الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Kingdom of Saudi Arabia

National Cybersecurity Strategy

(Overview)

Sharing Notice: White
Document Classification: Open

December 2020

In the Name of Allah,
The Most Gracious,
The Most Merciful

“My first objective is for our Nation to be a successful and pioneering role model in the world at all fronts, and I will work with you to achieve it.”

The Custodian of the Two Holy Mosques

King Salman Bin Abdulaziz Al Saud

“We live in a time of scientific innovations and unprecedented technologies, and these technologies can bring huge benefits, and at the same time they may result in new challenges, such as changing work patterns… as well as increasing the risks of cybersecurity and information flow. This requires us to address these challenges as soon as possible to avoid them turning into economic and social crises.”

His Royal Highness

Mohammed Bin Salman Bin Abdulaziz Al Saud

Crown Prince, Deputy Prime Minister, Minister of Defense

Contents

Forward

The Kingdom holds a prominent global and regional position, which requires great efforts to protect and enhance it on all fronts. It serves the guests of the Two Holy Mosques, represents a major source of energy in the global markets, seeks to provide an attractive investment destination for local and foreign investments, and contributes to enhancing regional and global security.

The Kingdom will – with God's permission – proceed with leadership from the Custodian of the Two Holy Mosques King Salman Bin Abdulaziz Al Saud – may God grant him success – and His Royal Highness the Crown Prince Mohammed Bin Salman Bin Abdulaziz – may God protect him and care for him – and in accordance with the Kingdom's Vision 2030, towards enhancing its regional and international standing, and growing its economic power. It has also strived and will continue to strive to empower safety and security as it considers them the foundation for its structure, development, and prosperity to bring about a bright future.

The Kingdom's status renders it a target for actors looking to harm its security, economy, and development. As such, cyber attacks, which are increasing globally, has made cybersecurity a priority for all countries with the aim of strengthening their cyberspace and protecting themselves from various risks, threats, and geopolitical dimensions.

Nowadays, threats and cyber attacks have become more sophisticated and dangerous to countries, their systems, and their institutions through innovative and unforeseen methods that are expected to rise in the future as these actors, threat mechanisms, and threat technologies are quickly shared across the globe to help conduct attacks.

The Kingdom is aware of cyber threats and realizes that cybersecurity is a key pillar and objective in enhancing its position and protecting its vital interests, national security, critical infrastructure, key sectors, and government services and activities. As such, the Kingdom has reinforced its cybersecurity efforts and activities. One of the key outcomes was approving the establishment of the National Cybersecurity Authority (NCA), its regulations, and linking it directly to the King – God Bless Him – whereas it will oversee cybersecurity matters in the Kingdom and be the national reference for cybersecurity.

The NCA has been assigned important strategic objectives, of which the most prominent is developing the National Cybersecurity Strategy, overseeing its execution, and proposing amendments.

As such, the NCA has based this Strategy on a clear and specific vision aiming to achieve a secure and trusted Saudi cyberspace that enables growth and prosperity, endorsing the local economy, supporting businesses and other activities, providing opportunities for cybersecurity developments in the Kingdom, offering new jobs, building specialized capabilities, and providing incentives for research and development.

The Strategy aims to establish an integrated national cybersecurity organization that is aligned with the most distinguished international practices in the field; build a comprehensive approach that enables all stakeholders to improve their cybersecurity; protect their networks, systems, and electronic data; develop cybersecurity principles; and reinforce organization and individual awareness of their national responsibilities. As such, it will achieve a high level of cybersecurity maturity and professionalism as each stakeholder is responsible for their own cybersecurity standing as long as they are in alignment with the NCA and its mandate.

Supporting and funding this Strategy will be in alignment with the Kingdom's efforts in maintaining and enhancing safety and security. It will also help achieve its ambitious vision (Vision 2030) and preserve its developmental, social, and economic gains, thus improving the efforts of their national organizations in raising the level of cybersecurity. As result, the Kingdom was ranked 13th in the Global Cybersecurity Index (GCI) for 2018, which is managed by the International Telecommunication Union (ITU) of the United Nations.

As we realize that challenges are still substantial nowadays and overcoming them will require great efforts from both the NCA and national stakeholders, in addition to the high cost of cybersecurity and the even higher cost of cyber incidents – God Forbid – we hope that this National Cybersecurity Strategy and its frameworks will be implemented to reduce risks, increase trust, and enable growth.

May God Grant Us Success.

Dr. Musaed Bin Mohammed Al-Aiban
Chairman of the Board of Directors of the National Cybersecurity Authority

Executive Summary

Executive Summary

An integrated and secure national digital infrastructure is one of the most important drivers of growth and prosperity in the Kingdom of Saudi Arabia. However, the rapid expansion of technology usage has introduced new Cybersecurity vulnerabilities and cyber threats. These evolving threats necessitate strengthening the Kingdom's overall cybersecurity posture so that networks, information technology, operational technology systems, and related hardware and software components are secured, thus protecting services and data from penetration, disruption, modification, entry, use, or exploitation. By doing so, the critical technical linkages between government services and critical national infrastructure are secured and growth of the Kingdom's digital economy is supported.

The National Cybersecurity Authority (NCA) prepared the Kingdom's first National Cybersecurity Strategy to guide implementation of key initiatives as specified by Royal Decree No. 6801 to achieve an appropriate balance between enhancing cybersecurity, raising confidence, and contributing to the Kingdom's growth and prosperity.

This Executive Summary provides key insight into the methodology employed to develop the Strategy, its vision and national strategic goals, national organization roles and responsibilities, national cybersecurity frameworks, and the action plan.

