriptive framework of required functional components, integrations, and data objects to enable entities to deliver better value more quickly and safely while lowering costs and increasing product team productivity.

The primary benefits of using the requirement to deploy functions are as follows:

Business Benefits

- Increasing the delivery speed of Product Backlog Items.
- Increased availability of new product releases.
- Increased testing coverage and traceability lead to higher change success rates and lower security risks.
- Traceability and transparency from requirement and/or backlog item to Product Release.
- Security and compliance reduce risk by design. Interoperability, communication, and collaboration among stakeholders and teams involved have all improved (including external vendors).
- Service component reuse has become the norm as product development and delivery have become so standardized..

- The delivery of product backlog items has been accelerated (e.g., new features or resolving defects or problems)
- Increasing the rate at which new products are introduced: Using the same automatable architecture across teams can improve release frequency predictability and manageability (and, by extension, standardized tools for the most automatable parts of the development and release chains). By ensuring that the Product Release includes all the content required for automated instantiation, the Requirement to Deploy functional and data models provide an architecture capable of reducing the time from committed code to live systems to zero. That will Increase the rate at which new products are introduced.
- More complete and traceable testing capability should result in higher change success rates and reduced security risks.
- End-to-end transparency and traceability from requirement and/or backlog item to Product Release.
- Reducing the risk due to security and compliance by design, and this is to the maintaining process of the association between entity policy and requirement data objects throughout the product lifecycle by the requirement to deploy functions. This persistent traceability enables designers to ensure that all non-functional requirements are accounted for so that products are designed per standards and policies from sources such as security management, governance, risk, & compliance, legal & regulatory, enterprise architecture, and financial management.
- Improved interoperability, communication, and collaboration among involved stakeholders and teams (including external vendors): Applications and services can be sourced or developed in collaboration with a variety of parties, each of which uses its own processes and tooling. The requirement to deploy functional criteria defines an interoperability standard that allows entities to enforce a consistent, standardized description of planned activities as well as function and data interoperability.


Security in Architecture & Portfolio
Security in Development
Security in Delivery
Security in Operations
Foundational Capabilities
Security in National Cyber responsibility

Main Consolidating Capabilities Related to JNCSF

Security in Delivery

One of the most important methodologies in the service production life cycle is the service delivery security methodology. Security in delivery is a critical component of this methodology.

Security in Delivery refers to the measures taken to protect data and services during transformation and delivery. Such measures include secure encryption, tracking and monitoring systems, and personnel background checks on delivery. The goal of security delivery is to ensure that services/data are delivered to the intended recipient safely and securely, without being lost, stolen, or tampered with during transit.

Security in delivery capability has several key elements, including:

SECURITY IN DELIVERY KEY ELEMENTS

ENCRYPTION

Encryption is the process of converting plain text into a coded format that only authorized parties with the appropriate decryption key can read. This helps to prevent unauthorized parties from intercepting and reading.

AUTHENTICATION

Authentication is the process of verifying the identity of the data sender and receiver. This helps to prevent unauthorized access to sensitive information and ensures that data can only be received and transmitted by authorized parties.

ACCESS CONTROL

Access control is the process of managing access to data and resources based on predefined security policies. This helps to prevent unauthorized access to sensitive information and ensures that only authorized parties can access and use data.

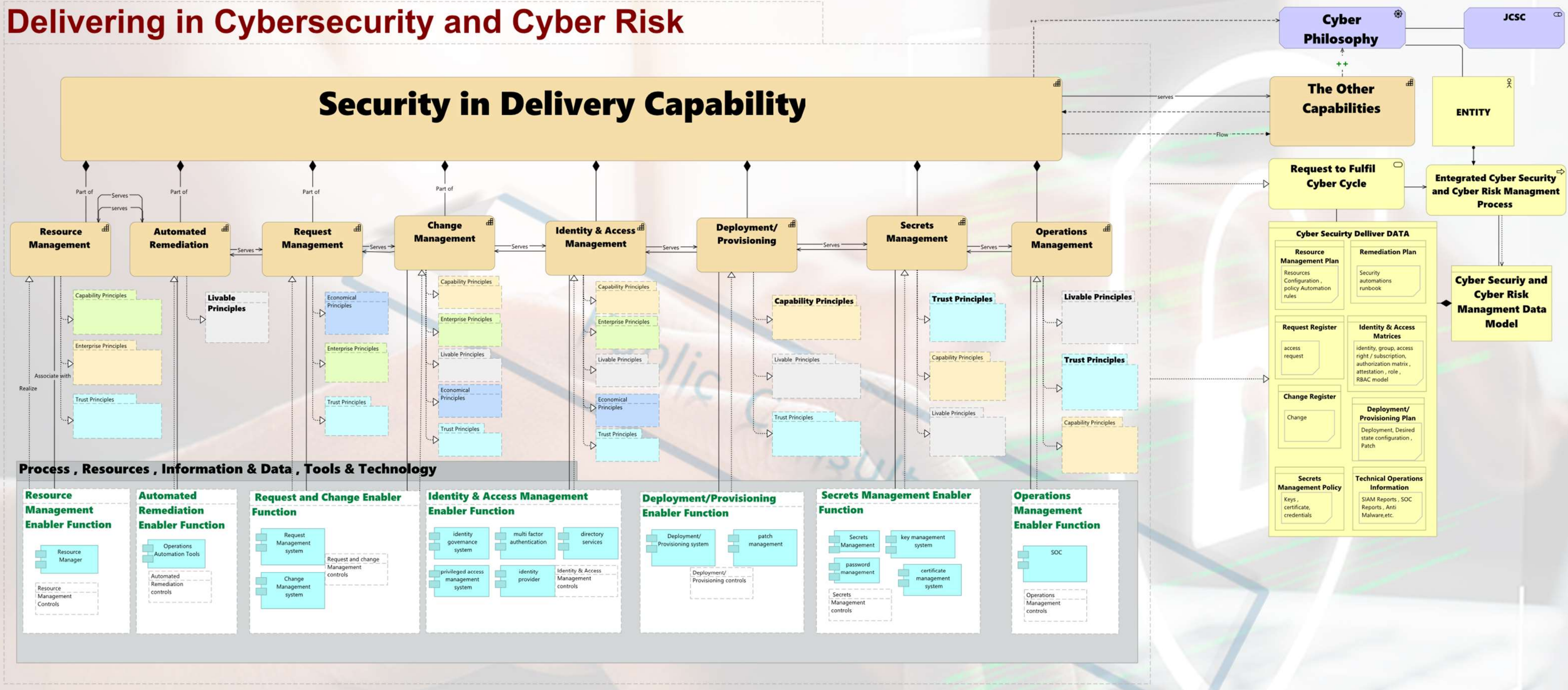
NETWORK SECURITY

Network security entails safeguarding networks and systems against attacks and unauthorized access. Examples include firewalls, intrusion detection and prevention systems, and other security technologies.

