الاستراتيجية الوطنية
للأمـن السيـبـــــــراني

NATIONAL CYBER SECURITY STRATEGY

2024 - 2030

State of Qatar

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Foreword from
His Excellency the Prime Minister of Qatar

“Cybersecurity is pressing imperative in our lives to maintain the security of our economy, infrastructure and personal information for our people in the light of the rapid development we are witnessing. Given Qatar’s ambitious visions, we need a strategy that enables us to manage risks, address cyber threats and enhance Qatar’s prosperity as modern technologies evolve. The launch of the National Cyber Security Strategy is part of our endeavour to support our ambitious society in keeping with the technological development that our world is witnessing through its principles and objectives.

This strategy will undoubtedly be a fundamental pillar for achieving Qatar’s 2030 vision.

This strategy has been designed to put innovation and adaptability at the core of it, recognize that cyber threats are evolving and increasing in complexity. In order to protect Qatar’s digital and sovereign assets by employing the best available expertise, competencies and techniques, the strategy stressed the need for effective partnerships to exchange information and expertise with local and international public and private entities, as well as providing the appropriate environment for attracting, training and developing the best cyber security professionals.

We affirm the need for all residents of Qatar to cooperate and join forces in their different nationalities and cultures in order to promote the State of Qatar and enhance its prosperity. This is a place that the new Cyber Security Strategy will seek to consolidate in order to safeguard the security of our digital assets and place the State of Qatar at the forefront of contributing to the development of cyber security in the international arena.”

His Excellency Sheikh Mohammed bin Abdulrahman bin Jassim Al-Thani
Prime Minister and Minister of Foreign Affairs

Foreword from His Excellency the President of NCSA

“I have the honour to put in your hands Qatar’s new National Cyber Security Strategy, through which we aspire to have our state at the forefront of countries seeking to ensure the safe use of current and emerging technologies, this laying solid foundations for a future society.

Our world is expecting a fast-moving digital transformation that has made cybersecurity one of the greatest challenges facing countries today. Because interconnected services were growing in number and digital channels were of unprecedented importance, cyberspace had direct effects on the realities of national security and people’s daily lives, and a comprehensive, resilient and forward-looking National Cyber Security had to be adopted.

Designed to address these challenges and emerging threats, this strategy also aims to enable our nation to thrive and take advantage of the latest technological innovations. Recognizing the need to protect critical systems and infrastructure from cyberattacks using advanced methodologies that recognize the shift from cyber risk to digital risk and from cyber security to cyber resilience.

In addition to addressing emerging threats, the strategy also emphasises the importance of innovation, R&D, and talent attraction. The strategy recognises that a strong workforce is crucial for effective cyber security. In this spirit, it seeks to prepare a variety of competent personnel in the field.

The strategy also attaches great importance to promoting innovation in the cybersecurity sector by creating an environment in which entrepreneurs and start-ups can design innovative solutions to cybersecurity challenges.

The new Cyber Security Strategy presents a comprehensive and modern approach to strengthen cyber security, one that prepare the State of Qatar to deal with the challenges of the future. At the same time, it encourages innovation, research and development, and the preparation and attraction of specialized cadres so that Qatar becomes and active contributor to the global cybersecurity system.”

His Excellency Eng. Abdulrahman bin Ali Al-Farahid Al-Malki
The President of National Cyber security Agency

TABLE OF **CONTENTS**

LIST OF TABLES

LIST OF FIGURES

GRATITUDE & APPRECIATION

Enriched constructive inputs from stakeholders within the National Cyber Security Agency and various institutions and entities in the State contributed to the development of the National Cyber Security Strategy. The Strategy's development journey included joint action and several workshops with different sectors to study Qatar's cyber landscape, strengths, current and future risks, challenges, and opportunities.

The National Cyber Security Agency takes this opportunity to thank and appreciate all institutions and entities involved in developing, reviewing, and adopting the National Cyber Security Strategy.

National Cyber Security Agency
الوكالة الوطنية للامن السيبراني

INTRODUCTION

In recent years, technology has reshaped the way of life, work, and social interactions both in Qatar and globally. Digital transformation has unleashed new prospects as well as new challenges. It is crucial to harness the potential of emerging technologies, ensure safety and security online, enhance overall national cyber security capabilities, and develop a dynamic cyber security industry. However, in a hyper-connected world, threats in cyberspace are continually evolving. The public and private sectors and individuals must unite their efforts to ensure a safe cyber environment in which Qatar can prosper.

Qatar has consistently recognized that cyber security should strike a balance between protecting organizations and individuals and maximizing the opportunities of digitalization. This consistent, proactive, and comprehensive approach has been successful in Qatar. It has resulted in the creation of the Qatar Computer Emergency Response Team (Q-CERT) in 2005, the publication of the first National Cyber Security Strategy (NCSS) in 2014, the development of laws and regulations to secure cyberspace, the establishment of the Cyber Security Center of the Ministry of Interior, and an increase in investments in emerging technologies, research and innovation as a result of enhanced trust in the safety and security of those technologies. Qatar's approach has also led to the implementation of initiatives to raise awareness and knowledge of cyber security, as well as the development of several partnerships at the regional and international levels – all aimed at increasing the nation's cyber security maturity.

As technology and interconnectivity have grown, so too have cyber challenges. Cyber threats are dynamic and increasing in sophistication, frequency, and impact. The dynamic threat landscape requires the NCSS to be refreshed to meet current national cyber security needs while allowing for digital innovation. The establishment of the National Cyber Security Agency (NCSA) in 2021, whose mandate includes coordinating cyber security activities in the country, was an additional driver to develop a new NCSS. As cyber security is a shared responsibility, the NCSS 2024–2030 represents a collective call to action for all organizations and individuals in Qatar. The new NCSS builds on past efforts and successes and has benefited from the collective input of more than 30 organizations, including government, industry, and academia. It is aligned with and will contribute to Qatar National Vision 2030. Additionally, efforts have been made to align the new NCSS with the National Development Strategy.

The new NCSS will guide Qatar's efforts to enhance cyber resilience, promote a cyber security culture throughout society, and drive research, innovation, and investments in cyber security. It will also drive efforts to increase cyber security capabilities and capacity and create new opportunities for Qatar, promoting a secure and prosperous digital age.

01

CYBER SECURITY CURRENT CONTEXT

1. Cyber Security
Current Context

Qatar has been on a journey of continuous improvement in cyber security, with significant achievements in the field in the past few years. However, the global cyber threat landscape continues to evolve, and new challenges have emerged. The NCSS will help Qatar enhance its cyber security capabilities to respond to these global challenges effectively.

1.1 Cyber Threat Landscape

Over the years, malicious groups have continued to increase the volume of cyber-attacks, simultaneously diversifying the types of such attacks. Threat actors are using increasingly sophisticated tools, expanding their targets, becoming more determined to perpetrate cyber-attacks not only on Information Technology (IT) but also on Operation Technology (OT) environments, and implementing attack methods that evade detection. This makes the global cyber threat landscape extremely unpredictable[1]. Globally, the average ransomware attack cost was estimated at (US$ 4.54 million[2]) in 2022, and the global average data breach cost was (US$ 4.35 million[2]) .

Specifically, the average cost of a data breach initiated by social engineering techniques was (US$ 4.10 million[3]) in 2022. However, on average, the costliest initial attack vectors were phishing (US$ 4.91 million[2]) followed by business email compromise (US$ 4.89 million[2]).

- **Average cost of ransomware attacks**
  2022
  4.54
  Million US Dollars

- **Average cost of data breach**
  4.35
  Million US Dollars

- **Phishing messages**
  4.91
  Million US Dollars

- **Corporate email breach**
  4.89
  Million US Dollars

The most significant systemic challenge to the country and the global economy lies in cyber-attacks targeting the energy sector – particularly gas – where the country's supply is critical to many international partners. Qatar is in a key position internationally: its location, energy reserves, capital, people, and culture have made it an essential global partner. However, Qatar's increasing importance on the global stage has made the country an attractive target for cyber threats. It is necessary to continuously enhance national cyber security capabilities, to face evolving cyber risks, and to reduce the country's exposure to potential cyber-attacks or disruptions.

1.2 Qatar's Responses and Achievements up to 2024

Qatar was the first country in the region to identify Cyber-attacks as a national threat, leading to the establishment of Qatar Computer Emergency Response Team (Q-CERT) in 2005, whose efforts were directed towards four key activities:

- provide accurate and timely information on current and emerging information security threats and vulnerabilities;
- respond to threats and vulnerabilities relevant to national constituencies;
- promote the adoption of information security standards, processes, methods, best practices, and tools; and
- build the local capacity and capability to manage cyber risks by providing specialized training and awareness.

The country's commitment to cyber security was demonstrated by delivering the first Qatar National Cyber Security Strategy (2014). Since then, Qatar has taken steps to centralize cyber security governance and coordinate national efforts, with the critical turning point being the establishment of the NCSA[4] in 2021.

In preparation for the 2022 FIFA World Cup, Qatar released the "Qatar 2022 Cyber security Framework"[5]. The result of a collaborative effort, this comprehensive framework defined the cyber security capabilities required to safeguard critical national services and digital platforms supporting the World Cup.

The successful delivery of the Qatar 2022 FIFA World Cup demonstrated the effectiveness of Qatar's efforts to develop national cyber capabilities.

Cyber Industry and Innovation

Qatar is actively promoting the development of its local cyber security industry and digital research and cyber innovation programs, its cyber security market was estimated at US$1 billion in 2022 and is expected to reach US$1.6 billion by 2026 (annual growth of 12.7%)[6].

The government has also established research centers for cyber security, providing funding to support cyber security innovation and research in industry. For example, QSTP provides state-of-the art facilities and support services to start-ups, tech ventures, and global technology companies, the Qatar National Cyber Security Research Lab (NCSRL) , supports the development of national cyber security plans and programs for research and development in partnership with domestic and international industry, academia, and research institutions, and Qatar Computing Research Institute (QCRI) is another such research center that has been working to identify new threat vectors, and develop cyber security solutions tailored to national needs. Additionally, these research centers have contributed to training cyber security professionals, enhancing national capacity and capability to manage cyber-attacks.