The Comprehensive methodology used to prepare the Strategy consisted of the following:

- Referencing and aligning with key national resources, foremost of which is the Kingdom's Vision 2030, in addition to relevant national regulations including the regulations of the NCA
- Studying the most pervasive local, national, and international cyber risks
- Designing a comprehensive reference framework, based on international best practices and recent developments in the cybersecurity domain, to build the Strategy – inclusive of all aspects of cyber defense operations, capacity building, organization design and policy, and others
- Cybersecurity Benchmark: Benchmarking cybersecurity best practices and lessons learned across 20 countries, especially those with developed national cybersecurity capabilities
- Analyzing the current cybersecurity threat landscape in the Kingdom
- Formulating the Strategy's vision and core elements

The Strategy's vision, which balances the Kingdom's aspiration to provide both security and facilitate growth, is as follows:

> A resilient, secure, and trusted Saudi cyberspace that enables growth and prosperity

Through this Strategy, NCA establised an integrated cybersecurity framework in the Kingdom focusing on six areas: Unify, Manage, Assure, Defend, Partner, and Build. These areas are described as follows:

Unify

Whole-of-Nation Cybersecurity Governance

Manage

Adaptive Cyber Risk Management on National Level

Assure

Cyber Ecosystem Assurance

Defend

Strengthening national technical defense capabilities against cyber threats (Dynamic Defense)

Partner

Strengthening Partnerships and Cooperation in Cybersecurity (Collaborative Security)

Build

National Capacity Building and Cybersecurity Industry Development (Cyber Ecosystem Development)

The roles and responsibilities of organizations in the national cyber ecosystem include the NCA, military and security organizations, civil government organizations, private sector organizations, the national community, and the international community.

Four national cybersecurity frameworks were built to augment the Strategy and provide an essential foundation needed to achieve the national strategic goals. These are as follows:

National Cybersecurity Risk Management Framework

National Cybersecurity Incident Response Framework

National Cybersecurity Information Sharing Framework

National Cybersecurity Capability Building Framework

The Strategy will be implemented over a five-year period and is sequenced along three tracks consisting of 14 initiatives and 70 discrete projects. The three implementation tracks are as follows:

Track #1: High-Return Projects

Launching urgent specific projects that have a tangible impact in raising the cybersecurity maturity of the Kingdom.

Track #2: Cybersecurity Catalyst Program

Providing basic cybersecurity services to national organizations that raise the overall level of cybersecurity in the Kingdom.

Track #3: National Initiatives

Implementing a set of five-year national initiatives and projects with long-term strategic impacts.

A set of key performance indicators (KPI) has been identified and constructed to measure progress against each of the national strategic goal areas (Unify, Manage, Assure, Defend, Partner, and Build) of the Strategy. The KPIs will be measured through a defined set of sub-indicators.

To establish A resilient, secure, and trusted Saudi cyberspace that enables growth and prosperity, this Strategy will be implemented in collaboration with stakeholders across the Kingdom as well as under the relevant national authorities and with the leadership of the NCA.

01

> “The strategy aims to direct national efforts into reinforcing the security of the Kingdom’s cyberspace”

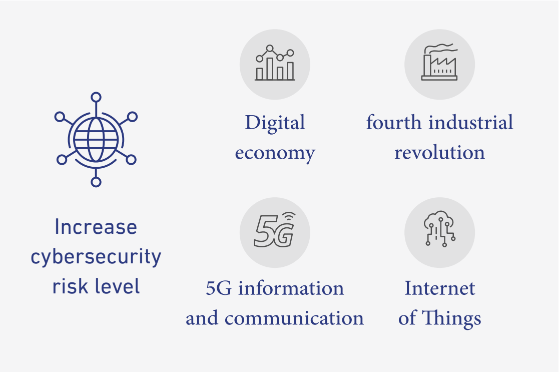
Introduction

Introduction

Cybersecurity is a critical national priority; it is vital to protecting the Kingdom's economy and securing digital services and infrastructure. It is one of the main pillars needed to enable Vision 2030, considering growth in the Kingdom regarding the provision of digital services and spreading the use of technology. The Strategy aims to:

- Direct national efforts into reinforcing the security of the Kingdom's cyberspace by following secure practices needed to address new technology.
- Protect national entities and critical national infrastructure information, data, and systems.
- Build a capable cyber workforce.
- Support and enable national organizations.
- Facilitate private sector investment
- Create an environment that fosters cybersecurity innovation.

The Strategy considers the current cybersecurity environment and context and is informed by international data, events, variables, and trends as well the current shift towards a digital economy, the launch of the fourth industrial revolution, and the imminent arrival of 5G information and communications technology services. The impact of the growing emerging technologies, such as Internet-of-Things (IoT), has resulted in an expanded attack surface and increased risk levels. In the past, the impact of cyber attacks was often limited to data; however, today their impact on both society and the economy is far greater.