Overall, security in delivery is a critical aspect of cybersecurity that helps to protect data and information while it is being transmitted or delivered over a network. By implementing strong encryption, authentication, access control, and network security measures, organizations can help to ensure the confidentiality, integrity, and availability and safety of sensitive information or services.

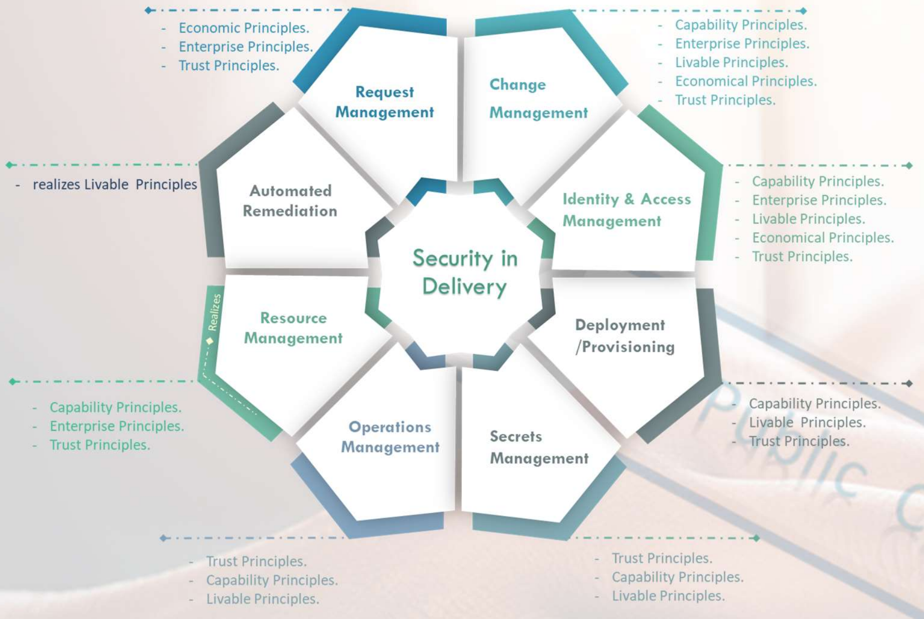
Enterprise Architecture Module (EAM) Related to the Main Capability of Security in Delivery

The enterprise architecture module shown below summarizes the capabilities and sub-capabilities of the main capability of security in delivery:


Delivering in Cybersecurity and Cyber Risk
Security in Delivery Capability
Cyber Philosophy
JCSC
The Other Capabilities
ENTITY
serves
Flow
Request to Fulfil Cyber Cycle
Entegrated Cyber Security and Cyber Risk Managment Process
Cyber Secuirty Delliver DATA
Resource Management Plan
Resources Configuration , policy Automation rules
Remediation Plan
Security automations runbook
Request Register
access request
Identity & Access Matrices
identity, group, access right / subscription, authorization matrix , attestation , role , RBAC model
Change Register
Change
Deployment/ Provisioning Plan
Deployment, Desired state configuration , Patch
Secrets Management Policy
Keys , certificate, credentials
Technical Operations Information
SIAM Reports , SOC Reports , Anti Malware,etc.
Cyber Securiy and Cyber Risk Managment Data Model
Part of
Serves
serves
Resource Management
Automated Remediation
Request Management
Change Management
Identity & Access Management
Deployment/ Provisioning
Secrets Management
Operations Management
Associate with
Realize
Capability Principles
Enterprise Principles
Trust Principles
Livable Principles
Economical Principles
Process , Resources , Information & Data , Tools & Technology
Resource Management Enabler Function
Resource Manager
Resource Management Controls
Automated Remediation Enabler Function
Operations Automation Tools
Automated Remediation controls
Request and Change Enabler Function
Request Management system
Change Management system
Request and change Management controls
Identity & Access Management Enabler Function
identity governance system
multi factor authentication
directory services
privileged access management system
identity provider
Identity & Access Management controls
Deployment/Provisioning Enabler Function
Deployment/ Provisioning system
patch management
Deployment/ Provisioning controls
Secrets Management Enabler Function
Secrets Management
key management system
password management
certificate management system
Secrets Management controls
Operations Management Enabler Function
SOC
Operations Management controls

The next points are to describe the model

- The capabilities are divided into main capabilities, with each realization being associated with the other capability in a collaborative manner; a summary of these main capabilities is provided below:



- Resource Management Capability realizes Capability Principles, Enterprise Principles, and Trust Principles.
- Automated Remediation realizes Liveable Principles
- Request Management realizes the Economic Principles, Enterprise Principles, and Trust Principles.
- Change Management realize: Capability Principles, Enterprise Principles, Livable Principles, Economical Principles, and Trust Principles.
- Identity & Access Management realizes Capability Principles, Enterprise Principles, Livable Principles, Economical Principles, and Trust Principles.
- Deployment/Provisioning realize Capability Principles, Livable Principles, and Trust Principles
- Secrets Management realizes Trust Principles, Capability Principles, and Livable Principles
- Operations Management realizes Trust Principles, Capability Principles, and Livable Principles.

- All the related capabilities are formed by utilizing, developing, and maintaining underlying functions that may consist of Tools, People, Technology, and information or data.
- Each Main Sub Capability serves the other with the importance of the strategy and enterprise architecture interrelation.
- The full capability is connected to the rest of the framework capabilities in terms of serving wise and flow of information.
- The Main Data output from the planning eco-cycle as part of the holistic cyber data models are :
  - Request Register
  - Change Register
  - Identity & Access Management
  - Deployment/Provisioning
  - Secrets Management Policy
  - Technical Operations Information
  - Resource Management Plan
  - Remediation Plan
- Capability influences the General Philosophy of the Jordan Cyber Security Center.

Benefits to the Capability of Security in Delivery

Benefits

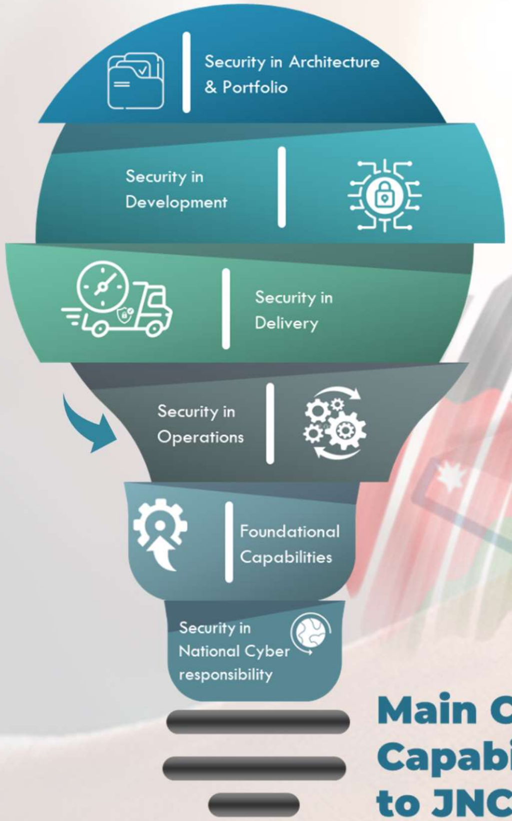
- Data Protection
- Comply With Various Regulations and Standards
- Reputation
- Cost effective

- **Data Protection -** Security in delivery ensures that the data being transmitted is protected from unauthorized access, alteration, or theft. This helps to prevent data breaches and the loss of sensitive information.