Development of Laws and Regulations to Secure Cyberspace

Qatar adopted a cybercrime law, the Cybercrime Prevention Law No. 14 of 2014, which covers crimes involving hacking into computer systems, information programs, networks, and websites[7]. Qatar has since issued other important cyber-related legislation, such as the Personal Data Privacy Protection Law No.13 of 2016[8] , which regulates data privacy in the State of Qatar.

In addition, Qatar has adopted a set of policies and frameworks, such as the National Data Classification Policy and the National Information Assurances Standards (NIA), which provide direction on how to implement a full-fledged Information Security Management System (ISMS). The country has also established policies and standards covering cyber security in areas such as cloud security, industrial control systems, and standards for secure software development lifecycle, among other topics.

The country has also made great efforts to address supply chain risks. Qatar has developed the National Information Security Compliance Framework (NISCF), which offers Certification services for organizations and Accreditation services for Service Providers. It complements Qatar's National Information Assurance Framework to establish a safe and vibrant cyberspace.

Additionally, the State of Qatar has been authorized by the Common Criteria Management Committee of the Common Criteria Recognition Arrangement, to issue Certificates for Information Security of IT Products and Systems

Establishing solid foundations to enhance cyber capabilities and awareness

Qatar has been pivotal in raising capacities and building competencies in cyber security and launching multiple national programs to disseminate cyberculture and cyber awareness to address risks and threats to all segments of society. A key initiative framework being the Cyber Eco, a cyber security curriculum project in partnership between the National Cyber Security Agency and the Ministry of Education and Higher Education.

Global Contributions and International Commitments

At the international level, Qatar has endorsed and pursued significant initiatives to contribute to global cyber security resilience. It has promoted information sharing and collaboration while increasing its participation in regional and international cyber bodies. Some key examples of such involvement include

Project Stadia[9] – an INTERPOL initiative that supports global cooperation on security arrangements, including cyber, in major sporting events, the Open-Ended Working Group (OEWG), established by General Assembly resolution 73/27 to address pressing global cyber security challenges by fostering dialogue and collaboration among UN member states, industry stakeholders, nongovernmental organizations, and academia, and the Common Criteria Recognition Arrangement (CCRA).

Although Qatar has taken several steps to enhance its cyber resilience, the country must continue to adapt and push onward to meet rising challenges. The following section describes several pressing cyber security challenges that countries worldwide, including Qatar, face, as well as potential opportunities in cyberspace.

1.3 Challenges and Opportunities

Cyber-attacks are becoming more frequent, sophisticated, and severe. The world, including Qatar, faces a growing range of challenges to which the new NCSS must respond. Nevertheless, such challenges can also bring new opportunities to enhance cyber security capacity and capability.

- **National cyber risk and crisis management to effectively tackle the changing cyber threat landscape**

The rising frequency of cyber-attacks against CNI is a growing global cause for concern. International studies have shown that organizations experiencing cyber disruption incur an average financial loss of around US$2.8 million per incident, with the oil and gas industry being the most heavily impacted[10]. In addition to financial losses, the potential risk of severe disruption to CNI could lead to a national and even global crisis.

THE MOST AFFECTED

Oil & Gas sector is highly impacted by cyber-attacks targeting the national critical infrastructure

2.8 Million US Dollars

Average global losses incurred by organizations due to cyber disruptions

Countries can deal with this threat by developing consistent methodologies and approaches to national cyber risk and crisis management practices. These methodologies can allow authorities to enhance national capabilities and prepare for potential cyber threats regarding protection, detection, and response. Additionally, they can help mitigate long-term effects, such as increased vulnerability to future attacks, reputational damage, and loss of public trust.

■ Cyber threat information sharing and cyber incident response capabilities to counter sophisticated cyber-attacks

Malicious actors continually refine their tools and techniques, increasing the sophistication and frequency of cyber-attacks. Organizations, therefore, need robust and efficient cyber threat intelligence sharing practices.

The exchange of knowledge and information about cyber threats, incidents, vulnerabilities, mitigations, and best practices can improve strategic national coordination and collaboration among stakeholders and enhance cyber incident management capabilities. Cyber threat information sharing, coupled with more robust cyber incident management capabilities, increase the overall ability to protect against cyber threats.

■ Coordination and cooperation among Critical National Infrastructure (CNI) stakeholders to improve cyber security resilience

Cyber-attacks against CNI are a global concern but have particular relevance for Qatar. Successful attacks targeting CNI, such as in the energy sector, could disrupt the national, regional, and international economies.

CNI sectors, particularly those heavily reliant on Operational Technology (OT), represent high-level targets, making it vital to maintain a register of CNI and critical assets and their potential risks to the country.

More vital collaboration between government authorities, sector regulators, and CNI operators can enhance CNI's cyber security resilience. Working together, stakeholders can share information on potential cyber security threats and risk mitigation techniques. Information should be exchanged across different CNI sectors to ensure that experience learned in one industry can be used to protect other CNI sectors.

■ Supply chain security to protect the overall cyber environment

Many organizations rely on suppliers to deliver products, systems, and services. Since industry and the services sector change as technology develops, so do cyber threats. Securing the supply chain is as necessary as malicious actors either target suppliers as a route into a core entity or where they target critical operational platforms in use across different sectors. It requires a coordinated approach that focuses on potential risks in using third-party suppliers and develops an understanding of how weaknesses in one part of the chain can affect overall cyber security.

Appropriate legal and regulatory frameworks to tackle emerging cyber risks

As the technological environment develops, so do cyber risks. If legal and regulatory frameworks are not appropriately formulated and updated, the rapid rise of emerging technologies, new products, and services without clear security standards can create new vulnerabilities. This is mainly because the speed at which emerging technologies are developed and adopted is much faster than the ability of the legal system to mandate security measures[11]. For example, in recent years, organizations have adopted solutions involving artificial intelligence, machine learning (AI/ML), and the Internet of Things (IoT), which may pose relevant challenges if not properly understood and controlled.

Additionally, recent international studies have found that business executives recognize the value of cyber security laws and regulations as a means of reducing cyber risks[12]. Global best practices increasingly indicate that properly enforced cyber security regulations can contribute to cyber resilience across all sectors, including lowering risks from supply chains and sector interdependencies[12].

Therefore, this is a crucial opportunity to promote the development of appropriate legal and regulatory frameworks that consider the changing threat landscape, adapt to evolving technologies, and strike the right balance between security and innovation.

Cybercrime investigation and prosecution capacity and capabilities to promptly deal with new forms of cybercrime

Cybercrime has been described as one of the top ten global risks for the next decade[12]. With the rise of cybercrime-as-a-service worldwide, the sophistication of attacks is rising, while the bar for entry is lowered for potential criminals[13].

One significant challenge is law enforcement and the judiciary's capacity and expertise to investigate and prosecute cybercrimes. Keeping pace means constantly learning new techniques and skills, requiring countries like Qatar to provide enhanced training in cybercrime matters and equip law enforcement and the judiciary with the appropriate knowledge, tools, and skills.

Fighting cybercrime also requires national and international cooperation. The growing significance of digital evidence and forensics (especially in ensuring prosecution) means promoting and enhancing collaboration between law enforcement and other stakeholders is essential. The effective collection, sharing, preservation, and utilization of digital evidence is crucial, as is the exchange of cybercrime data and best practices. Continuously enhancing both the capacity and capability of law enforcement and prosecution authorities, providing them with the appropriate knowledge, skills, and tools, will represent an opportunity to tackle new forms of cybercrime promptly.

Stronger coordination to promote cyber security innovation

Accelerating cyber security innovation is vital to improving a country's cyber security technology. Cyber security innovation must keep pace with other emerging technologies to identify and manage potential cyber risks, thus enhancing the protection of individuals and organizations. For instance, although technologies such as quantum computing could solve complex problems much faster than classical computers and bring advancements to many industries, quantum computing could also threaten encryption systems that underpin the world's digital infrastructure[14]. Investing in cyber security innovation is essential to ensure that new technology entering the market is secure.

Cyber security innovation offers protection from potential and future risks and can also be an opportunity to develop the domestic cyber industry and potential exports. For cyber security innovation to become a critical economic enabler, greater coordination between academia, research-focused institutions, and industry is needed. Improved collaboration among stakeholders has the potential to facilitate the transition from cyber security research to market adoption by addressing any misalignment that may exist between research findings and business practices.

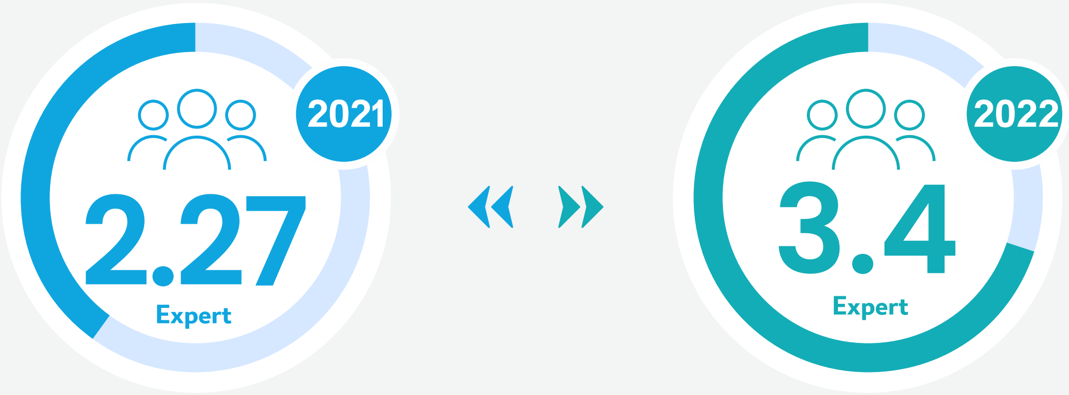
More investments to encourage the development of a national cyber security industry

Access to appropriate funding mechanisms can help support cyber security research and innovation projects, speeding up the translation of research and prototypes in start-ups, for example, into cyber security products commercialized in the market.

Providing incentives to strengthen the domestic cyber security industry and support cyber security startups and companies is a fundamental opportunity to diversify Qatar's economy and advance cyber security innovation. This effort should be coupled with measures to encourage investments to strengthen current established businesses and create new ones.