Increase cybersecurity risk level

Digital economy

fourth industrial revolution

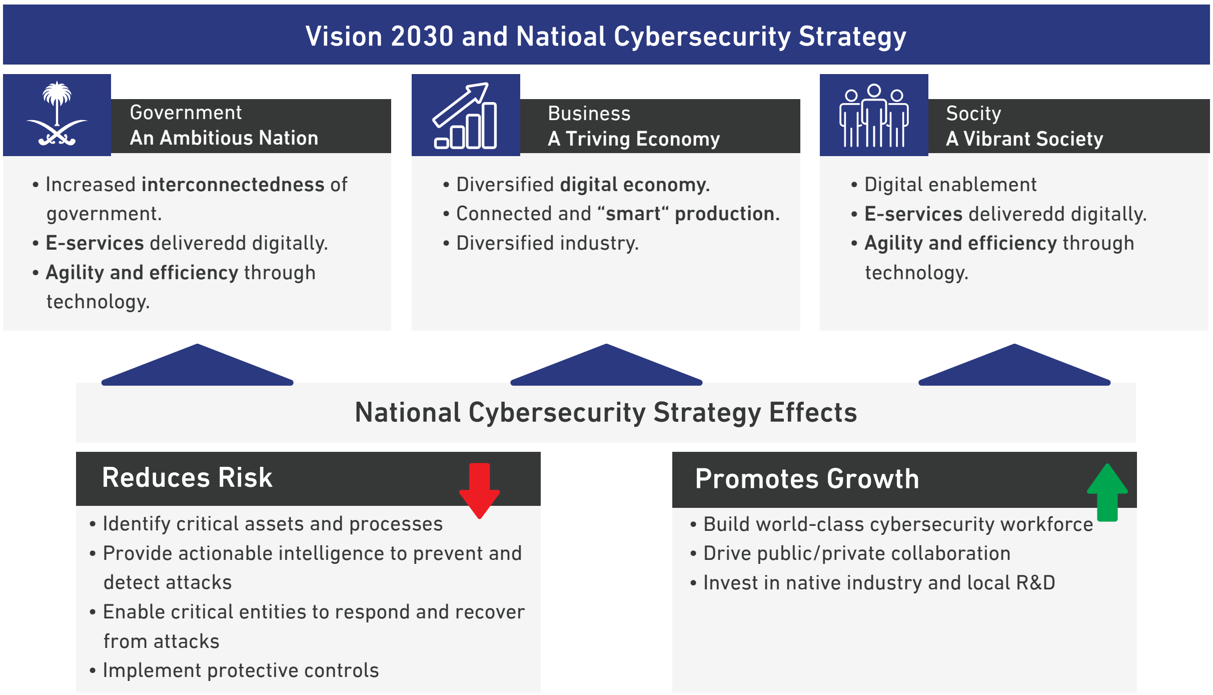
5G information and communication

Internet of Things

Technical systems and infrastructure across countries are exposed to cyber risks. As such, the cost of cyber attacks will continue to grow at both the national and global level. This incentivizes countries to invest more resources to manage these risks. At the same time countries should capitalize upon opportunities to develop their digital infrastructure and foster economic prosperity.

Thus, it is vital to implement and activate this Strategy to manage the Kingdom's cyberspace in an integrated fashion. The Strategy's vision, key principles, and national strategic goals will direct all cybersecurity activities in the Kingdom. It is expected that national organizations and the private sector will align their cybersecurity priorities with those of the Strategy. The NCA will facilitate interpretation of this Strategy, roles and responsibilities, and relevant frameworks where policies, governance mechanisms, standards, controls, guidelines, and indexes are drawn and implemented.

This Strategy was built using a methodology, aligned to the Kingdom's Vision 2030, inclusive of its themes, goals, programs, and frameworks. The alignment between the Kingdom›s Vision 2030 and the Strategy is as follows:



Vision 2030 and Natioal Cybersecurity Strategy

Government
An Ambitious Nation

- Increased **interconnectedness** of government.
- **E-services** deliveredd digitally.
- **Agility and efficiency** through technology.

Business
A Triving Economy

- Diversified **digital economy.**
- Connected and "**smart**" **production.**
- Diversified industry.

Socity
A Vibrant Society

- Digital enablement
- **E-services** deliveredd digitally.
- **Agility and efficiency** through technology.

National Cybersecurity Strategy Effects

Reduces Risk

- Identify critical assets and processes
- Provide actionable intelligence to prevent and detect attacks
- Enable critical entities to respond and recover from attacks
- Implement protective controls

Promotes Growth

- Build world-class cybersecurity workforce
- Drive public/private collaboration
- Invest in native industry and local R&D

Figure (1): Vision 2030 and the National Cybersecurity Strategy

The elements of the Strategy have been identified and include the basic principles of development and the Strategy's vision and national strategic goals. The Strategy highlights the related national cybersecurity frameworks needed to operationalize the Strategy. It also provides an overview of roles and responsibilities for national organizations, including the action plan consisting of its implementation tracks, initiatives, projects, and KPIs.

NCA will lead national efforts through this Strategy and work on improving the engagement, participation, and integration of national entities to achieve a secure and trusted Saudi cyberspace that enables growth and prosperity .

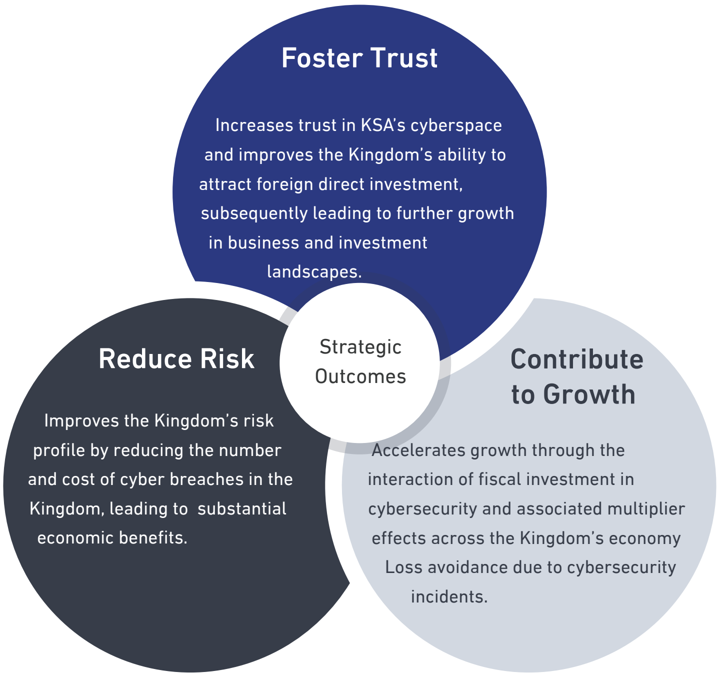

Foster Trust
Increases trust in KSA's cyberspace and improves the Kingdom's ability to attract foreign direct investment, subsequently leading to further growth in business and investment landscapes.
Strategic Outcomes
Reduce Risk
Improves the Kingdom's risk profile by reducing the number and cost of cyber breaches in the Kingdom, leading to substantial economic benefits.
Contribute to Growth
Accelerates growth through the interaction of fiscal investment in cybersecurity and associated multiplier effects across the Kingdom's economy Loss avoidance due to cybersecurity incidents.