- **Compliance -** Security in delivery helps organizations to comply with various regulations and standards, such as HIPAA and PCI-DSS, which require secure data transmission.

- **Reputation Protection -** Organizations that implement security in delivery can protect their reputation by demonstrating to customers and partners that they take the security of their data seriously.

- **Cost effective -** Implementing security in delivery can ultimately save organizations money by reducing the risk of data breaches, which can be costly in terms of both financial and reputational damage.


Security in Architecture & Portfolio
Security in Development
Security in Delivery
Security in Operations
Foundational Capabilities
Security in National Cyber responsibility

Main Consolidating Capabilities Related to JNCSF

Security in Operations

Security in operations refers to the practices and processes that aim to protect an entity's services, information systems, networks, and data from unauthorized access, use, disclosure, disruption, modification, or destruction. These operations encompass a wide range of activities such as incident response, threat intelligence, vulnerability management, and so on.

The security in operations functions also provides a comprehensive overview of the digital operations business and the services provided by an Operations team, including security operations. This point of view provides an understanding of the interdependence of its many domains, as well as responsiveness to business requests and requirements.

One of the main objectives of security operations is to detect security incidents in operations and respond to them in a timely and effective manner, all while continuously improving the entities' overall security situation. Continuous monitoring and analysis of security data, as well as regular testing and updating of security controls, are required. Furthermore, security operations teams must have clear incident response plans and conduct regular exercises to ensure operations' incident response capabilities are effective.

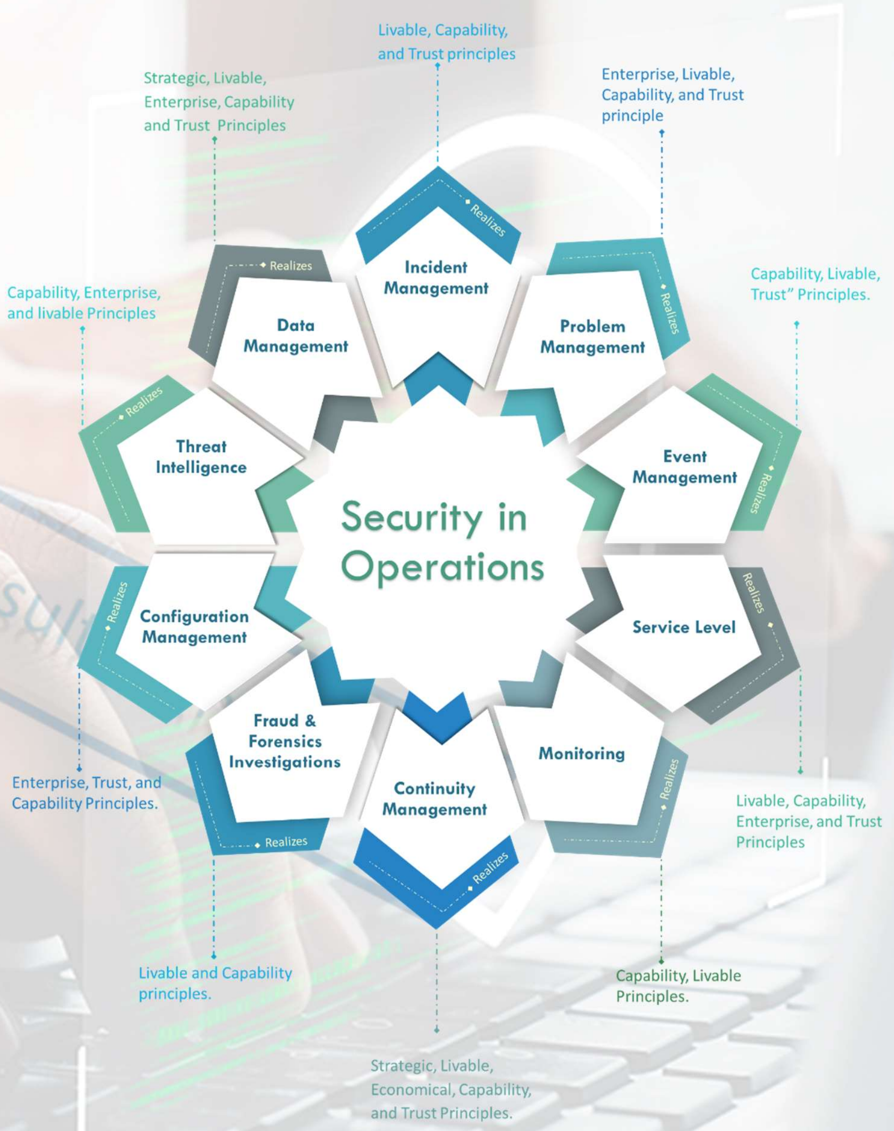
Security in operations functions brings together operations functions to improve services and efficiencies, thereby lowering risk.

Security operations are a collection of key capabilities designed to protect an entity, service, networks, and systems. Incident response, threat intelligence, and vulnerability scanning are examples of these activities.

These activities are listed below, along with a brief description of each.