Expansion of incentives to pursue a cyber security career

The cyber workforce gap mismatch between the supply and demand of cyber security professionals is undoubtedly one of the most complex and pressing global cyber security challenges[15] and is a primary reason why organizations struggle to achieve cyber resilience. The shortfall between supply and demand for cyber security experts was estimated at 2.27 million poeple in 2021[16] and 3.4 million in 2022 worldwide[16].



The difference between supply & demand for cyber security experts between 2021 & 2022 globally

Considering the substantial size of the cyber security workforce gap globally, it is important to encourage individuals to pursue a career in this field from an early stage. Engaging students and young people in cyber security can be challenging for many countries, including Qatar. Initiatives should be developed to show the benefits of cyber security careers in schools, as well as an opportunity to develop local talent and a high-skilled cyber security workforce in the country.

- ### Cyber security talent to be attracted and retained

The cyber security workforce gap globally and locally is accentuated by the failure of organizations to retain cyber security talents over a period of time. Countries around the world face challenges when it comes to both acquiring and retaining qualified cyber security professionals. International studies show that cyber security experts often leave their positions because of insufficient financial rewards, limited opportunities for growth and advancement, high work stress levels, and a lack of management backing. Initiatives that encourage continuing professional development within the cyber security career path, including incentives and promotional mechanisms, can be an opportunity to attract and retain the most skilled and talented cyber security professionals.

Human-related cyber risks to be addressed

Human behavior is often an underlying reason why cyber-attacks are successful. A limited understanding of cyber threats, insufficient training, and a lack of basic cyber security awareness can transform any user into a potential vulnerability. Most organizations identify human error as one of the most common causes of successful intrusions[17].

This is a challenge not just for Qatar but also for all countries. National and international efforts are needed to improve training and awareness at scale. Furthermore, initiatives can be targeted to specific segments of society and tailored to their needs. Raising awareness of cyber security risks represents an opportunity to reduce human errors in cyberspace.

More international collaboration to deal with global cyber risks

Unlike more traditional threats, cyberspace's interconnected nature and increased digitalization and globalization make cyber risks and threats less readily confined to national borders. Cyber-attacks often have an international impact, complicating government responses. Countries must work with the international community to ensure a safe cyberspace, develop global solutions, and ensure the safety of individuals.

Contributing internationally on cyber security issues – especially in multilateral countries such as the United Nations – requires relevant officials to be confident and skilled in cyber policy to promote the country's capabilities overseas, including developing partnerships with other cyber agencies.

Initiatives encouraging international partnerships and collaborations can strengthen a country's position in the global cyber landscape. Likewise, supporting the development of regional and international norms, focusing on using modern technologies for peaceful purposes, can also contribute to reinforcing a country's role on the global stage.

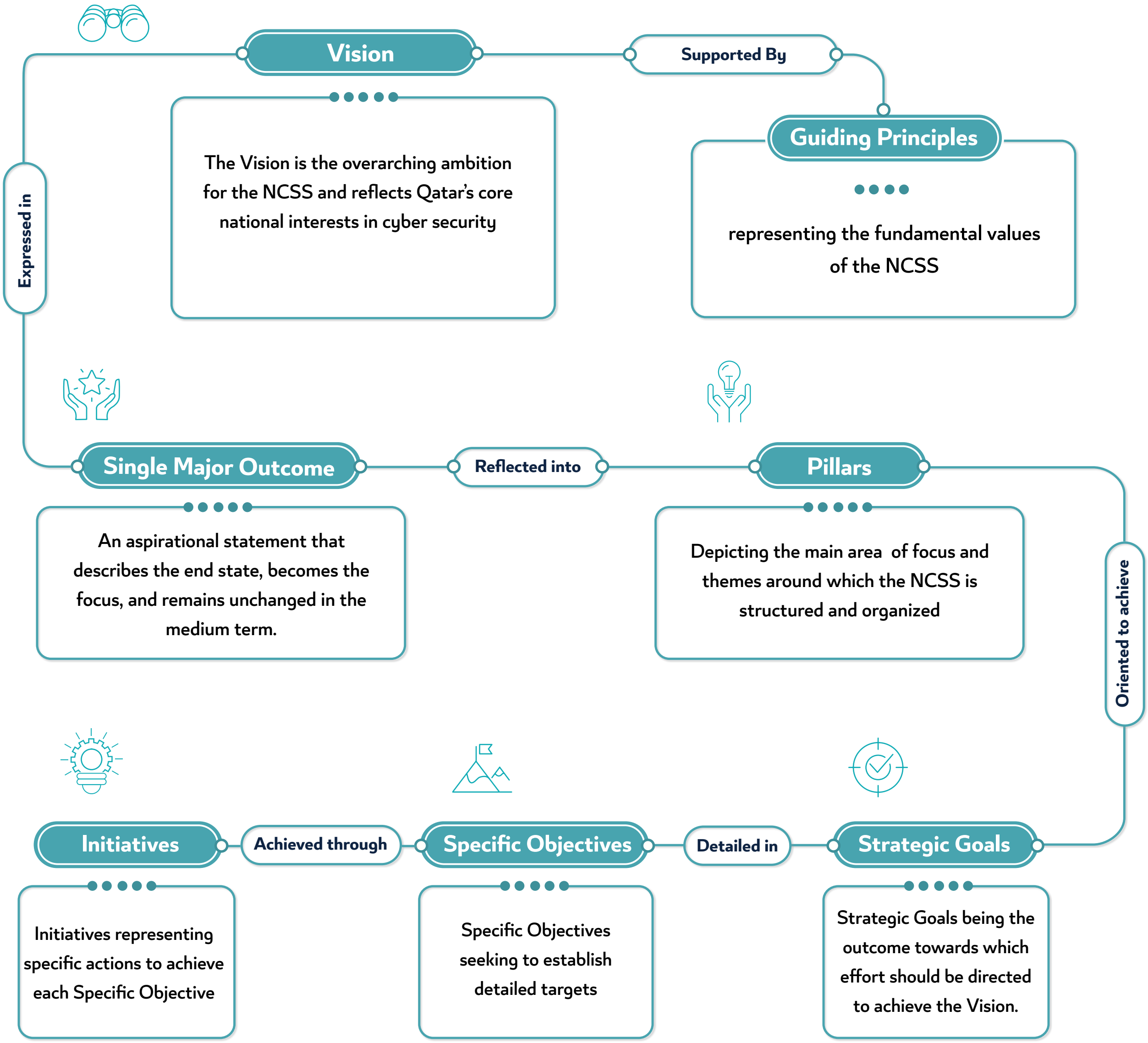
These challenges and opportunities will be addressed by the components of the NCSS (2024–2030) – particularly the Vision, Guiding Principles, Pillars, Strategic Goals, Specific Objectives and Initiatives. As described in the following sections.

02

THE CORE COMPONENTS **OF THE NCSS**

2. The core components of the NCSS

This NCSS is organized around six core components, which together set out the overall cyber security direction for the country:



Vision

The Vision is the overarching ambition for the NCSS and reflects Qatar's core national interests in cyber security

Supported By

Guiding Principles

representing the fundamental values of the NCSS

Expressed in

Single Major Outcome

An aspirational statement that describes the end state, becomes the focus, and remains unchanged in the medium term.

Reflected into

Pillars

Depicting the main area of focus and themes around which the NCSS is structured and organized

Oriented to achieve

Strategic Goals

Strategic Goals being the outcome towards which effort should be directed to achieve the Vision.

Detailed in

Specific Objectives

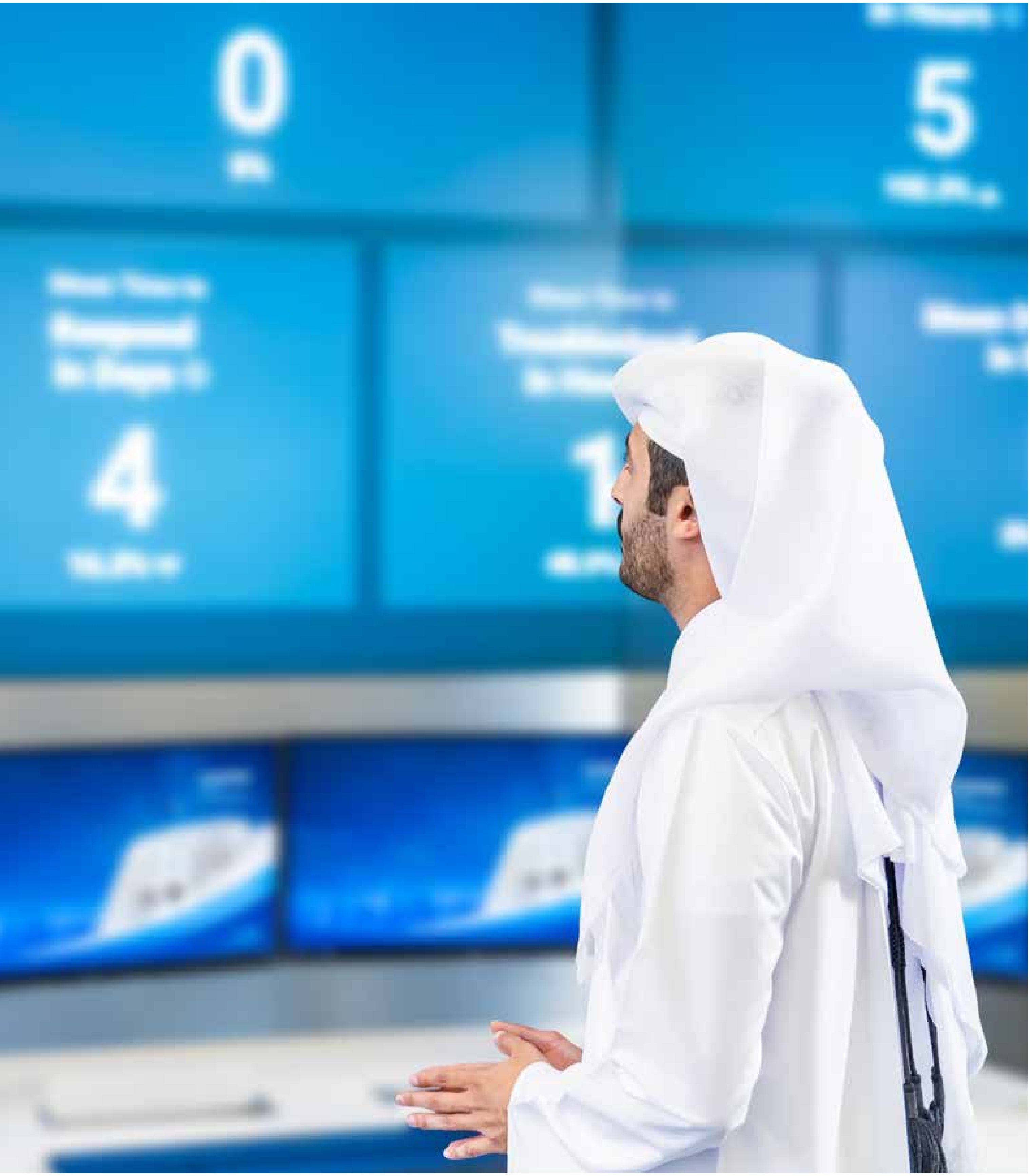
Specific Objectives seeking to establish detailed targets

Achieved through

Initiatives

Initiatives representing specific actions to achieve each Specific Objective

Figure 1 : NCSS 2024 - 2030: Core Components and Interrelations



2.1 - Vision & Single Major Outcome

The Vision of the Qatar NCSS 2024-2030 embraces the commitment to collaboration and cooperation across stakeholders, working for a common purpose: cyberspace that individuals and organizations can trust. Increased security and resilience are the key enablers for advancing the country's development and prosperity.