Figure (2): Strategic Outcomes

02

National Cybersecurity Strategy Methodology

National Cybersecurity Strategy Methodology

The Strategy was established using a comprehensive approach consisting of six stages. It included analyzing the most critical global and national cybersecurity risks and a comprehensive reference framework covering the core domain areas of cybersecurity. The Kingdom's cybersecurity current state was examined in detail. The best global cybersecurity practices, expertise, and technologies were considered, compared to the Kingdom's specific needs, and integrated into the Strategy – including the vision and national strategic goals that all national organizations must aim to achieve as specified by their assigned cybersecurity roles and responsibilities and under the leadership of the NCA. The six steps leveraged to develop the Strategy are as follows:

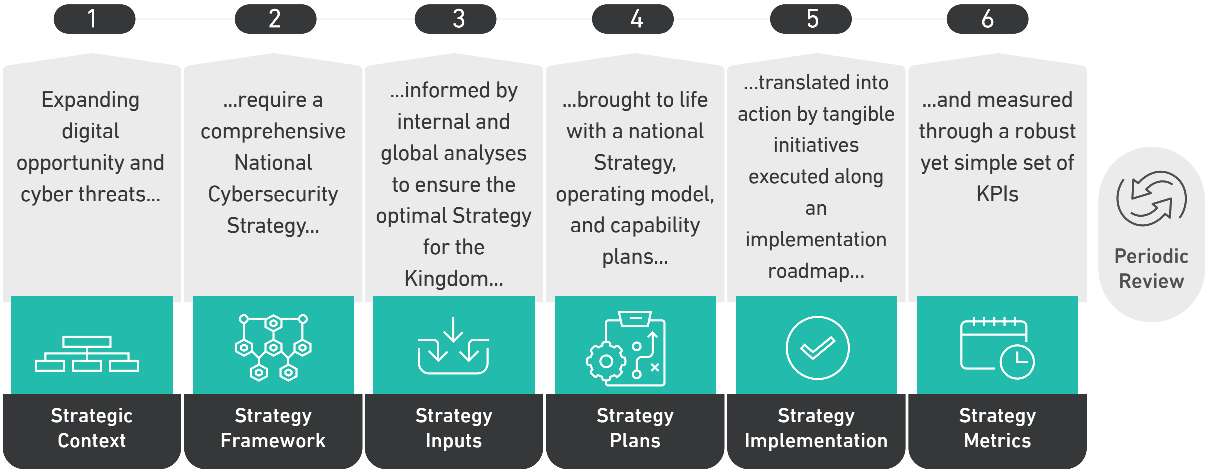

1
Expanding digital opportunity and cyber threats...
Strategic Context
2
...require a comprehensive National Cybersecurity Strategy...
Strategy Framework
3
...informed by internal and global analyses to ensure the optimal Strategy for the Kingdom...
Strategy Inputs
4
...brought to life with a national Strategy, operating model, and capability plans...
Strategy Plans
5
...translated into action by tangible initiatives executed along an implementation roadmap...
Strategy Implementation
6
...and measured through a robust yet simple set of KPIs
Strategy Metrics
Periodic Review

Figure (3): National Cybersecurity Strategy Development

2.1 Strategy Reference Model

In order to set a practical model for the different domains of cybersecurity, A reference model for the Kingdom was developed based on national and international best practices and the most recent, relevant cybersecurity challenges the Kingdom faces today. This model establishes a structure to examine the most important cybersecurity areas at the national level.

The model consists of six dimensions and 18 main cybersecurity elements. The model was used in a current state study of the Kingdom's cybersecurity. In addition, the model guided benchmarks of 20 nations, including countries with mature cybersecurity capabilities, which helped inform development the Strategy's vision, national strategic goals, initiatives, and projects.

The reference model used to develop the Strategy is as follows:

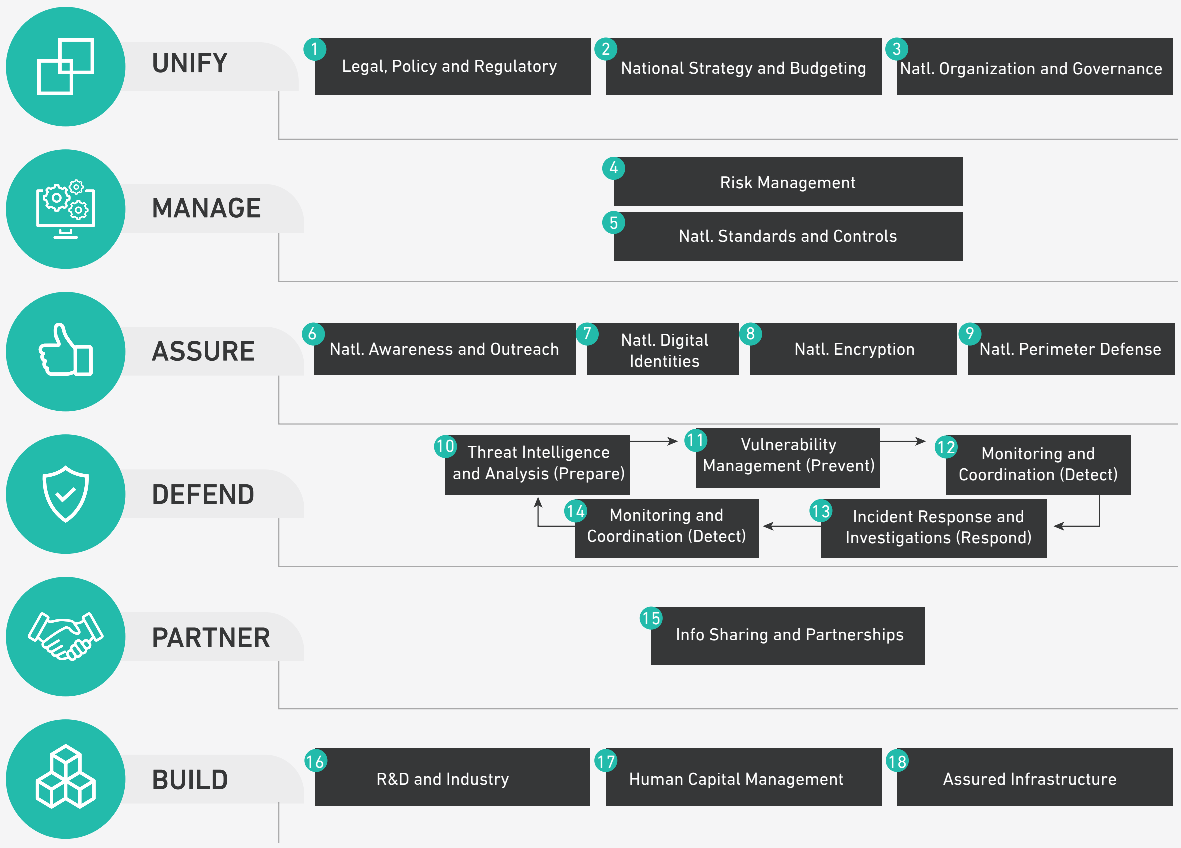

UNIFY
1 Legal, Policy and Regulatory
2 National Strategy and Budgeting
3 Natl. Organization and Governance
MANAGE
4 Risk Management
5 Natl. Standards and Controls
ASSURE
6 Natl. Awareness and Outreach
7 Natl. Digital Identities
8 Natl. Encryption
9 Natl. Perimeter Defense
DEFEND
10 Threat Intelligence and Analysis (Prepare)
11 Vulnerability Management (Prevent)
12 Monitoring and Coordination (Detect)
13 Incident Response and Investigations (Respond)
14 Monitoring and Coordination (Detect)
PARTNER
15 Info Sharing and Partnerships
BUILD
16 R&D and Industry
17 Human Capital Management
18 Assured Infrastructure

Figure (4): Strategy Reference Model

03

Strategy Elements

Strategy Elements

The Strategy was developed and includes its main elements, the elements are, key principles, vision, national strategic goals and key performance indicator.

3.1 Key Principles

The current state analyses and the international benchmark study shows an important of seven key principles for developing the Strategy, these principles are:

Whole-of-Nation Alignment

Centralized Governance, Decentralized Operations

Agile and Future-Focused

Prioritization Based on Risk Level

Cooperation and support

Relying on Saudi Nationals and Investment Opportunities

Setting benchmarks and performance indicators

- **"Whole-of-Nation Alignment"**

The integration and coordination of efforts across the government sector and the private sector, and centralized policies and organizations. With shared responsibilities.

- **"Centralized Governance, Decentralized Operations"**

Setting roles and responsibilities at the national level, which contributes to clarity and speed of implementation.

- **"Agile and Future-Focused"**

Flexibility and rapidly deploy and iterate capabilities in cyberspace, and effective interaction with technical developments, and harness emerging technologies to reduce renewable threats.

- **"Prioritization Based on Risk Level"**

Aligning resources and capabilities according to the risk level and continuously reassessing risks, ensure the optimal use of available resources.

- **"Cooperation and support"**

Share information and lessons learned with national and international partners.

- **“Relying on Saudi Nationals and Investment Opportunities”**

Investing in national talent, fostering innovation, developing the national industry, and attracting international investments, enhance the economic impact of the Kingdom.

- **“Setting benchmarks and performance indicators”**

Measuring performance to ensure the achievement of the objectives and to address the difficulties.

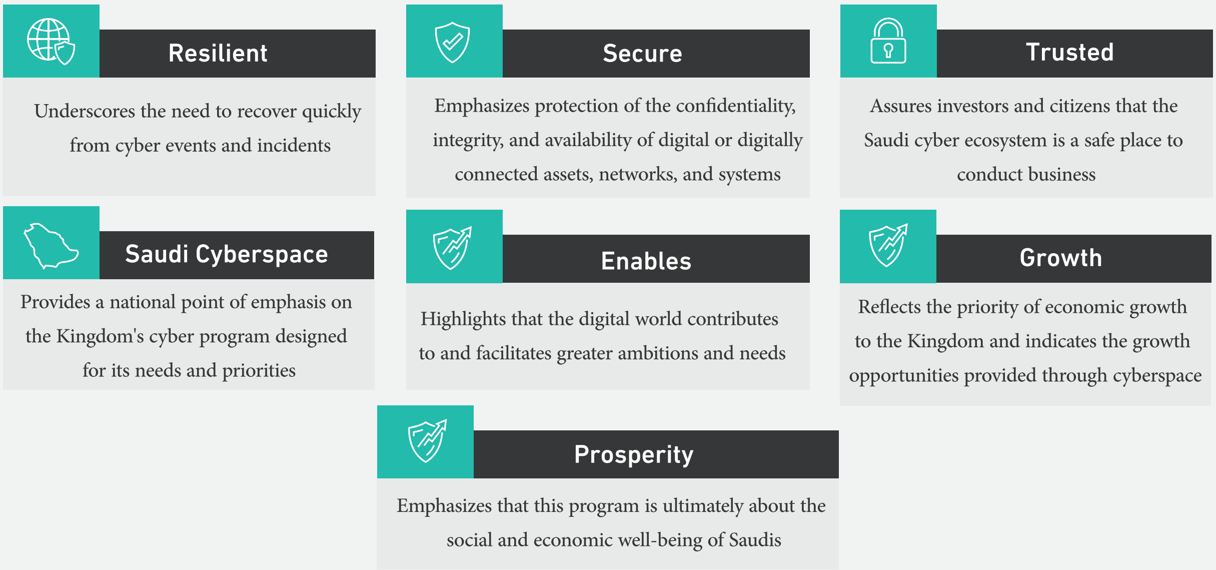
3.2 Vision

The vision was formulated to reflect the ambitious Strategy in the Kingdom, which achieves a balance between enhancing cybersecurity, raising confidence, and contributing to the Kingdom’s growth and prosperity.