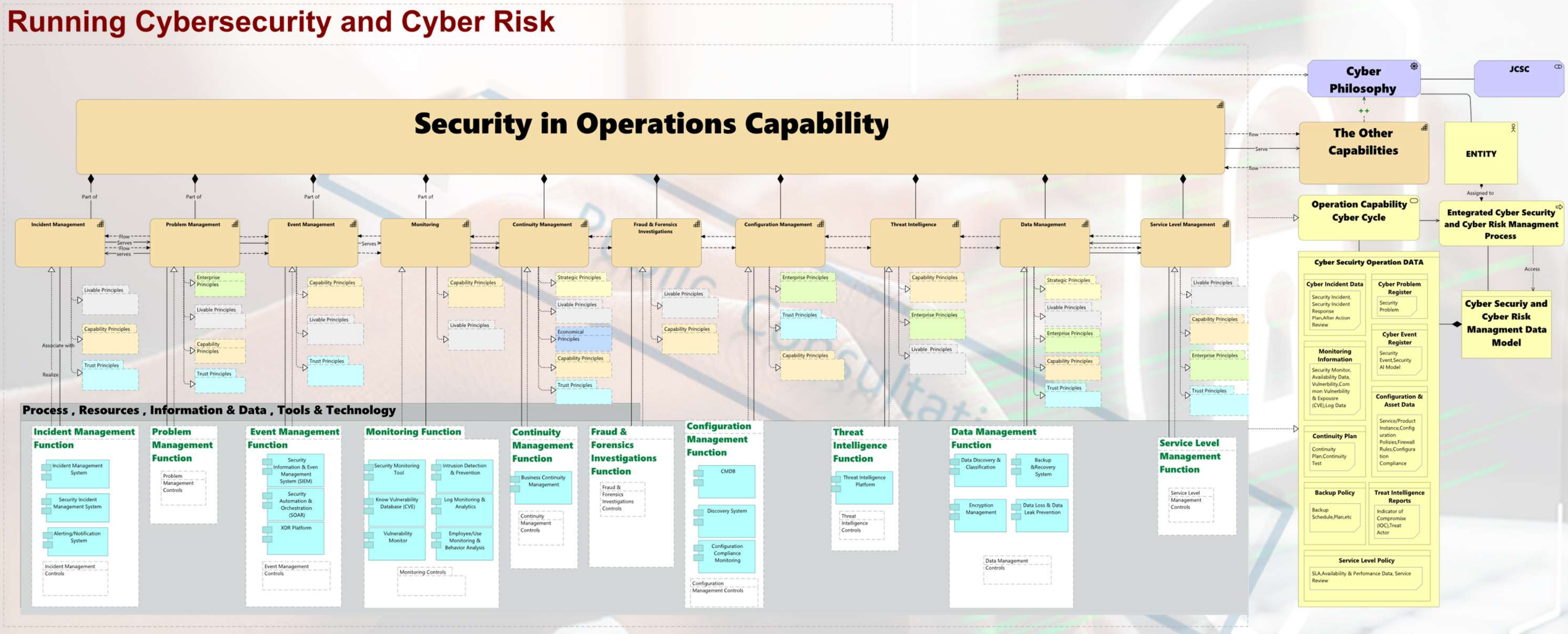
- Incident Response: This refers to the process of identifying, containing, and mitigating the effects of a security incident. Detecting, analyzing, and responding to security incidents is typically the responsibility of a team of security professionals. They may use a variety of tools and techniques to identify potential threats, such as intrusion detection systems, security information and event management (SIEM) systems, and network analysis tools.
- Threat Intelligence: it is the gathering and analysis of information about potential threats to an entities assets. This data can be used to discover new vulnerabilities, track the activities of known attackers, and devise mitigation strategies for potential attacks. entities can gather threat intelligence from various sources, including open-source information, industry groups, and government agencies.
- Monitoring: Monitoring for potential threats is also an important aspect of operational security. This can include monitoring network traffic, logging system events, and detecting and responding to potential threats using security tools such as intrusion detection and prevention systems.

- Vulnerability Scanning: This major key identifies, assesses, and mitigates vulnerabilities in an entities assets, networks, and systems. This includes scanning for vulnerabilities regularly, identifying and prioritizing the most critical ones, and implementing remediation measures.
- Problem Management: Majorly its aids in the identification, analysis, and resolution of security-related issues that may arise within an entity. To reduce the risk of future occurrences, it is critical to have a process in place to identify, diagnose, and fix security vulnerabilities or incidents.
- Configuration Management: This assists in ensuring the security of an entities technologies, IT, OT, IoT and ET systems and infrastructure, as well as the proper control and tracking of changes to those systems. This can include putting in place security controls, such as access controls, to safeguard sensitive data and resources.
- Continuity Management: it is critical for ensuring an entities ability to continue operations in the event of a security incident or disruption. This can include creating incident response plans and procedures and regularly testing and training to ensure the plans are effective.
- Data Management: The process of protecting and managing sensitive data, such as personal information, financial data, and proprietary information, is known as data management. This includes putting in place data-protection safeguards such as identification, decomposition, classification, encryption and developing policies and procedures for managing and storing data.
- Service Level Management: The process of ensuring that an entity's IT, OT, IoT,IIoT and ET systems and services meet the needs of its customers and stakeholders is known as service level management. Entities can ensure that their systems meet the required standards and that customers and stakeholders are satisfied with the service provided by having clear service level agreements (SLA) and monitoring the performance of these systems. This is an example of monitoring and reporting on system availability, performance, and security.


Security in Operations
Incident Management
Livable, Capability, and Trust principles
Problem Management
Enterprise, Livable, Capability, and Trust principle
Event Management
Capability, Livable, Trust” Principles.
Service Level
Livable, Capability, Enterprise, and Trust Principles
Monitoring
Capability, Livable Principles.
Continuity Management
Strategic, Livable, Economical, Capability, and Trust Principles.
Fraud & Forensics Investigations
Livable and Capability principles.
Configuration Management
Enterprise, Trust, and Capability Principles.
Threat Intelligence
Capability, Enterprise, and livable Principles
Data Management
Strategic, Livable, Enterprise, Capability and Trust Principles
Realizes

Enterprise Architecture Module (EAM) Related to the Main Capability of Security in Operations

The enterprise architecture module shown below summarizes the capabilities and sub-capabilities of this main capability:


Running Cybersecurity and Cyber Risk
Security in Operations Capability
Part of
Incident Management
Problem Management
Event Management
Monitoring
Continuity Management
Fraud & Forensics Investigations
Configuration Management
Threat Intelligence
Data Management
Service Level Management
Flow
Serves
Flow
serves
Serves
Associate with
Realize
Livable Principles
Capability Principles
Trust Principles
Enterprise Principles
Strategic Principles
Economical Principles
Process , Resources , Information & Data , Tools & Technology
Incident Management Function
Incident Management System
Security Incident Management System
Alerting/Notification System
Incident Management Controls
Problem Management Function
Problem Management Controls
Event Management Function
Security Information & Even Management System (SIEM)
Security Automation & Orchestration (SOAR)
XDR Platform
Event Management Controls
Monitoring Function
Security Monitoring Tool
Intrusion Detection & Prevention
Know Vulnerability Database (CVE)
Log Monitoring & Analytics
Vulnerability Monitor
Employee/Use Monitoring & Behavior Analysis
Monitoring Controls
Continuity Management Function
Business Continuity Management
Continuity Management Controls
Fraud & Forensics Investigations Function
Fraud & Forensics Investigations Controls
Configuration Management Function
CMDB
Discovery System
Configuration Compliance Monitoring
Configuration Management Controls
Threat Intelligence Function
Threat Intelligence Platform
Threat Intelligence Controls
Data Management Function
Data Discovery & Classification
Backup &Recovery System
Encryption Management
Data Loss & Data Leak Prevention
Data Management Controls
Service Level Management Function
Service Level Management Controls
flow
Serve
flow
Cyber Philosophy
++
JCSC
The Other Capabilities
ENTITY
Assigned to
Operation Capability Cyber Cycle
Entegrated Cyber Security and Cyber Risk Managment Process
Access
Cyber Secuirty Operation DATA
Cyber Incident Data
Security Incident, Security Incident Response Plan,After Action Review
Cyber Problem Register
Security Problem
Cyber Event Register
Security Event,Security AI Model
Monitoring Information
Security Monitor, Availability Data, Vulnerbility,Common Vulnerbility & Expousre (CVE),Log Data
Configuration & Asset Data
Service/Product Instance,Configuration Polisies,Firewall Rules,Configuration Compliance
Continuity Plan
Continuity Plan,Continuity Test
Backup Policy
Backup Schedule,Plan,etc
Treat Intelligence Reports
Indicator of Compromise (IOC),Treat Actor
Service Level Policy
SLA,Availability & Perfomance Data, Service Review
Cyber Securiy and Cyber Risk Managment Data Model