Vision

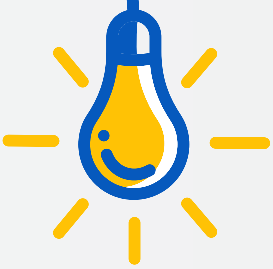
"Collaborative efforts to reinforce confidence in cyberspace for an advanced and prosperous Qatar"

Single Major Outcome: A Cyberspace of Robust security and resiliency for the state of Qatar

Figure 2 : NCSS Vision and Single Major Outcome

The Single Major Outcome

The Single Major Outcome for the Qatar NCSS 2024-2030 is an aspirational milestone that encapsulates the essence of the NCSS. An unwavering reference point guides Qatar towards a secure and resilient cyberspace. It represents a fundamental commitment to securing the digital domain for the benefit of individuals and organizations. As a stable and unchanging focus point, the Single Major Outcome ensures that every effort and initiative undertaken within the NCSS contributes to achieving the NCSS Vision. As mentioned above, a more secure and resilient cyberspace will strengthen the country's development and underpin its continued prosperity in the digital age by mitigating cyber-attacks that could cost billions.



2.2 - Guiding Principles

Six Guiding Principles have been identified, representing the NCSS's foundation. They steer and inform the NCSS's development and guide the stakeholders in implementing Initiatives. Suppose the Guiding Principles are followed and applied throughout the entire strategy's lifecycle (from development to implementation to monitoring). In that case, they will underpin the achievement of both the Strategic Goals and Vision.

Shared Responsibility

Encourage each actor in the cyber ecosystem to play an active role, take responsibility for their cyber security practices and contribute to enhancing cyber national capabilities.

Risk-based Approach

Reduce cyber risks to an acceptable level, whilst taking into account the specific context and objectives at stake.

Results-Oriented

Focus on effective and achievable goals that will deliver the NCSS Vision.

Individuals' Human Rights

Recognise the rights and responsibilities of individuals in the digital environment.

Economic Prosperity

Increase cyber security and resilience as a key safeguard that promotes economic prosperity and growth.

Coordination and Collaboration

Coordinate, join and align national efforts to improve national cyber security.

Figure 3: NCSS Guiding Principles

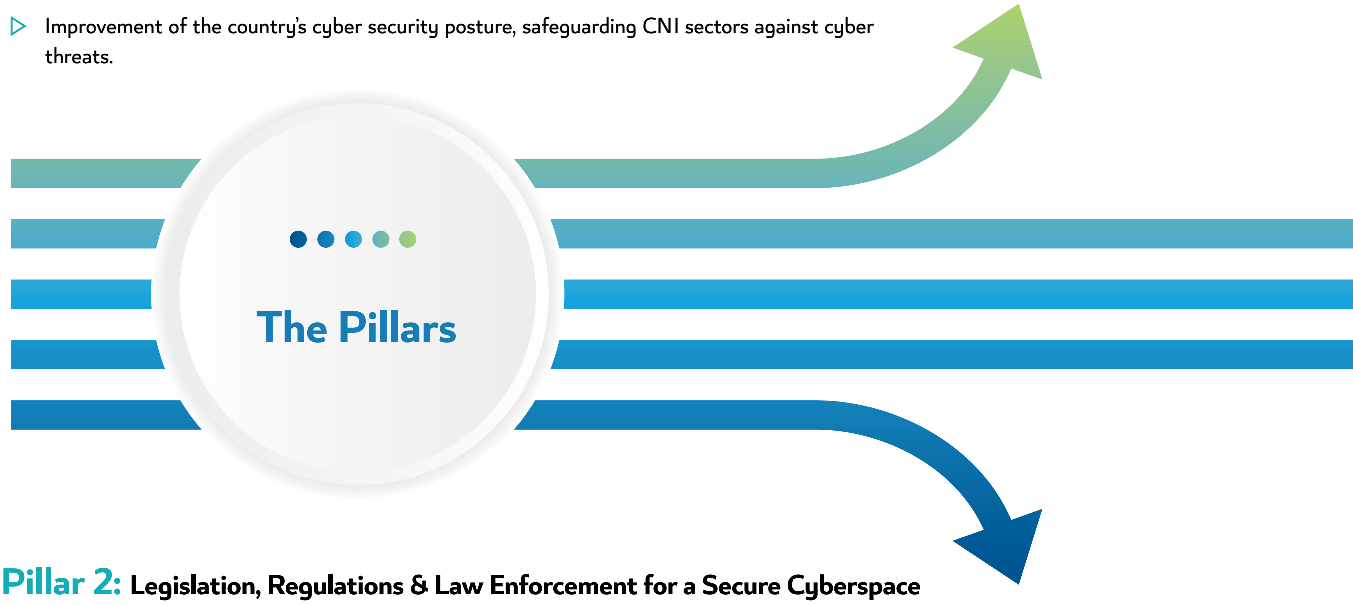
2.3 - Pillars, Strategic Goals, Specific Objectives

1. The Pillars of the NCSS and associated Strategic Goals

The identification of the NCSS Pillars was guided and informed by a set of drivers, which helped set the direction of Qatar's cyber security aspirations for the future. These drivers were identified based on growing global cyber security challenges, the country's critical cyber security achievements, and desired future outcomes, including overall national ambitions for transformation expressed by the Qatar National Vision 2030 and the six Guiding Principles at the heart of the NCSS.

Pillar 1: Cyber Security and Resilience in the Qatar Ecosystem

- Effective adoption of latest trends in cyber security, based on potential cyber risks identified at the national level, creating an ecosystem where each stakeholder plays a role in enhancing national cyber security capabilities.
- National coordination to increase the level of cyber security, resilience, and trust in the cyber environment.
- Empowerment of individuals and organisations to manage cyber risks, and feel protected and safeguarded in cyberspace.
- Improvement of the country's cyber security posture, safeguarding CNI sectors against cyber threats.



Pillar 2: Legislation, Regulations & Law Enforcement for a Secure Cyberspace

- Expansion of legislative and regulatory tools to keep pace with the cyber security challenges brought by the latest technologies.
- Regulation of cyberspace to protect individuals' rights and interests while enabling prosperity and growth.
- Enhancement of cybercrime investigation and prosecution capacity and capabilities, to promptly deal with new forms of cybercrime.

Pillar 3: A Thriving & Innovative Data-driven Economy

- Development of cyber security research and innovation capabilities, to contribute to diversifying Qatar's economy.
- Promotion of creativity and innovation for advanced technological developments.
- Development of a national cyber security industry.

Pillar 4: Cyber Culture & Workforce Talent Development

- Empowerment of a world-class educational system that equips individuals with adequate cyber security knowledge, skills and competencies.
- Development and retention of a highly skilled cyber security workforce.
- Promotion of a strong cyber security culture among individuals and organisations.

Pillar 5: International Cooperation and Trusted Partnerships

- Enhancement of regional and international cooperation to deal with global cyber risks.
- Enhancement of Qatar's role and contribution in the international cyber security arena.

Table 1: Drivers and Strategic Goal

Five Pillars are identified, representing the foundational building blocks upon which the NCSS is structured and organized. They consist of the core cyber security-related themes the NCSS will address to fulfill its Vision.

The purpose of the Pillars is to provide comprehensive coverage across all NCSS focus areas. Although each pillar addresses a specific area, the Pillars are interconnected and underpin each other. Progress in one Pillar provides a general cyber security foundation that supports the outcomes of the other Pillars and, when combined, fulfills the NCSS vision.

A strategic goal has been meticulously formulated for every pillar to ensure NCSS focus is well governed and properly maintained and to attain the desired outcomes of each pillar. These strategic goals are instrumental in delineating the direction of collective efforts toward realizing the intended results.

Pillars	Strategic Goals
Pillar 1: Cyber Security & Resilience in the Qatar Ecosystem	Strengthen the security and resilience of Qatar's cyber ecosystem, with an emphasis on the Critical National Infrastructure based on the evolving cyber risks, and national priorities.
Pillar 2: Legislation, Regulations, and Law Enforcement for a Secure Cyberspace	Promote the national legal and regulatory frameworks to empower a secure cyberspace with well-defined and established national cyber security governance and operating model.
Pillar 3: A Thriving & Innovative Data-driven Economy	Develop and enhance national cyber security capabilities by encouraging cyber security R&D and Innovation across public and private sectors, and encouraging investments for a thriving cyber industry.
Pillar 4: Cyber Culture & Workforce Talent Development	Boost a talented cyber security workforce, and endorse a cyber security culture across society.
Pillar 5: International Cooperation & Trusted Partnerships	Play an active role in international relations and cyber diplomacy, to promote cooperation at the regional and international levels for a secure, resilient, and peaceful cyberspace.

Figure 4: Pillars and associated Strategic Goals

2. Achieving the Strategic Goals through the Specific Objectives

Strategic Goals have been defined as the desired outcomes to which efforts are directed within each Pillar. Combined, they serve as the stepping stones towards realizing the NCSS vision. To ensure their attainability, each strategic goal is supported by defining specific objectives for each NCSS Pillar.