The vision meets the Kingdom’s needs, priorities, and expectations, and emphasizes the protection of technical and operational systems and critical infrastructure. Additionally, it reinforces the confidence of national organizations, investors, and individuals in the Kingdom, and enables economic and social growth in the Kingdom. The vision is as follows:

“A resilient, secure, and trusted Saudi cyberspace that enables growth and prosperity”

This vision is applicable across all the Kingdom's cyberspace. It meets the Kingdom's needs, priorities, and aspirations, and emphasizes protection of technical and operational systems and sensitive infrastructure in addition to the ability to withstand and respond to cyber incidents, absorb damage, and recover in a timely manner. The vision is comprised of five components as follows:



Resilient
Underscores the need to recover quickly from cyber events and incidents

Secure
Emphasizes protection of the confidentiality, integrity, and availability of digital or digitally connected assets, networks, and systems

Trusted
Assures investors and citizens that the Saudi cyber ecosystem is a safe place to conduct business

Saudi Cyberspace
Provides a national point of emphasis on the Kingdom's cyber program designed for its needs and priorities

Enables
Highlights that the digital world contributes to and facilitates greater ambitions and needs

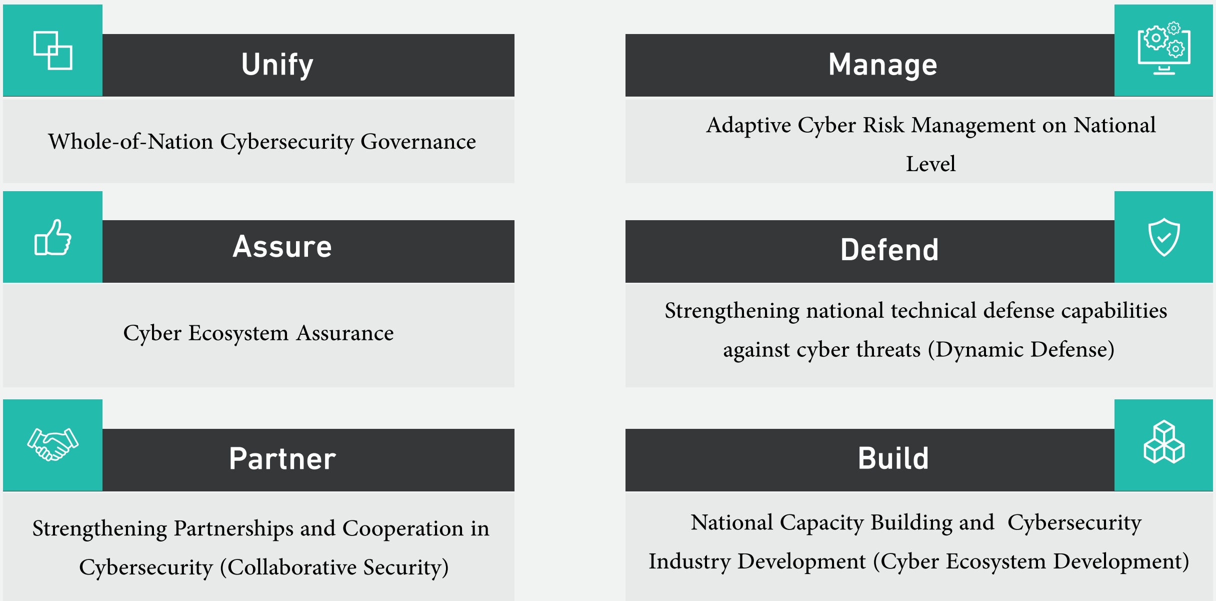
Growth
Reflects the priority of economic growth to the Kingdom and indicates the growth opportunities provided through cyberspace

Prosperity
Emphasizes that this program is ultimately about the social and economic well-being of Saudis

Figure (5): Vision

3.3 Strategic Goals

To achieve the Kingdom's vision of "A resilient, secure, and trusted Saudi cyberspace that enables growth and prosperity" six national strategic goals must be achieved as part of the Strategy. The national strategic goals are detailed as follows:



Unify
Whole-of-Nation Cybersecurity Governance

Manage
Adaptive Cyber Risk Management on National Level

Assure
Cyber Ecosystem Assurance

Defend
Strengthening national technical defense capabilities against cyber threats (Dynamic Defense)

Partner
Strengthening Partnerships and Cooperation in Cybersecurity (Collaborative Security)

Build
National Capacity Building and Cybersecurity Industry Development (Cyber Ecosystem Development)