The next points are to describe the model

- The capabilities consist of the below main capabilities:
  - Incident Management Capability
  - Problem Management Capability
  - Event Management Capability
  - Monitoring Capability
  - Continuity Management Capability
  - Configuration Management Capability
  - Threat Intelligence Capability
  - Data Management Capability
  - Service Level Management Capability
  - Fraud & Forensics Investigations Capability

- The operation cycle's "Run" phase, also known as security in operations functions, provides a framework for the secure operation of digital products and services, ensuring that all running systems are within defined boundaries and managed securely, with a comprehensive overview of business operations and security operations to provide an understanding of relationships and responsiveness to business needs.
- Each main capability realizes some main principles as below, where each realization may be associated with the other capability in a collaboration manner:
  - The Incident Management Capability realizes all "Livable, Capability and Trust "principles.
  - The Problem Management Capability realize all the "Enterprise, Livable, Capability and Trust" principle.
  - The Event Management Capability realizes all the "Capability, Livable, Trust" Principles.
  - The Monitoring Capability realizes all the "Capability and Livable" principles.
  - The Continuity Management Capability realizes all the "Strategic, Livable, Economical, Capability and Trust" Principles.
  - Fraud & Forensics Investigations Capability realize all the "Livable and Capability "principles.
  - Configuration Management Capability realizes all the "Enterprise, Trust, and Capability" Principles.
  - Threat Intelligence Capability realizes all the "Capability, Enterprise, and livable" Principles.
  - Data Management Capability realizes all the "Strategic, Livable, Enterprise, Capability and Trust" Principles.
  - Service Level Management Capability realizes all the "Livable, Capability, Enterprise and Trust" Principles.
- All of sub capabilities are formed by utilizing, developing, and maintaining underlying functions, which may include Tools, People, Technology, and information or data.
- Each Main Sub Capability complements the others.
- In terms of serving and information flow, the entire capability is unquestionably linked to the rest of the framework capabilities.
- The Main Data output from the planning eco-cycle as part of the holistic cyber data models are:

  -Cybersecurity Incident Data
  -Cybersecurity Problem Register
  -Monitoring Information
  -Backup Policy
  -Service Level Policy
  -Cybersecurity Event Register
  -Continuity Plan
  -Configuration & Asset Data
  -Threat Intelligence Reports
- This main capability is part of influencing the General Philosophy of the Jordan Cyber Security Center.

Benefits to the Capability of Security in Operations

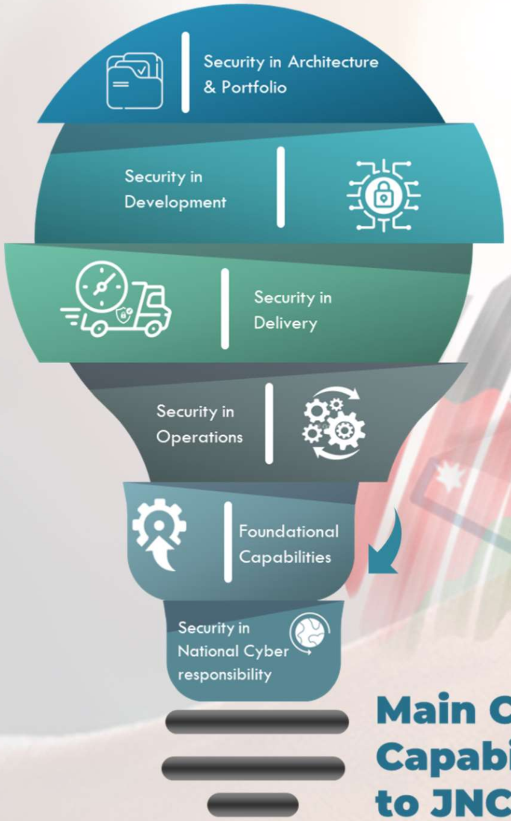
The key benefits for security in operations are:

Benefits

- Increase Efficiency and Reduce Cost.
- Reduce Risk.
- Continuous Service Improvement.
- Other Benefits of Security in Operations.

Increase efficiency and reduce cost by:

- Centralized Event Management for faster analysis.
- Automation between and across business functions.
- Knowledge management and self-service linkage.
- Improving the speed at which issues with an Actual Product Instance are identified.
- Driving operating/service level targets.
- Improving the speed at which issues with an Actual Product Instance are proactively detected.


Security in Architecture & Portfolio
Security in Development
Security in Delivery
Security in Operations
Foundational Capabilities
Security in National Cyber responsibility

Main Consolidating Capabilities Related to JNCSF

Fundamental Capabilities

Fundamental capabilities in cybersecurity are the foundational skills and knowledge that entities and individuals must have in order to effectively protect their services, systems, networks, and data from unauthorized access, misuse, and malicious attacks. These capabilities are essential for ensuring the confidentiality, integrity, and availability and safety of information and services, which are the four main pillars of information security.

- One of the most important fundamental capabilities in cybersecurity is policy management which refers to the process of creating, implementing, and maintaining policies hirarichy and procedures that govern an entities security practices. These policies and procedures are designed to ensure that the entities information assets are protected and that the entities is in compliance with relevant laws, regulations, and industry standards.

- Another fundamental capability in cybersecurity is the risk and compliance management, which is the process of identifying, measuring, and prioritizing potential threats to an entity and taking steps to minimize or eliminate those risks. It also involves ensuring that the entity is in compliance with all relevant laws, regulations, and industry standards.

- One more fundamental capability in cybersecurity is the audit management, which is the process of evaluating an entities services, information and technology systems, processes, and controls to ensure that they are functioning effectively and efficiently and that they are in compliance with relevant laws, regulations, and industry standards. Audit management is a key element of overall risk and compliance management.

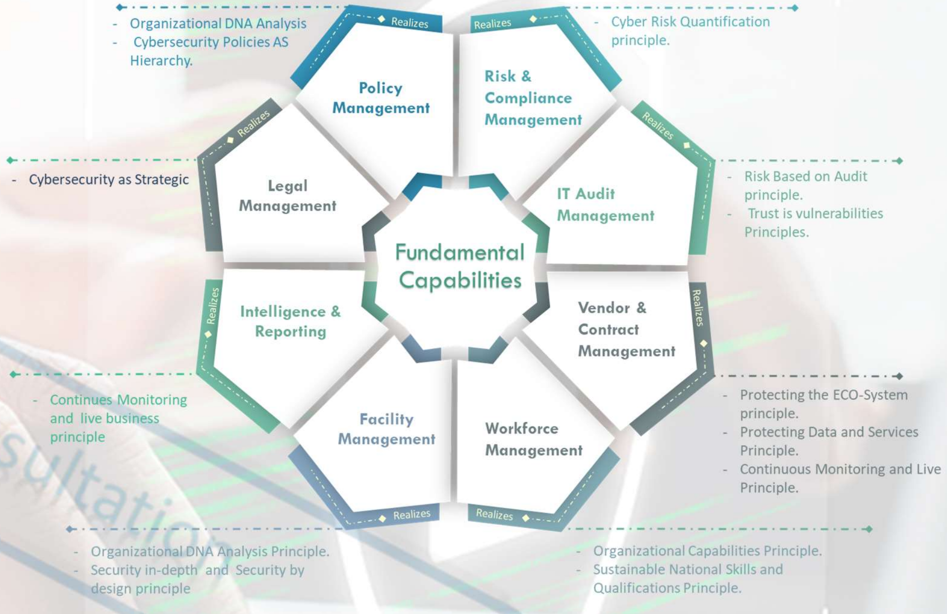
- Vendor and contract management, whichrefers to the process of managing relationships with external vendors and the contracts and agreements that govern these relationships. This process involves identifying, measuring the risks of selecting vendors, managing the procurement process, and overseeing the performance of vendors and the fulfillment of their contracts according to the entity's Cybersecurity standards.

- Workforce management, is the process of coordinating and optimizing the activities of employees within an entity. This includes tasks such as scheduling, forecasting, and analyzing workforce data, security checks, hiring, and training employees, and setting goals and priorities in order to improve efficiency and productivity. Workforce management is typically concerned with ensuring that an entity has the right number of employees with the right skills in the right place at the right time, in order to meet the needs of the business.

- Legal management is another fundamental capability in cybersecurity, this refers to the process of managing the legal affairs and risks of an entity. This can include tasks such as reviewing and drafting legal documents, providing legal advice, managing litigation and disputes and ensuring compliance with laws and regulations. The goal of legal management is to protect the entities interests and assets, minimize legal risk, and ensure compliance with laws and regulations that apply to the entities operations and activities.

- Facility management (FM) is another fundamental capability in cybersecurity, which is the process of managing and maintaining an entities buildings, equipment, and grounds, as well as the services that support the core business of an entity. It is an interdisciplinary field that includes a wide range of activities, such as maintenance, security, cleaning, energy management, safety, and health. The goal of facility management is to ensure that the entities physical assets and infrastructure are well-maintained, safe, and secure and that they support the entities operations and objectives.

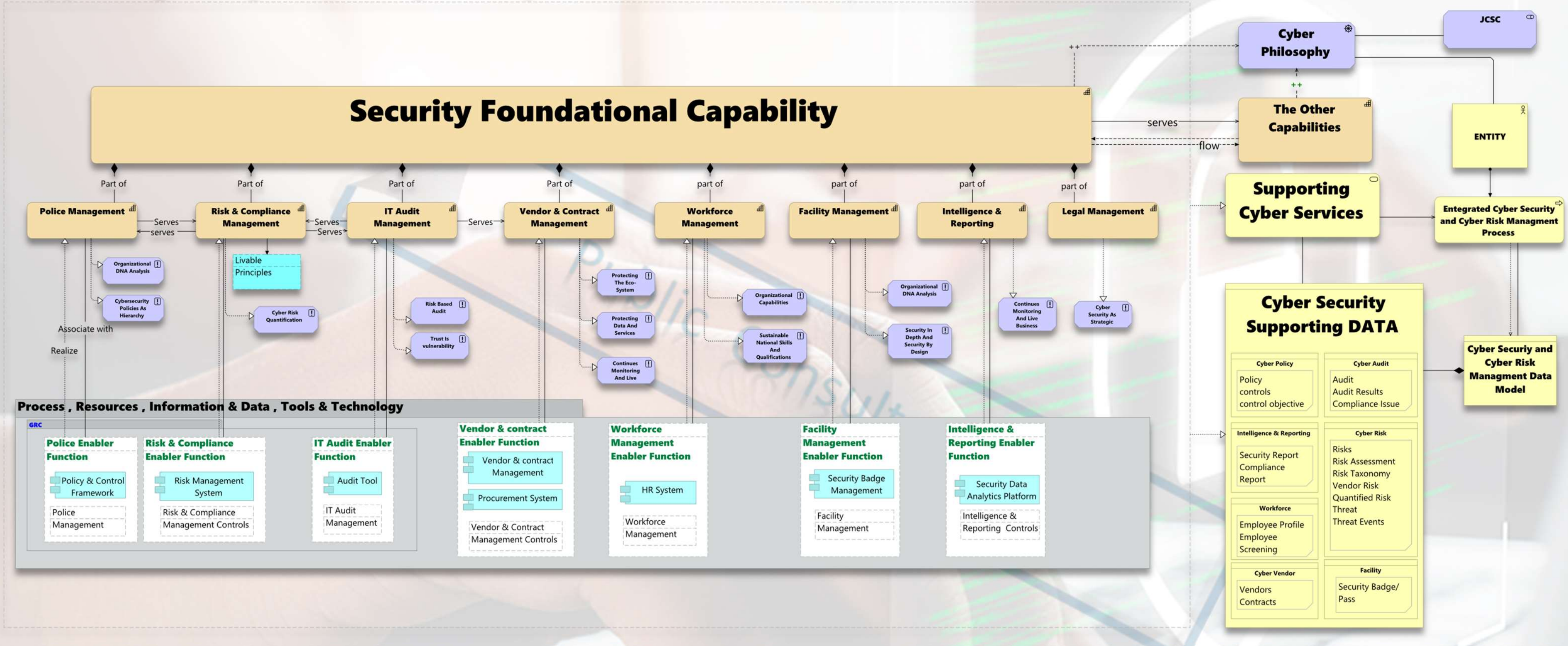
- Finally, intelligence and reporting is another fundamental capability in cybersecurity, this refers to the process of gathering, analyzing, and disseminating information about cyber threats, vulnerabilities, and attacks that are relevant to an entities information systems and networks. This can include tasks such as monitoring for malicious activity on the entities networks, analyzing log data and threat intelligence, and identifying patterns and trends that can indicate a potential cyber attack.


Fundamental Capabilities
Policy Management
Risk & Compliance Management
IT Audit Management
Vendor & Contract Management
Workforce Management
Facility Management
Intelligence & Reporting
Legal Management
Realizes
- Organizational DNA Analysis
- Cybersecurity Policies AS Hierarchy.
- Cyber Risk Quantification principle.
- Risk Based on Audit principle.
- Trust is vulnerabilities Principles.
- Protecting the ECO-System principle.
- Protecting Data and Services Principle.
- Continuous Monitoring and Live Principle.
- Organizational Capabilities Principle.
- Sustainable National Skills and Qualifications Principle.
- Organizational DNA Analysis Principle.
- Security in-depth and Security by design principle
- Continues Monitoring and live business principle
- Cybersecurity as Strategic

Enterprise Architecture Module (EAM) Related to the Fundamental Capabilities

The enterprise architecture module shown below summarizes the capabilities and sub-capabilities of the fundamental capabilities:

Supporting for Cybersecurity and Cyber Risk


Cyber Philosophy
JCSC
Security Foundational Capability
serves
flow
The Other Capabilities
ENTITY
Supporting Cyber Services
Entegrated Cyber Security and Cyber Risk Managment Process
Cyber Securiy and Cyber Risk Managment Data Model
Part of
Part of
Part of
Part of
part of
part of
part of
part of
Police Management
Serves
serves
Risk & Compliance Management
Serves
Serves
IT Audit Management
Serves
Vendor & Contract Management
Workforce Management
Facility Management
Intelligence & Reporting
Legal Management
Organizational DNA Analysis
Cybersecurity Policies As Hierarchy
Associate with
Realize
Livable Principles
Cyber Risk Quantification
Risk Based Audit
Trust Is vulnerability
Protecting The Eco-System
Protecting Data And Services
Continues Monitoring And Live
Organizational Capabilities
Sustainable National Skills And Qualifications
Organizational DNA Analysis
Security In Depth And Security By Design
Continues Monitoring And Live Business
Cyber Security As Strategic
Process , Resources , Information & Data , Tools & Technology
GRC
Police Enabler Function
Policy & Control Framework
Police Management
Risk & Compliance Enabler Function
Risk Management System
Risk & Compliance Management Controls
IT Audit Enabler Function
Audit Tool
IT Audit Management
Vendor & contract Enabler Function
Vendor & contract Management
Procurement System
Vendor & Contract Management Controls
Workforce Management Enabler Function
HR System
Workforce Management
Facility Management Enabler Function
Security Badge Management
Facility Management
Intelligence & Reporting Enabler Function
Security Data Analytics Platform
Intelligence & Reporting Controls
Cyber Security Supporting DATA
Cyber Policy
Policy
controls
control objective
Cyber Audit
Audit
Audit Results
Compliance Issue
Intelligence & Reporting
Security Report
Compliance
Report
Cyber Risk
Risks
Risk Assessment
Risk Taxonomy
Vendor Risk
Quantified Risk
Threat
Threat Events
Workforce
Employee Profile
Employee
Screening
Cyber Vendor
Vendors
Contracts
Facility
Security Badge/
Pass

The next points are to describe the model

- The capability services as a supporting phase regarding achieving an integrated cyber security and cyber risk management process WHERE each entity is directed to ensure the execution of the process.
- Each main capability realizes some main principles as below, where each realization may be associated with the other capability in a collaboration manner:

1. **Policy Management Capability** realizes two Principles entity DNA Analysis & Cybersecurity Policies AS Hierarchy.
2. **Risk & Compliance Management Capability** realizes all livable principles and realizes the Cyber Risk Quantification principle.
3. **IT Audit Management Capability** realizes Risk Based Audit principle and Trust is vulnerabilities Principles.

4. **Vendor & Contract Management** realize protecting the ECO-System principle, protecting Data and Services principle, and Continuous Monitoring and Live principle.
5. **Workforce Management Capability** realize entity Capabilities Principle and Sustainable National Skills and qualification Principle
6. **Facility Management** realize entity DNA Analysis Principle and Security in depth and security by design principle
7. **Intelligence & Reporting Capability** realize Continues Monitoring and live business principle
8. Legal Management capability realizes cyber security as a strategic imperative

- All the sub-main capabilities are formed by utilizing, developing, and maintaining underlying enabler functions that may consist of tools, people, technology, and information or data where some technology tools are mentioned in the architecture.
- The full capability is connected to the rest of the framework capabilities in terms of serving wise and flow of information.
- The primary data output from the planning eco-cycle as part of the holistic cyber data models are :

  - Cybersecurity Policy
  - Intelligence & Reporting
  - Facility Management
  - Cybersecurity vendor
  - Cybersecurity Risk
  - Cybersecurity Audit
  - Workforce Management

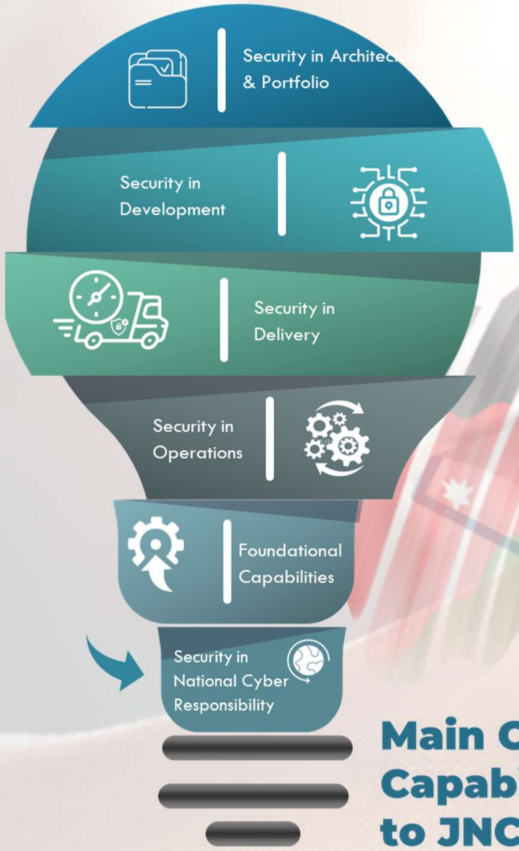
- The capability is part of influencing the general philosophy of the Jordan Cyber Security Center.

Benefits to the Fundamental Capabilities

Benefits

- They provide a basic level of protection for an organization's assets and data.
- They help to identify and mitigate cyber risks.
- They support compliance with regulatory requirements.
- They improve overall security posture and resilience.
- They can help to prevent cybercrime and protect intellectual property.
- They can reduce costs associated with security breaches.

- **They provide a basic level of protection for an entities assets and data:** Without basic security measures, an entities data and information may be vulnerable to cyber-attacks; that is why one of the most important benefits of foundational capabilities from cyber attacks is providing essential information protection.
- **They help to identify and mitigate cyber risks:** Without incident response and security awareness training, an entity may be unable to detect and respond to cyber threats effectively, and having the basic capability will solve such a problem.
- **They support compliance with regulatory requirements:** Many industries are subject to regulations that necessitate specific security measures. Without foundational capabilities, an entity may be out of compliance and subject to fines or penalties.
- **They improve overall security posture and resilience.**



Main Consolidating Capabilities Related to JNCSF

Security in National Cyber Responsibility

Cybersecurity is a collective responsibility, shared between countries, businesses, accademia and individuals. Countries worldwide are increasingly realizing cybersecurity's importance in protecting national security and its significant impact on economic growth. As a leading country in this field and a member of the elite promoting social interaction to deepen their understanding of cybersecurity and its information, Jordan has been keen to support cybersecurity as an idea and application that combines the social and economic sectors harmoniously and efficiently.

And as a country of security and safety and a destination for students and investors worldwide, it was easy to transform it into an awareness center for cybersecurity and its applications.

This is accomplished by facilitating safe and interactive investment opportunities and by providing cybersecurity awareness and training programs at the student level, in collaboration with various economic entities throughout the Hashemite Kingdom Of Jordan, private and governmental, with universities, colleges, and youth groups, all to implant the concept and refine the application of cybersecurity, as well as benefiting from youth ideas in this field.

This collaboration and these programs will aid in the following areas:

- Introducing the concept of cyber security and raising awareness about the significance of its application
- The discussion and the exchange of experiences will aid in developing the approved cybersecurity curricula.
- Taking advantage of and adopting youth ideas, in addition to allowing the field to keep up with generations and their ideas.
- Increase awareness of the importance of cyberattack protection and how to avoid them.
- Encourage, enable and foster Cybersecurity Startups to initaiate building National Cybersecurity Products and Technologies.

All of the above is the essence of Security in National Cyber Responsibility as a main capability.

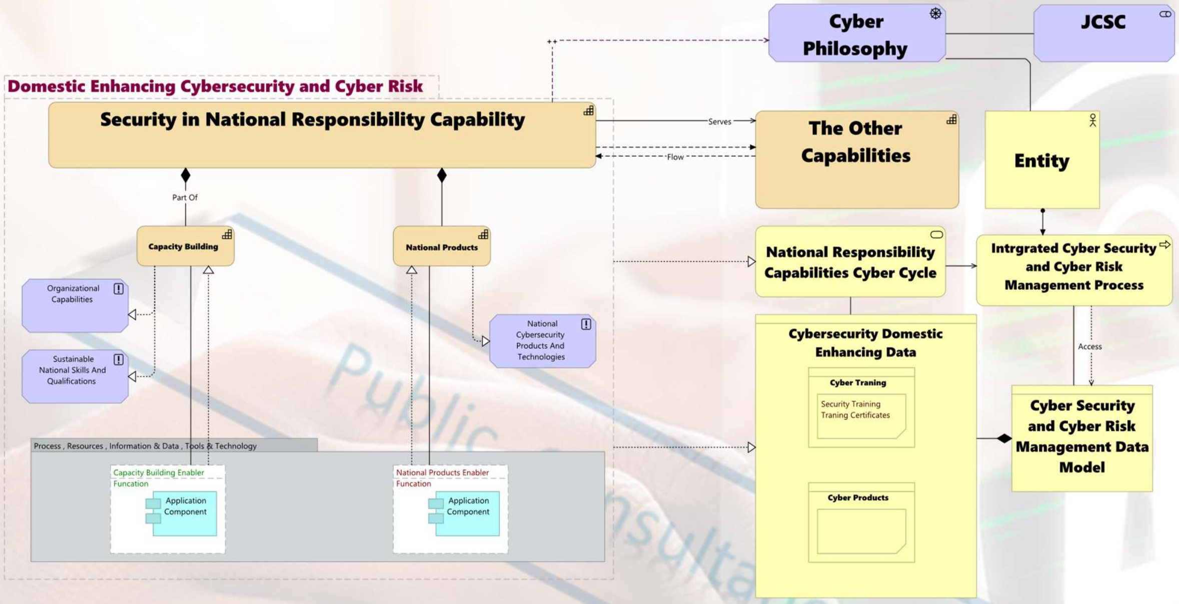
This main capability consists of the following capabilities:

- Capacity Building: All organizations need to develop value-driven programs to enable universities students to gain knowledge, skills and qualifications which will help the nation to develop and sustain the national capabilities and to fullfill the high demand on cybersecurity resources.

- Building National Cybersecurity Products: All organizations need to develop value-driven programs to motivate and enable cybersecurity startups as well as national companies to develop and enhance cybersecurity products and solutions.

Enterprise Architecture Module (EAM) Related to the Main Capability of Security in National Cyber Responsibility

The below Enterprise architecture modeling view summarizes the security National Responsibility Capabilities:


Domestic Enhancing Cybersecurity and Cyber Risk
Security in National Responsibility Capability
Part Of
Capacity Building
National Products
Organizational Capabilities
Sustainable National Skills And Qualifications
National Cybersecurity Products And Technologies
Process , Resources , Information & Data , Tools & Technology
Capacity Building Enabler Funcation
Application Component
National Products Enabler Funcation
Application Component
Cyber Philosophy
JCSC
Serves
Flow
The Other Capabilities
Entity
National Responsibility Capabilities Cyber Cycle
Intrgrated Cyber Security and Cyber Risk Management Process
Access
Cybersecurity Domestic Enhancing Data
Cyber Traning
Security Training Traning Certificates
Cyber Products
Cyber Security and Cyber Risk Management Data Model

The next points are to describe the model

- The capability services as the National Responsibilities phase for achieving an integrated cyber security and cyber risk management process in which each entity is directly responsible for ensuring process execution.
- Where each may be associated with the other capability in a collaborative manner:
  - Capacity Building capability highlights the principle of organizational capabilities and the principle of sustainable national skills and qualifications.
  - National products capability realizes national cybersecurity products and technologies principle.
- All sub-capabilities are created by utilizing, developing, and maintaining underlying enabler functions such as Tools, People, Technology, and information or data where technology tools are mentioned in the architecture.
- The full capability is inextricably linked to the rest of the framework capabilities regarding serving and information flow.
- The Main Data output from the planning eco-cycle as part of the holistic cyber data models are Cybersecuity Training and awarness and National Cybersecuity vendors
- Capability is part of influencing the General Philosophy of the Jordan Cyber Security Center.

Benefits of the Main Capability of Security in National Cyber Responsibility

Benefits

- Increased availability of highly skilled cybersecurity professionals.
- Attract international investments.
- Encourage entrepreneurship and innovation.
- Cooperate with educational authorities to develop curricula on cybersecurity.

- Increased availability of highly skilled cybersecurity professionals can lead to more secure and stable economic systems and promote economic growth and innovation by providing businesses with the tools and resources they need to protect their digital assets, reducing the lack of a skilled workforce in the cyber security field.

- Attract international investment and boost trust in the country's digital infrastructure, which can significantly attract foreign investment.

- Encourage entrepreneurship and innovation by giving students and professionals the necessary skills and knowledge to start cybersecurity-focused businesses. This will have an economic impact by providing unlimited research and development that increase the opportunity to capitalize on the accelerated digital transformation cycle achieving economic growth. Interaction between governmental and private entities with educational institutions will help to alleviate this problem by providing funds for research and adopting related youth ideas.