◇ PILLAR 1: Cyber Security and Resilience in the Qatar Ecosystem

Strategic Goal	Specific Objectives
Strengthen the security and resilience of Qatar's cyber ecosystem, with an emphasis on the Critical National Infrastructure based on the evolving cyber risks, and national priorities.	1. Advance the country's situational awareness of national cyber risks and threats, ensuring a protected and resilient cyberspace in Qatar.
	2. Strengthen the national and institutional technical capabilities in Qatar to protect, detect, respond to, and mitigate cyber threats in a timely manner.
	3. Manage national cyber crises effectively by coordinating with the right authorities at the national level, ensuring the prompt response and recovery from cyber crises and the continuity of critical services.
	4. Promote CNI resilience and continuity of critical services in coordination with sector regulators and Critical National Infrastructure operators.

Table 2: Pillar 1 Specific Objectives

PILLAR 2: Legislation, Regulations & Law Enforcement for a Secure Cyberspace

Strategic Goal

Promote the national legal and regulatory frameworks to empower a secure cyberspace with well-defined and established national cyber security governance and operating model.

Specific Objectives

1. Develop appropriate legal and regulatory frameworks, which take into account the changing threat landscape, and strike the right balance between security and innovation.
2. Develop regulations for the public and private sectors that drive security assurance, compliance, and participation with supervision mechanisms.
3. Continue to enhance the capacity and capability of national law enforcement authorities to investigate, prosecute, and combat all forms of cybercrime effectively.

Table 3: Pillar 2 Specific Objectives

PILLAR 3: A Thriving & Innovative Data-driven Economy

Strategic Goal

Develop and enhance national cyber security capabilities by encouraging cyber security R&D and Innovation across public and private sectors, and investments for a thriving cyber industry.

Specific Objectives

1. Drive a coordinated effort on cyber security R&D and innovation that is aligned with both market needs and national security priorities.
2. Promote sustainable investments so Qatar becomes a Cyber Security Innovation Hub, bringing highly innovative technologies, solutions and products to the cyber security market.
3. Encourage investments to sustain the development of a national cyber security industry and to contribute to the country's Gross Domestic Product (GDP).

Table 4: Pillar 3 Specific Objectives

PILLAR 4: Cyber Culture and Workforce Talent Development

Strategic Goal	Specific Objectives
Boost a talented cyber security workforce, and endorse a cyber security culture across society.	1. Align knowledge and skills taught in educational and training programmes with the cyber needs of both government and the private sector. 2. Empower individuals across society by providing relevant knowledge and skills to pursue a career in cyber security. 3. Nurture, motivate and engage potential talent to pursue a career in cyber security. 4. Attract and retain skilled professionals within the cyber security domain, to bridge the cyber security capacity gap within the country. 5. Enable individuals in Qatar to understand cyber security risks, and enhance their cyber culture, becoming capable of taking appropriate steps to protect their organisations and themselves.

Table5: Pillar 4 Specific Objectives

PILLAR 5: International Cooperation and Trusted Partnerships

Strategic Goal	Specific Objectives
Play an active role in international relations and cyber diplomacy, to promote cooperation at the regional and international levels for a secure, resilient, and peaceful cyberspace.	1. Create and reinforce trusted partnerships at the regional and international levels to drive collaboration, building mutual cyber capacity, capability, and understanding of shared threats. 2. Strengthen Qatar's cyber diplomacy capabilities to enhance Qatar's role in international and regional cyber discussions, events, and Initiatives. 3. Enhance Qatar's contribution to the global cyber security debate, with the intention of building a secure, peaceful, and stable international cyberspace that promotes the development of positive international cyber norms. 4. Enhance Qatar's outreach efforts at the international level to promote Qatar's cyber security profile.

Table6: Pillar 5 Specific Objectives

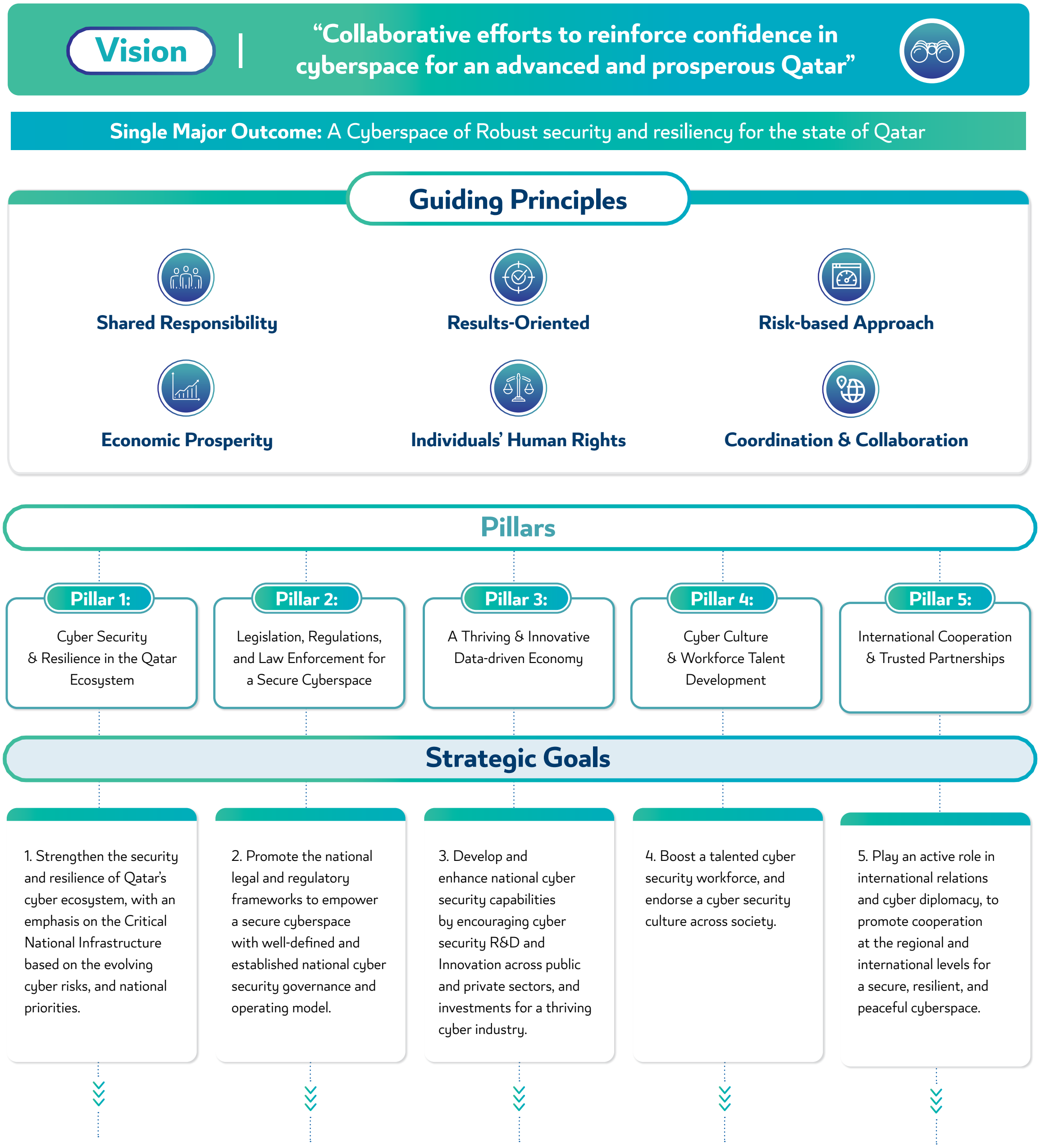
03

IMPLEMENTATION OF THE NCSS

3. Implementation of the NCSS 2030

The NCSS 2024-2030 will be effectively implemented through the collaborative efforts of different stakeholders. Their joint work will enable the implementation of Initiatives, which collectively will help accomplish the Specific Objectives of each Pillar. The combined results of the Specific Objectives will contribute to reaching the strategic goals and, finally, the NCSS Vision.

A set of initiatives has been identified for each specific objective to ensure the successful execution of the NCSS.



Vision | “Collaborative efforts to reinforce confidence in cyberspace for an advanced and prosperous Qatar”

Single Major Outcome: A Cyberspace of Robust security and resiliency for the state of Qatar

Guiding Principles

- **Shared Responsibility**
- **Results-Oriented**
- **Risk-based Approach**
- **Economic Prosperity**
- **Individuals’ Human Rights**
- **Coordination & Collaboration**

Pillars

Pillar 1:	**Pillar 2:**	**Pillar 3:**	**Pillar 4:**	**Pillar 5:**
Cyber Security & Resilience in the Qatar Ecosystem	Legislation, Regulations, and Law Enforcement for a Secure Cyberspace	A Thriving & Innovative Data-driven Economy	Cyber Culture & Workforce Talent Development	International Cooperation & Trusted Partnerships