Figure (6): Strategic Goals

1. Unify: Whole-of-Nation Cybersecurity

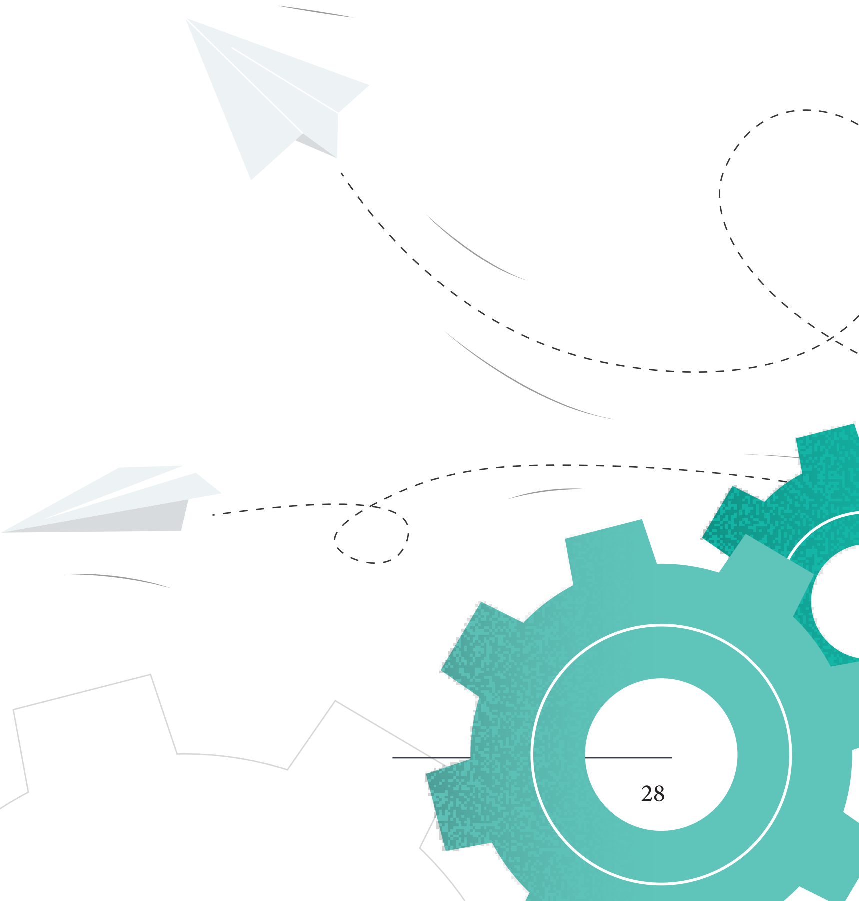
In order to ensure the achievement of high degrees of coordination and alignment; a comprehensive national cybersecurity governance approach must be adopted that defines roles and responsibilities of organizations as well as their integration to develop and execute regulations and policies, and monitoring compliance according to national standards across all cybersecurity domain areas. In addition to having unified mechanisms for planning and budgeting, and effectively prioritizing cybersecurity; which promotes higher Spending efficiency.

2. Manage: Adaptive Risk Management

Effectively managing cyber risks at the organization, sector, and national levels, and ascertaining damage in the cyber domain, the level of impact, and the best methods to mitigate the damage. In addition to defining protection and defense measures according to the level of risk.

3. Assure: Cyber Ecosystem Assurance

Setting comprehensive controls, national standards, and a compliance monitoring system that protects the cybersecurity ecosystem, raising the communities' level of cybersecurity awareness and continuing to communicate and engage through public outreach awareness programs for organizations, individuals, and destinations. To achieve maturity and application of cybersecurity controls at the organization, sector, and national levels.



4. Defend: Dynamic Defense

Continual development and enhancement of national capabilities to defend against cyber threats through identification of cyber threats and attacks in addition to response, recovery, and remediation resulting from cyber attacks.

5. Partner: Collaborative Security

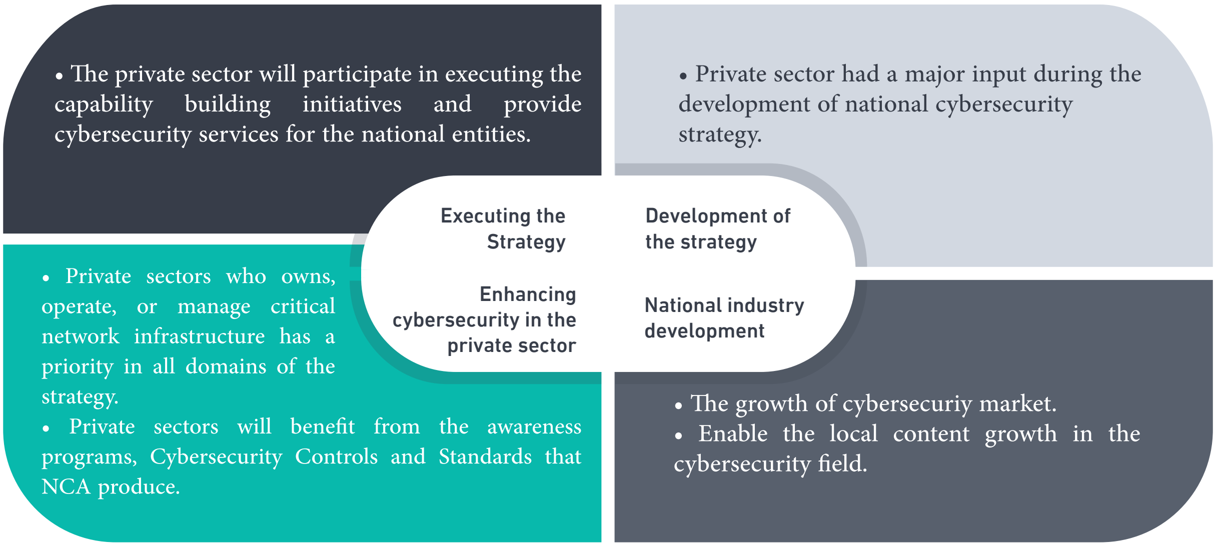
Establishing and enhancing both national and international partnerships through advanced information sharing mechanisms

6. Build: Cyber Ecosystem Development

Protecting the Kingdom›s cyberspace through the presence of a strong, qualified cybersecurity workforce that facilitates a thriving national cybersecurity industry; In addition to Building patriotism in the workforce through cybersecurity education programs and high-quality training; and Enabling growth and prosperity through cybersecurity investment in incentive programs, industry, research and development, and innovation

4.1 Private Sector

The private sector is one of the core elements of the national cyber ecosystem and plays a fundamental role in enhancing cybersecurity across the Kingdom. Therefore, it is considered across key aspects of the Strategy, as shown below:



Executing the Strategy

- The private sector will participate in executing the capability building initiatives and provide cybersecurity services for the national entities.