Strategic Goals

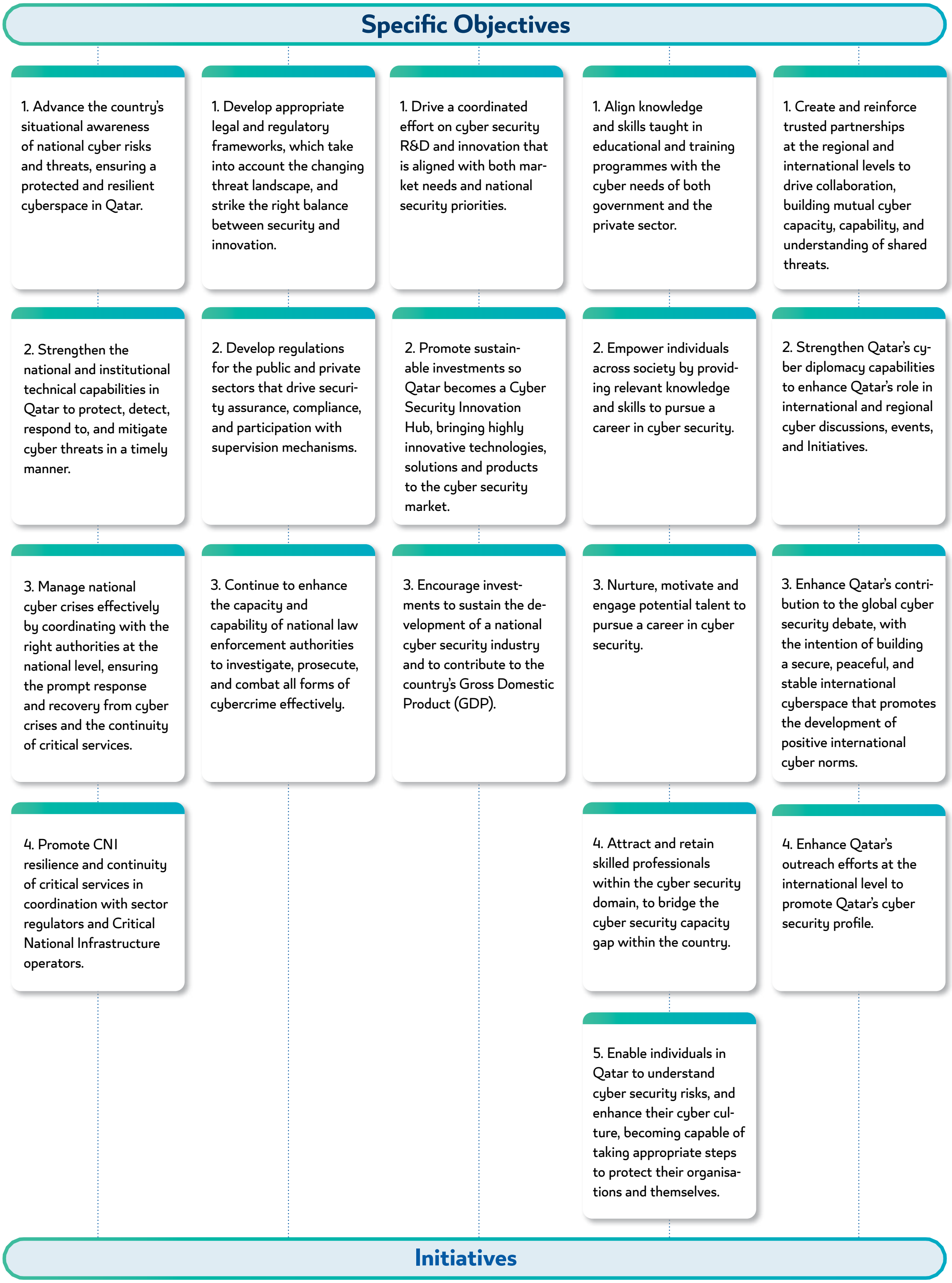
1. Strengthen the security and resilience of Qatar’s cyber ecosystem, with an emphasis on the Critical National Infrastructure based on the evolving cyber risks, and national priorities.

2. Promote the national legal and regulatory frameworks to empower a secure cyberspace with well-defined and established national cyber security governance and operating model.

3. Develop and enhance national cyber security capabilities by encouraging cyber security R&D and Innovation across public and private sectors, and investments for a thriving cyber industry.

4. Boost a talented cyber security workforce, and endorse a cyber security culture across society.

5. Play an active role in international relations and cyber diplomacy, to promote cooperation at the regional and international levels for a secure, resilient, and peaceful cyberspace.



Specific Objectives

1. Advance the country's situational awareness of national cyber risks and threats, ensuring a protected and resilient cyberspace in Qatar.

2. Strengthen the national and institutional technical capabilities in Qatar to protect, detect, respond to, and mitigate cyber threats in a timely manner.

3. Manage national cyber crises effectively by coordinating with the right authorities at the national level, ensuring the prompt response and recovery from cyber crises and the continuity of critical services.

4. Promote CNI resilience and continuity of critical services in coordination with sector regulators and Critical National Infrastructure operators.

1. Develop appropriate legal and regulatory frameworks, which take into account the changing threat landscape, and strike the right balance between security and innovation.

2. Develop regulations for the public and private sectors that drive security assurance, compliance, and participation with supervision mechanisms.

3. Continue to enhance the capacity and capability of national law enforcement authorities to investigate, prosecute, and combat all forms of cybercrime effectively.

1. Drive a coordinated effort on cyber security R&D and innovation that is aligned with both market needs and national security priorities.

2. Promote sustainable investments so Qatar becomes a Cyber Security Innovation Hub, bringing highly innovative technologies, solutions and products to the cyber security market.

3. Encourage investments to sustain the development of a national cyber security industry and to contribute to the country's Gross Domestic Product (GDP).

1. Align knowledge and skills taught in educational and training programmes with the cyber needs of both government and the private sector.

2. Empower individuals across society by providing relevant knowledge and skills to pursue a career in cyber security.

3. Nurture, motivate and engage potential talent to pursue a career in cyber security.

4. Attract and retain skilled professionals within the cyber security domain, to bridge the cyber security capacity gap within the country.

5. Enable individuals in Qatar to understand cyber security risks, and enhance their cyber culture, becoming capable of taking appropriate steps to protect their organisations and themselves.

1. Create and reinforce trusted partnerships at the regional and international levels to drive collaboration, building mutual cyber capacity, capability, and understanding of shared threats.

2. Strengthen Qatar's cyber diplomacy capabilities to enhance Qatar's role in international and regional cyber discussions, events, and Initiatives.

3. Enhance Qatar's contribution to the global cyber security debate, with the intention of building a secure, peaceful, and stable international cyberspace that promotes the development of positive international cyber norms.

4. Enhance Qatar's outreach efforts at the international level to promote Qatar's cyber security profile.

Initiatives

Figure 5 : Detailed overview of the components of the NCSS 2024-2030

3.1- Pillar 1 – Cyber Security and Resilience in the Qatar Ecosystem

Specific Objective 1

Advance the country's situational awareness of national cyber risks and threats, ensuring a protected and resilient cyberspace in Qatar.

Initiatives – Specific Objective 1

1.1.1 ▷ Enable a national cyber risk management approach to monitor, assess, and address cyber risks at the national level in coordination with public and private organizations.

1.1.2 ▷ Develop a tailored information-sharing framework, protocols, and secure channels for public and private organizations in Qatar, to share information on cyber threats, vulnerabilities, risks, and incidents.

1.1.3 ▷ Centralise cyber threat intelligence information accessible to public and private organizations in Qatar, to increase their situational awareness on key cyber risks, and capability to anticipate future cyber threats.

Specific Objective 2

Strengthen the national and institutional technical capabilities in Qatar to protect, detect, respond to, and mitigate cyber threats in a timely manner.

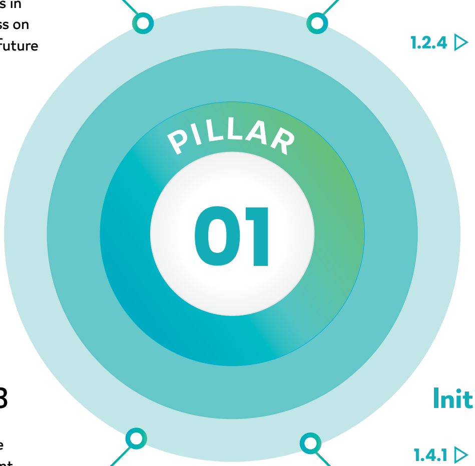
Initiatives – Specific Objective 2

1.2.1 ▷ Establish specific cyber security requirements for public and private organizations, considering their different sizes and nature, to effectively manage cyber risks and enhance their cyber incident management maturity.

1.2.2 ▷ Enable public and private organizations to assess and improve their cyber security maturity level.

1.2.3 ▷ Encourage public and private organizations to assess the financial impact of cyber risks and adopt cyber insurance to minimize the costs of cyber-related impact.

1.2.4 ▷ Support and facilitate the establishment of sector cyber security incident response teams (CSIRTs).



Initiatives – Specific Objective 3

1.3.1 ▷ Establish a centralised governance structure for national cyber security crisis management and disaster recovery, with clear roles and responsibilities defined for relevant national authorities with the participation of representatives from different sectors.

1.3.2 ▷ Develop and implement national cyber crisis management mechanisms, enabling effective crisis response through proper coordination among government authorities and other organizations.

1.3.3 ▷ Establish cyber security resilience simulation programs to continuously practice, exercise, and monitor the national cyber preparedness capabilities.

Specific Objective 3

Manage national cyber crises effectively by coordinating with the right authorities at the national level, ensuring the prompt response and recovery from cyber crises and the continuity of critical services.

Initiatives – Specific Objective 4

1.4.1 ▷ Define the requirements for the identification and classification of CNI and critical assets within each sector, in coordination with sector regulators and operators.

1.4.2 ▷ Develop, in coordination with sector regulators and operators, a specific cyber risk management framework, including third-party risk management and supply chain security, to enable CNI to evaluate cyber risks and take the appropriate mitigation actions.

1.4.3 ▷ Establish national cyber incident reporting mechanisms tailored to CNI, to coordinate cyber incident prevention, detection, and response capabilities.

1.4.4 ▷ Establish cyber threat intelligence-sharing mechanisms within and across CNI sectors to facilitate the exchange of information and strengthen situational awareness of cyber risks.

Specific Objective 4

Promote CNI resilience and continuity of critical services in coordination with sector regulators and Critical National Infrastructure operators.

3.2- Pillar 2 – Legislation, Regulations and Law Enforcement for a Secure Cyberspace

Specific Objective 1

Develop appropriate legal and regulatory frameworks, which take into account the changing threat landscape, and strike the right balance between security and innovation.

Initiatives – Specific Objective 1

2.1.1 ▷ Develop a comprehensive legal framework to secure the cyberspace that clearly establishes and empowers the different authorities involved in the national cyber security matters based on their roles and responsibilities.

2.1.2 ▷ Establish cyber security regulatory requirements for public and private sectors, aligned with international best practices, that enhance organizations' security without hindering innovation.

2.1.3 ▷ Develop legislation including clear requirements for identifying and classifying CNI sectors, the critical organizations and infrastructure within such sectors, as well as their required cyber maturity levels.

2.1.4 ▷ Develop cyber security regulatory frameworks for the latest emerging technology trends, and enhance existing technology-related frameworks to reinforce cyber security requirements.

2.1.5 ▷ Enhance the legal framework to ensure effective investigation and prosecution of cybercrimes in light of the evolving technology and cyber threat landscape.

Specific Objective 2

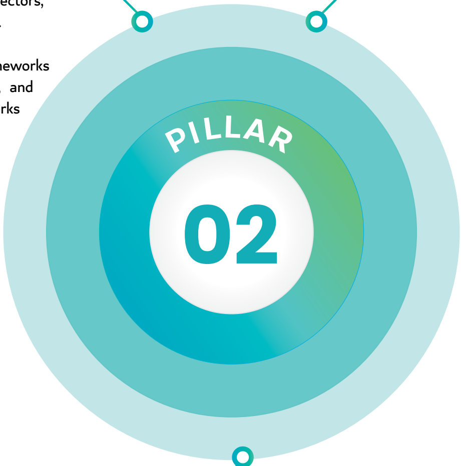
Develop regulations for the public and private sectors that drive security assurance, compliance, and participation with supervision mechanisms.

Initiatives – Specific Objective 2

2.2.1 ▷ Strengthen and enhance accreditation programs to ensure that provided services comply with relevant national requirements.

2.2.2 ▷ Improve and expand the existing certification programs to ensure that the technologies and products offered in the Qatari market meet an adequate level of cyber security.

2.2.3 ▷ Define specific cyber security requirements and programs for licensing cyber security service providers that are needed before entry into the country's cyber security market.



Initiatives – Specific Objective 3

2.3.1 ▷ Equip law enforcement authorities and judiciary with tools, skills, and knowledge to manage the full cycle of cybercrime cases.

Specific Objective 3

Continue to enhance the capacity and capability of national law enforcement authorities to investigate, prosecute, and combat all forms of cybercrime effectively.

3.3- Pillar 3 – A Thriving & Innovative Data-driven Economy

Specific Objective 1

Drive a coordinated effort on cyber security R&D and innovation that is aligned with both market needs and national security priorities.

Specific Objective 2

Promote sustainable investments so Qatar becomes a Cyber Security Innovation Hub, bringing highly innovative technologies, solutions and products to the cyber security market.

Initiatives – Specific Objective 1

3.1.1 ▷ Establish a governance structure at the national level to coordinate efforts among government, the private sector, and academia in R&D and innovation.

3.1.2 ▷ Develop a cohesive national cyber security innovation strategy, outlining key national priorities based on data-driven market analysis, in partnership with private sector and academia.

Initiatives – Specific Objective 2

3.2.1 ▷ Establish cyber security innovation incentive programmes to support contribution of organizations and people to bring new ideas to life, and the creation of a pool of researchers and professionals who invest in R&D as a source of innovation.

3.2.2 ▷ Build and expand cyber security development capability programmes to address cyber security emerging challenges and national priorities and reduce reliance solely on external capabilities and solutions.

Initiatives – Specific Objective 3

3.3.1 ▷ Support start-ups and companies in developing and offering innovative cyber security services and products.

3.3.2 ▷ Facilitate and support the creation of cyber security accelerators to support investments in cyber security projects by connecting potential investors with cyber security innovators.

Specific Objective 3

Encourage investments to sustain the development of a national cyber security industry and to contribute to the country's Gross Domestic Product (GDP).

3.4- Pillar 4 – Cyber Culture and Workforce Talent Development

Specific Objective 1

Align knowledge and skills taught in educational and training programmes with the cyber needs of both government and the private sector.

Initiatives – Specific Objective 1

4.1.1 ▷ Understand and identify the requirements for both the current and future cyber security workforce in terms of size, knowledge, skills and competencies as well as the potential challenges to the development of a highly skilled cyber security workforce.

4.1.2 ▷ Develop a national cyber security workforce reference that provides a common language and identifies the required knowledge, skills, and competencies for the different cyber security job roles in the public and private sectors.

Specific Objective 2

Empower individuals across society by providing relevant knowledge and skills to pursue a career in cyber security.

Initiatives – Specific Objective 2

4.2.1 ▷ Establish specific educational programmes in cyber security at all levels of education (primary, secondary, tertiary) to encourage individuals to pursue a career in cyber security.

4.2.2 ▷ Establish a national cyber security accreditation program for academic and professional degrees.

4.2.3 ▷ Coordinate efforts among universities and research centers to align and enhance the work of cyber security labs, complement students' theoretical knowledge with practical skills, and offer students the possibility of internships and apprenticeships.

4.2.4 ▷ Provide certified cyber security courses to upskill and empower industry professionals and practitioners with proper knowledge and skills.

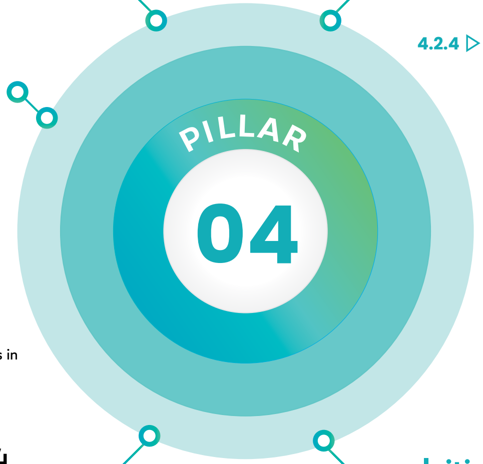
Specific Objective 3

Nurture, motivate and engage potential talent to pursue a career in cyber security.

Initiatives – Specific Objective 3

4.3.1 ▷ Develop programs to raise awareness about career opportunities in the cyber security field for students, parents, and guardians of students.

4.3.2 ▷ Promote and support cyber security studies in national scholarship programs.



Initiatives – Specific Objective 4

4.4.1 ▷ Understand and identify the challenges of attraction and retention in the cyber security workforce in Qatar, the results of which will be used to formulate and implement initiatives to enhance the cyber security workforce in Qatar.

4.4.2 ▷ Establish recognized cyber security positions in public and private organizations.

4.4.3 ▷ Develop career paths, including retention incentives, for cyber security professionals in the public and private sectors, to encourage long-term career development in the profession.

4.4.4 ▷ Encourage women's leadership in cyber security through the development of coaching and mentorship schemes.

Specific Objective 4

Promote CNI resilience and continuity of critical services in coordination with sector regulators and Critical National Infrastructure operators.

Initiatives – Specific Objective 5

4.5.1 ▷ Develop national cyber awareness programs for the general public, including children and the elderly, to promote cyber safety knowledge and skills.

4.5.2 ▷ Establish partnerships across government authorities and the private sector, to strengthen cyber security awareness among government staff and private sector employees.

4.5.3 ▷ Establish national programs to encourage embracing cyber ethics and cyber safety culture.

Specific Objective 5

Enable individuals in Qatar to understand cyber security risks, and enhance their cyber culture, becoming capable of taking appropriate steps to protect their organisations and themselves.

3.5- Pillar 5 – International Cooperation and Trusted Partnerships

Specific Objective 1

Create and reinforce trusted partnerships at the regional and international levels to drive collaboration, building mutual cyber capacity, capability, and understanding of shared threats.

Initiatives – Specific Objective 1

5.1.1 Develop international cyber partnerships to encourage cyber threat intelligence sharing.

5.1.2 Enhance existing bilateral and multilateral relations with countries and organizations, and build new regional and international partnerships to develop cyber security capability and capacity-building initiatives

5.1.3 Establish partnerships and cooperation mechanisms to counter transnational cyber threats, and identify, combat, and prosecute cybercrimes.

Specific Objective 2

Strengthen Qatar's cyber diplomacy capabilities to enhance Qatar's role in international and regional cyber discussions, events, and Initiatives.

Initiatives – Specific Objective 2

5.2.1 Enable diplomatic staff and other relevant officials to convey a common cyber security message in regional and international cyber security discussions, events, and forums that are aligned with Qatar's national interests.

5.2.2 Prepare diplomatic staff and other relevant officials to be active participants in selected regional and international cyber security discussions, events, and forums.

Initiatives – Specific Objective 3

5.3.1 Contribute to developing international law and cyber norms by actively participating in the United Nations (UN) and other regional and international processes.

5.3.2 Contribute to developing interoperable cyber security standards at the regional and international levels.

Specific Objective 3

Enhance Qatar's contribution to the global cyber security debate, with the intention of building a secure, peaceful, and stable international cyberspace that promotes the development of positive international cyber norms.

Initiatives – Specific Objective 4

5.4.1 Organise and host national and international cyber security events to promote Qatar's presence in the global cyber security landscape.

5.4.2 Support government authorities, the private sector, and academia in promoting their cyber-security-related initiatives to the international community.

Specific Objective 4

Enhance Qatar's outreach efforts at the international level to promote Qatar's cyber security profile.

04

IMPLEMENTATION, **MONITORING AND REVIEW**

4. Implementation, Monitoring and Review

Monitoring performance, especially alignment with the Qatar National Vision 2030, is critical to implement the NCSS successfully.

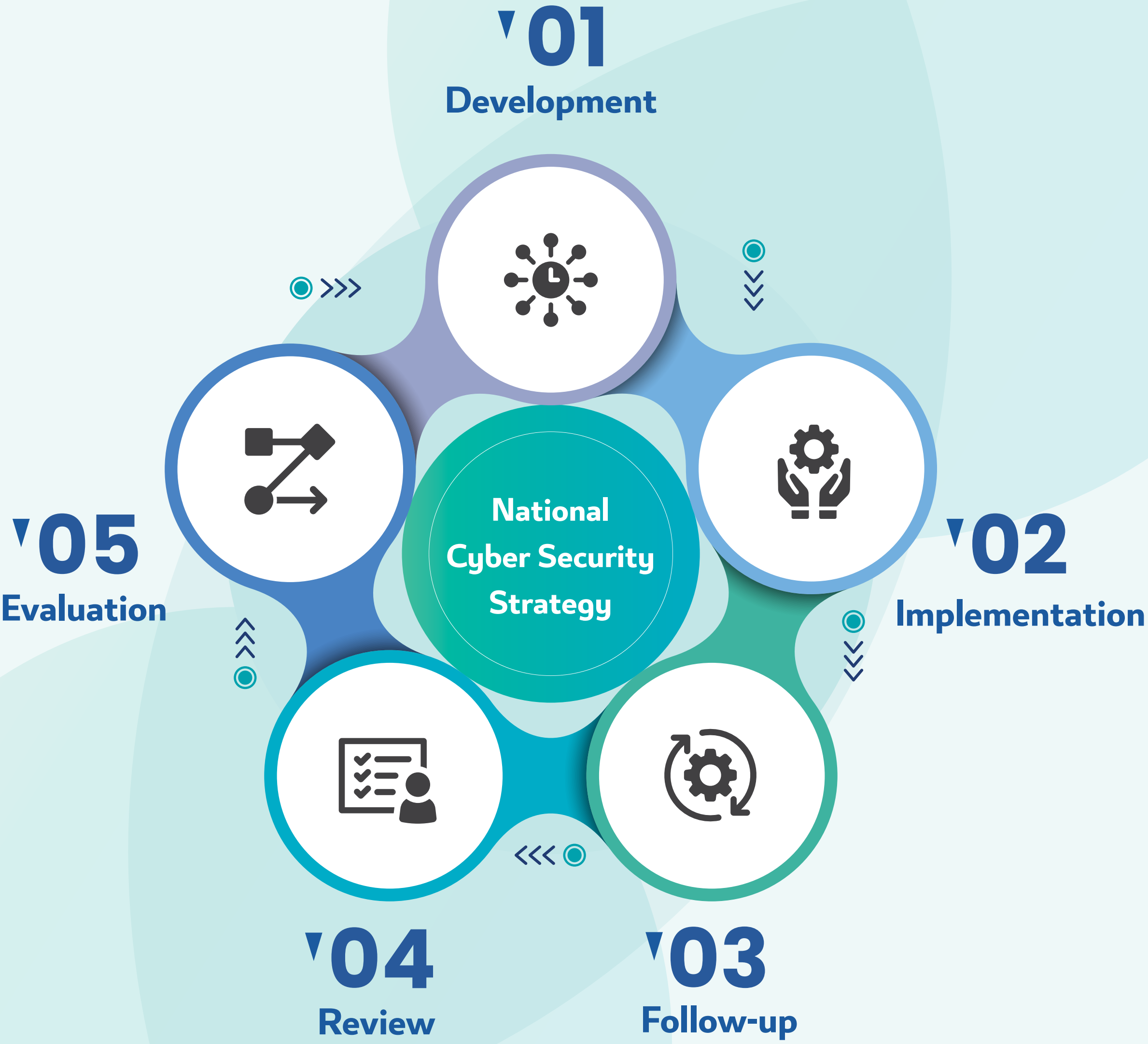
Through robust monitoring and review, NCSA will periodically assess the NCSS's activity and achievements with relevant stakeholders and evaluate whether the goals and metrics are still adequate. A set of KPIs will be used to track NCSS progress and measure the success of implementing Specific Objectives.

The Qatari cyber ecosystem will significantly benefit from this process. Monitoring and review will enable collecting information about the progress of Initiatives' implementation and contribute to impactful policymaking in cyber security. Additionally, the process will drive increased agility among stakeholders as they align with the progress made on their assigned initiatives.

The ability to adjust course when necessary ensures that implementation remains aligned with Qatar's needs. Given the rapid development of technologies and rising sophistication of cyber threats, periodic assessments of the cyber risk environment will be needed over the six years of the NCSS's life.

At the operational governance level, stakeholders responsible for implementing NCSS initiatives must monitor their progress and effectiveness. They should periodically report their results through a formal process to enable an overall understanding of how the NCSS is being implemented. When reported quickly and transparently, the results of monitoring and review activities can highlight deviations from the original implementation plan. Issues such as resources, timelines, and priority shifts can be promptly identified and addressed. This ensures that the fulfillment of Specific Objectives and Strategic Goals are not impacted.

Finally, Annual Reports will be prepared to describe the NCSS implementation status and lessons learned, providing a complete picture of how the NCSS is being implemented.


01
Development
02
Implementation
03
Follow-up
04
Review
05
Evaluation
National Cyber Security Strategy

05

CONCLUSION

5. Conclusion

The NCSS 2024–2030 encourages a collaborative effort to enhance the country's cyber resilience and capabilities for all stakeholders – from organisations to individuals – to address current and future cyber risks. "Shared responsibility" is key for the successful implementation of the NCSS, relying on strong collaboration and cooperation between the government, private sector, academia, and society.

The NCSS is a call to action. As such, it translates goals into concrete actions, to generate positive impacts on the current and future cyber security state. The NCSS was developed to be results-oriented, where its fundamental components – Strategic Goals, Specific Objectives, and Initiatives – are intertwined to support the overall Vision. To ensure the NCSS has a positive impact, monitoring will be a continuous activity throughout the entire NCSS lifecycle, and Annual Reports will be prepared to showcase progress.

Building on past national cyber security efforts whilst looking at the future, the NCSS empowers a resilient, trusted, and safe cyber environment. The NCSS helps achieve the goals of Qatar's National Vision 2030, contributing to the country's prominent position at the forefront of innovation, and securing a vibrant and prosperous future.

06

ANNEXES

06. Annexes

6.1 - ANNEX A: Glossary of key cyber security terms

Term	Definition
Critical Infrastructure	Physical assets, systems, or installations, which if disrupted, compromised, or destroyed, would have a serious impact on the health, safety, security, or economic well-being of Qatar or the effective functioning of the Qatari government.
Cyber crisis (or disruption)	An unplanned cyber event that causes assets to be inoperable for a length of time (e.g., minor, or extended power outage, extended unavailable network, or equipment or facility damage or destruction).
Cyber ecosystem	The aggregation and interactions of a variety of diverse participants (such as private firms, non profits, governments, individuals, and processes) and cyber devices (computers, software, and communications technologies).
Cyber event	A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation). An action marked, logged to a point in time that may require additional assessment.
Cyber incident	An adverse event that compromises Confidentiality, Integrity or Availability of an information asset, and has been verified as a potential threat.
Cyber resilience	Cyber resilience is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that include cyber resources.
Cyber risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the likelihood of occurrence of cyber events or incidents, and (ii) the adverse impacts that would arise if these events or incidents occur. A cyber risk could lead to financial loss, operational disruption, or damage from the failure of the digital technologies employed for informational and/or operational functions introduced to a manufacturing system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the manufacturing system.
Cyber security	The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: confidentiality, integrity (which may include authenticity and non-repudiation), and availability.

Term	Definition
Cyber threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.
Cyberattack	Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.
Cybercrime	Misconduct or crime committed using technology. Examples of cybercrime may include illegal access to systems or information, fraud, identity theft, or content-related offenses such as spam.
Cyberspace	A virtual or electronic environment that results from the interdependent network of information and communications technology (e.g., the Internet, telecommunications networks, computer systems, and embedded processors and controllers) that links people with services and information.
Emerging technologies	A set of promising technological innovations that have made a tangible impact on daily lives, although they are still in the early stages of development and application.
Incident response	The mitigation of violations of security policies and recommended practices.
Innovation	Innovation leverages research and development for the creation of products or services that can be new to an organization, market, or world. It can involve the development of new knowledge or technology, or adaptation of existing technology in novel ways to ultimately provide a positive economic and societal impact.
Threat intelligence	Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Table 7: Glossary of key cyber security terms

6.2 - ANNEX B: References

1 World Economic Forum. (2023, January 18). Global Cybersecurity Outlook 2023. Retrieved from: 06
https://www.weforum.org/reports/global-cybersecurity-outlook-2023

2 IBM. (2022). Cost of a data breach 2022. Retrieved from: 06
https://www.ibm.com/reports/data-breach

3 CrowdStrike. (2022). 2022 Global Threat Report 06
https://www.crowdstrike.com/global-threat-report/

4 National Cyber Security Agency. (n.d.) National Cyber Security Agency. Retrieved from: 07
https://ncsa.gov.qa/Retrieved February 2, 2023 from: https://ncsa.gov.qa/

5 Supreme Committee for Delivery & Legacy (2018). Qatar 2022 Cybersecurity Framework. Retrieved from: 07
https://www.qatar2022.qa/sites/default/files/Qatar2022Framework.pdf.

6 Trescon CyberSec. (2022, July 22). Spearheading The Security Infrastructure in Digitalized Qatar. World Cyber Security Summit. Retrieved from: 07
https://tresconglobal.com/conferences/cyber-sec/qatar/

7 Al Meezan. (2014, February 10). Cybercrime Prevention Law No. 14 of 2014. Al Meezan Qatar Legal Portal. Retrieved from: 07
https://www.almeezan.qa/LawPage.aspx?id=6366&language=ar

8 Al Meezan. (2016, December 29). Personal Data Privacy Protection Law No.13 of 2016. Al Meezan Qatar :Legal Portal. Retrieved from 07
https://www.almeezan.qa/LawPage.aspx?id=7121&language=ar

9 INTERPOL. (n.d.). Stadia activities. Retrieved from: 09
https://www.interpol.int/en/How-we-work/Project-Stadia/Stadia-activities

10 Trend Micro. (2022). The State of Industrial Cybersecurity. Retrieved from: 09
https://resources.trendmicro.com/IoT-survey-report.html

[11] World Economic Forum. (2023). Global Risks Report 2023. Retrieved from: https://www.weforum.org/reports/global-risks-report-2023 11

[12] World Economic Forum. (2023). Global Cybersecurity Outlook 2023. Retrieved from: https://www.weforum.org/reports/global-cybersecurity-outlook-2023 11

[13] Sophos. (2022). Sophos 2023 Threat Report- Maturing criminal marketplaces present new challenges to defenders. Retrieved from: https://www.sophos.com/en-us/content/security-threat-report 12

[14] World Economic Forum (2022). Organizations should make these 3 changes now to protect against the quantum computing threat. Retrieved from: https://www.weforum.org/agenda/2022/09/organizations-protect-quantum-computing-threat-cybersecurity/ 12

[15] World Economic Forum. (2023). Global Cybersecurity Outlook 2022. Retrieved from: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf 13

[16] (ISC)2 Cybersecurity Workforce Study. Retrieved from: https://www.isc2.org/Research/Workforce-Study?wpisrc=nl_cybersecurity202&wpmm=1 13

[17] World Economic Forum. (2023). Global Cybersecurity Outlook 2023. Retrieved from: https://www.weforum.org/reports/global-cybersecurity-outlook-2023 15