Development of the strategy

- Private sector had a major input during the development of national cybersecurity strategy.

Enhancing cybersecurity in the private sector

- Private sectors who owns, operate, or manage critical network infrastructure has a priority in all domains of the strategy.
- Private sectors will benefit from the awareness programs, Cybersecurity Controls and Standards that NCA produce.

National industry development

- The growth of cybersecuriy market.
- Enable the local content growth in the cybersecurity field.

Figure (8): Private Sector

”

Centralized Governance, Decentralized Operations

“

05

National Frameworks

National Frameworks

To achieve the national strategic goals of the Strategy and build technical cybersecurity capacities, four national cybersecurity frameworks were developed in parallel with the Strategy. These frameworks, as shown below, are foundational enablers to operationalize to achieve the national strategic goals.

National Frameworks

These frameworks considered the main element to achieve the strategic goals as clarify below:

National Cybersecurity Risk Management Framework

Manages national cyber risk and prioritize national assets based on criticality.

National Cybersecurity Incident Response Framework

Provides a national coordination framework on an event of cyber incident.

National Cybersecurity Information Sharing Framework

Fosters information sharing through a national platform to share cyber information.

National Cybersecurity Capability Building Framework

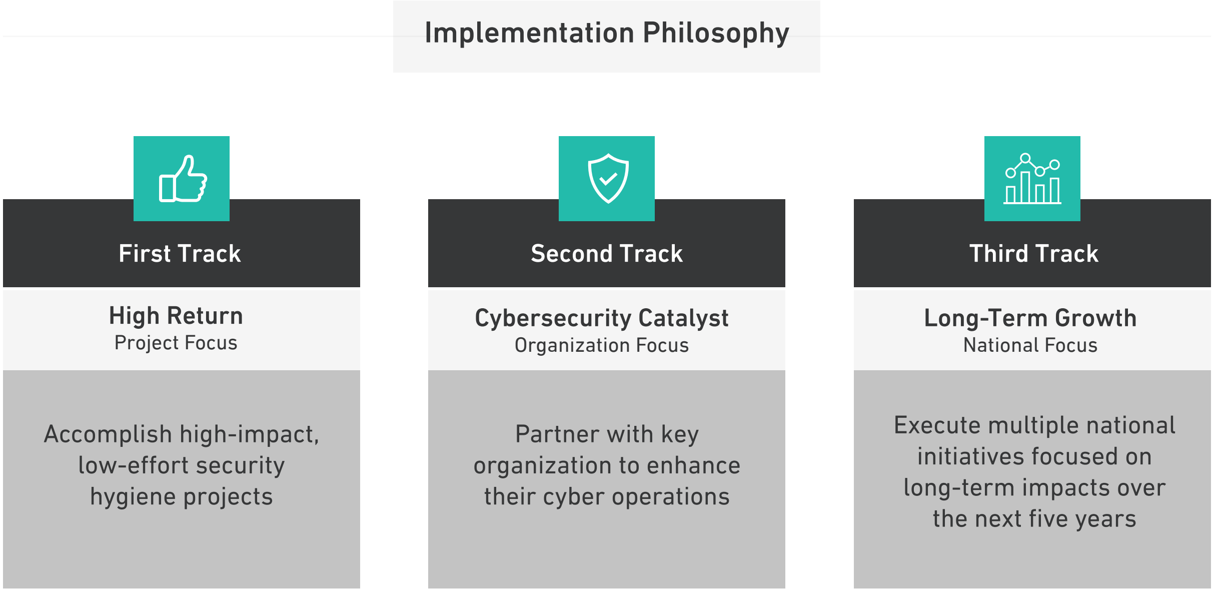
Defines key gaps in cybersecurity workforce in the kingdom and provide initiatives to overcome them.

06

Action Plan

Action Plan

The action plan created three main tracks to achieve measurable national impacts in both the short and long term. These three tracks, shown below, were set to achieve both the Strategy's vision and national strategic goals.



Implementation Philosophy

First Track	Second Track	Third Track
High Return Project Focus	**Cybersecurity Catalyst** Organization Focus	**Long-Term Growth** National Focus
Accomplish high-impact, low-effort security hygiene projects	Partner with key organization to enhance their cyber operations	Execute multiple national initiatives focused on long-term impacts over the next five years

Figure (8): Action Plan Tracks

07

Key Performance Indicators

Key Performance Indicators

Key Performance Indicators were designed to measure the Strategy's effectiveness in achieving its national strategic goals and to measure the level of progress against each goal over the next five years. The KPIs roll up to the three key strategic outcomes:

1. Foster Trust
2. Reduce Risk
3. Contribute to Growth

08

Conclusion

Conclusion

The Kingdom has adopted and implemented a comprehensive approach in its Strategy and is working to achieve the vision and the national strategic goals that will help protect the Kingdom's cyberspace and its vital interests, thereby enabling the Kingdom's Vision 2030.

The incorporation of government organizations, the private sector, and the community in the development of cybersecurity principles will ultimately enhance their awareness, sense of responsibility, and ability to protect assets and vital services. Cooperation and collaboration are essential for the strategy.

Additionally, the NCA will operationalize this Strategy, the roles and responsibilities, national cybersecurity frameworks, and additional relevant frameworks into a Kingdom-wide institutional framework through the issuance of policies, standards, and guidelines.

The NCA will also monitor the progress and advancement in achieving the national strategic goals and take corrective measures for national initiatives and projects as required. To achieve "A resilient, secure, and trusted Saudi cyberspace that enables growth and prosperity" this Strategy will be implemented in an integrated and collaborative way with all relevant stakeholders across the Kingdom

”

establish an integrated cybersecurity framework in the Kingdom

“

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority