المركز الوطني للأمن السيبراني
NATIONAL CYBER SECURITY CENTER

National Cyber Security Strategy
2025-2028

Kingdom of Bahrain

"Public Version"

Acknowledgements

This strategy reflects the spirit of national cooperation and resulted from a collective effort. It involved the active participation of individuals and organizations across the Kingdom of Bahrain, working together to shape the national cybersecurity strategy for 2025-2028.

The strategy development progressed through several phases, including the initiation, current state analysis, strategy formulation, and draft consultation. As part of these phases, eleven workshops were held with key stakeholders, engaging 319 participants, and twenty-five one-to-one meetings were conducted with entities from critical sectors to align priorities and objectives. A survey was also undertaken to assess cybersecurity at an organizational level, with participation from 173 institutions. Discussions and working sessions further supported these efforts to ensure the strategy is comprehensive and based on international best practices.

Sincere thanks are extended to all who contributed and participated. This collaborative effort is expected to support achieving the Kingdom's goals and further advance its digital transformation.

www.ncsc.gov.bh

Table of Contents

Executive Summary

01

Amid rapid digital transformation and technological innovation, the Kingdom of Bahrain is committed to leveraging digital technology to drive economic growth and development. Simultaneously, it prioritizes addressing cybersecurity threats and protecting the nation's digital infrastructure. As emerging technologies and increased connectivity reshape the global risk landscape, maintaining preparedness for the evolving complexities of cyberspace is crucial now more than ever.

Recognizing the critical importance of cybersecurity in today's interconnected landscape, the Kingdom has made it a national priority. This commitment began with the launch of the National Cyber Security Strategy (2021–2024), which has substantially strengthened the Kingdom's cybersecurity framework. The successful implementation of the strategic objectives and initiatives has further enhanced the overall cybersecurity resilience of the Kingdom.

The National Cyber Security Center (NCSC) was established to oversee cybersecurity efforts. Additionally, a national cybersecurity framework has been developed to protect Critical National Infrastructure (CNI), while the National Cybersecurity Incident Response Team (CSIRT) was created to ensure rapid and effective responses to threats. Moreover, the Kingdom has launched nationwide awareness campaigns to educate citizens, residents, and entities about cybersecurity best practices, fostering a culture of preparedness across the Kingdom.

Building on past achievements, the NCSC launched the National Cyber Security Strategy (2025–2028) using a structured methodology aligned with international standards. This methodology was implemented in four key phases: initiation, current state analysis, strategy development, and final approval. By engaging key stakeholders throughout the process, the methodology ensured that the strategy is tailored to the Kingdom's needs, providing a comprehensive view of the cybersecurity landscape, challenges, opportunities, and strategic priorities.

The Kingdom's strategy will be implemented over four years, serving as a comprehensive framework to protect the nation against evolving cyber threats while strengthening the national economy. The strategy aims to establish the Kingdom as a leader in secure, resilient, and trusted cyberspace, enabling digital innovation and sustainable growth. Its mission is to strengthen the Kingdom's digital ecosystem by advancing cybersecurity innovation, ensuring a secure and resilient cyberspace that supports national development and enhances global competitiveness.

The strategy is built on five strategic pillars to strengthen and advance the Kingdom's cybersecurity landscape which are Advanced Cyber Resilience, Robust Cybersecurity Governance, Extended Collaboration and Partnerships, Sustainable Awareness and Workforce Development, and Cyber Research, Development, and Innovation. Together, they represent a proactive and strategic approach to addressing cybersecurity threats effectively.

Bahrain's National Cyber Security Strategy (2025–2028) adopts a comprehensive approach to strengthening national security, driving economic growth, and advancing digital transformation. Built on five strategic pillars, the strategy strengthens cyber resilience, governance, collaboration, cyber awareness, workforce development, and research-driven innovation to address evolving threats. The strategy ensures a secure, adaptive, and globally aligned digital ecosystem by protecting CNI, strengthening regulations, fostering global partnerships, developing cybersecurity talent, and investing in innovation. These efforts reinforce the Kingdom's position as a leader in cybersecurity and the digital economy.

Introduction

02

As the Kingdom of Bahrain advances toward a digitally driven future, cybersecurity plays a pivotal role in safeguarding national security, economic growth and enabling digital transformation. With technology becoming increasingly integrated into all aspects of society, securing digital infrastructure is more essential than ever. Additionally, emerging technologies transform industries, drive innovation, and create new economic opportunities. However, the rapid technological evolution brings risks, including increased vulnerabilities and more sophisticated cyber threats. These threats target various entities, from CNI and SMEs to organizational and individual digital assets.

The Kingdom is committed to strengthening its cybersecurity framework through a proactive cybersecurity strategy that builds on the successes of the National Cyber Security Strategy (2021–2024). This initiative positioned the Kingdom as a Tier One country and a global role model among 194 nations in the Global Cybersecurity Index (GCI) of the International Telecommunication Union (ITU) in 2024. The National Cyber Security Strategy (2025–2028) is a comprehensive response to the evolving challenges of cyberspace. Its development process aligns with international best practices while addressing the Kingdom's cybersecurity needs.

The strategy was developed through a four-phase process: initiation, current state analysis, strategy development, and final approval. During the initiation phase, a development plan was created, and key stakeholders from CNI sectors were identified. The current state analysis phase involved conducting multiple assessments to evaluate the Kingdom's cybersecurity posture. In the development phase, a draft was developed and shared with stakeholders for consultation and feedback. In the final approval phase, the revised strategy was submitted for formal approval. The strategy's implementation will emphasize continuous and active engagement with CNI sector regulators and entities, supported by regular updates and evaluations to ensure effective implementation of the strategy, role clarity, and accountability.

The National Cyber Security Strategy (2025-2028) is based on five key pillars to establish a resilient, secure, and trustworthy cyberspace for the Kingdom. Advanced Cyber Resiliency secures CNI and SMEs with tailored defenses, threat detection, and response. Robust Cybersecurity Governance unifies national security through enforceable laws, standardized risk management, and continuous compliance. Extended Collaboration and Partnerships promotes national and global cooperation for improved threat intelligence sharing and coordinated responses.

Sustainable Awareness and Workforce Development fosters a security culture and builds national capabilities through targeted training. Cyber Research, Development, and Innovation fosters a sustainable cybersecurity ecosystem through research and local solutions, supporting private sector growth. A comprehensive action plan implements these pillars through strategic initiatives, enabling the Kingdom to flourish in an interconnected digital landscape.

Strategic Pillars

These pillars empower national cybersecurity through resilience, effective governance, strategic collaboration, skilled workforce, and innovation.

Bahrain’s Expanding Cyberspace

The Kingdom’s cyberspace is rapidly expanding. This growth is driven by the implementation of national digital transformative initiatives and strategies, such as the Information and Communication Technology (ICT) Strategy, the Digital Economy Strategy, the Sixth National Telecommunications Plan (NTP6), and the National Digital Trade Strategy. These efforts align with the Kingdom’s vision to strengthen digital infrastructure and connectivity, diversify the economy, and establish a leading position in the digital economy.

The deployment of high-speed fiber broadband and widespread 5G networks is creating a strong foundation for a thriving digital economy. The integration of emerging technologies like 5.5G and 6G further fosters a technology-driven and inclusive ecosystem for businesses and individuals. Additionally, investments in international connectivity, such as submarine cables and cross-border data exchange, position the Kingdom as a regional hub for digital services and cloud computing. These measures elevate the quality of internet services while enhancing the reliability, scalability, and resilience of the nation’s digital infrastructure.

Furthermore, the initiatives aimed at promoting the adoption of emerging technologies, including artificial intelligence (AI) and cloud computing, enhance operational efficiency. This is especially beneficial for SMEs, as it facilitates trade processes through digital trade platforms. This enables organizations to expand their market reach, enhance competitiveness, and capitalize on technological advancements. Additionally, the integration of financial technology (FinTech) solutions accelerates digital payment systems, streamlines financial operations, and promotes economic inclusivity by providing businesses and consumers with secure, efficient financial services.

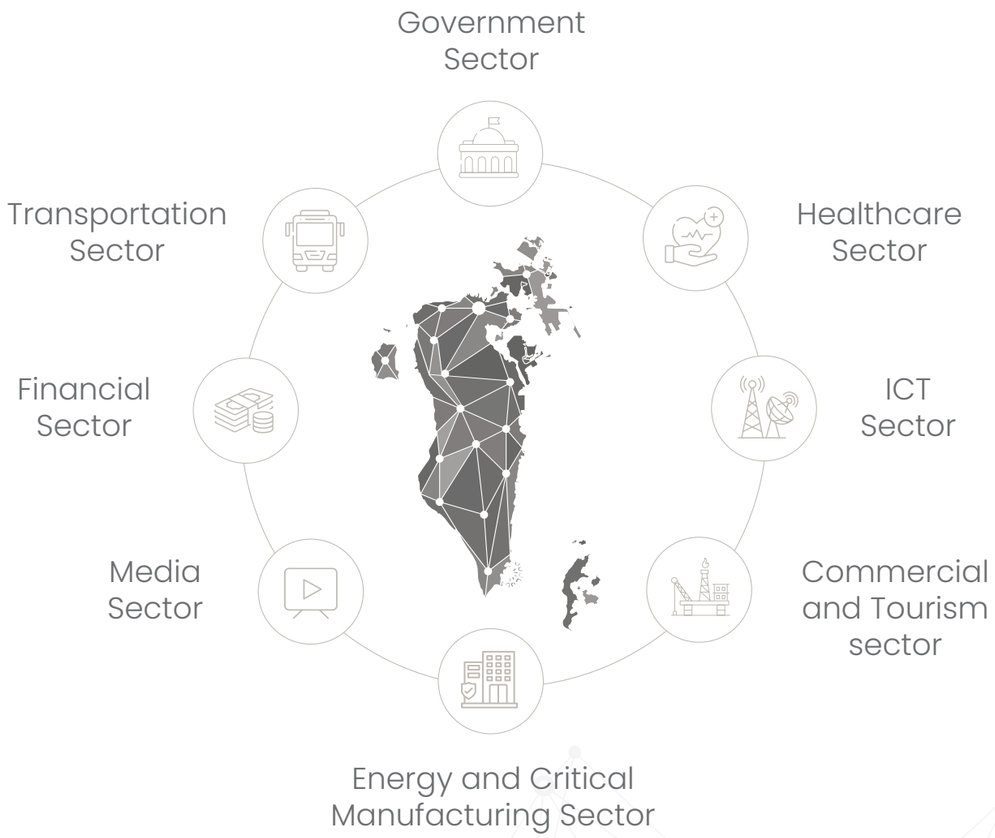
Critical National Infrastructure Sectors

04

Defining the CNI sectors is essential for safeguarding the kingdom's vital services and preventing disruptions that could threaten national security, economic stability, and public health. The National Cyber Security Strategy 2021-2024 defined seven CNI sectors, which are Government, Financial, Healthcare, Transportation, Information and Communication Technology (ICT), Gas, Electricity and Oil (GEO), and critical manufacturing.

During the development of the National Cyber Security Strategy 2025-2028, each sector is evaluated and assessed using the Political, Economic, Social, Technological, and Human (PEST-H) analysis tool, which identified the following sectors as CNI sectors:

CNI Sectors



Government Sector

It provides essential public services across the Kingdom. This includes ensuring the continuous and reliable operation of government functions that support national stability and resilience.

Financial Sector

It manages the national currency and delivers essential financial services, including banking, digital transactions, and support for the digital economy. It plays a vital role in sustaining the Kingdom's economy.

ICT Sector (Information and Communications Technology)

It includes all entities responsible for IT communications, connectivity, and services within the Kingdom. It ensures a seamless flow of information and facilitates secure communication.

Energy and Critical Manufacturing Sector

It ensures a reliable supply of electricity, oil, gas, and industrial goods. These are essential for economic stability, national security, and sustainable development.

Healthcare Sector

It safeguards public health, manages disease outbreaks, and delivers critical medical services. It ensures the continuous provision of both routine and emergency care.

Media Sector

It delivers accurate news and information, shapes public opinion, and ensures secure and responsible dissemination of content.

Transportation Sector

It enables the movement of people and goods domestically and internationally. It supports national and global supply chains by ensuring the timely delivery of resources and products.

Commercial and Tourism Sector

It provides critical economic and cultural exchange services, enables business operations, and promotes international trade. This sector also emphasizes facilities, hotels, and tourism, significantly contributing to economic growth.

Vision and Mission

05

The vision and mission of the National Cyber Security Strategy (2025-2028) reflect the Kingdom's commitment to establishing a secure, resilient, and trusted digital environment that fosters innovation and drives national growth. The vision defines the aspiration for the Kingdom to lead in cyberspace, aligning with its broader objectives of advancing digital transformation.

Vision

"Positioning Bahrain as a leader in secure, resilient, and trusted cyberspace, driving digital innovation and growth"

The mission outlines the strategic approach to achieving the vision. It focuses on enhancing the digital ecosystem through innovative cybersecurity measures and strong protection. It emphasizes the importance of safeguarding CNI, empowering businesses, raising awareness, and ensuring public trust, while also fostering domestic and international partnerships. It also addresses emerging threats to strengthen the Kingdom's cybersecurity resilience and global competitiveness.

Mission

"Elevating Bahrain's digital ecosystem as a leader in cybersecurity by supporting innovation and promoting a secure, resilient, and trusted cyberspace to drive national growth and boost global competitiveness"

Strategy Pillars and Objectives

06

The National Cyber Security Strategy (2025–2028) is built on five essential strategic pillars, each with defined objectives and outcomes to support the Kingdom's vision and mission. The core strategy pillars are Advanced Cyber Resilience, Robust Cybersecurity Governance, Extended Collaboration and Partnerships, Sustainable Awareness and Workforce Development, and Cyber Research, Development, and Innovation.

National Cyber Security Strategy Pillars

Advanced Cyber Resiliency — Pillar 01

Objectives

01 Strengthening the Protection of National Digital Infrastructure
02 Bolstering Threat Countering Capabilities
03 Enhancing Crisis Management and Incident Response

Robust Cybersecurity Governance — Pillar 02

Objectives

01 Enhancing Cybersecurity Regulations and Laws
02 Managing Cyber Risks at a National Level
03 Building on National Cybersecurity Policies and Standards
04 Maintaining Ongoing Cybersecurity Compliance

Extended Collaboration and Partnerships — Pillar 03

Objectives

01 Strengthening Domestic Cybersecurity Collaboration
02 Expanding Regional and Global Partnerships

Sustainable Awareness and Workforce Development — Pillar 04

Objectives

01 Broadening National Cybersecurity Awareness
02 Developing a Skilled Cybersecurity Workforce

Cyber Research, Development, and Innovation — Pillar 05

Objectives

01 Promoting National Research, Development, and Innovation Capabilities
02 Elevating the Cybersecurity Industry

Pillar
01

Advanced Cyber Resiliency

Objectives

01 Strengthening the Protection of National Digital Infrastructure

02 Bolstering Threat Countering Capabilities

03 Enhancing Crisis Management and Incident Response

Cyber resilience is essential to protecting the Kingdom's digital ecosystem. It ensures the capability to anticipate, resist, recover from, and adapt to cyber threats while sustaining critical functions and services. Cyber resilience enhances national security, builds public trust, and supports economic stability. Cyber resilience enables the Kingdom to thrive in an interconnected digital landscape. Achieving resilience requires coordinated efforts to safeguard digital infrastructure, counter threats effectively, strengthen crisis management, and enhance incident response capabilities.

Objective 01

Strengthening the Protection of National Digital Infrastructure

The growing dependence on digital infrastructure highlights the need for robust cybersecurity measures across CNI sectors and extends the protection to SMEs. Due to resource constraints, SMEs require tailored security solutions to strengthen their defense capabilities. It is crucial to ensure the protection of essential services and economic activities to strengthen their resilience against cyber threats.

To advance the scope of protection, a multi-layered approach will be adopted, combining immediate actions with long-term plans. This approach includes implementing cybersecurity frameworks, controls, and best practices tailored to the specific requirements of CNI and SMEs. It focuses on strengthening defenses, improving cybersecurity responses, and enhancing competency across these sectors.

Additionally, it increases trust in cybersecurity services by ensuring their quality and reliability. Fostering cross-sector communication will help enhance capabilities and enable a coordinated response to large-scale cyber threats.

Objective 02

Bolstering Threat Countering Capabilities

The evolving cyber threat landscape is shaped by adversaries using advanced technologies and driven by diverse motives. These threats pose significant risks to the continuity of essential services and the stability of digital infrastructure. To effectively combat these threats, it is crucial to enhance operational, intelligence, and technical capabilities to counter, disrupt, and respond to them while securing national infrastructure and ensuring resilience.

Building trust among key stakeholders and CNI entities is essential for a coordinated, layered approach to threat intelligence sharing at both national and sectoral levels. The approach focuses on having a tailored threat information-sharing platform that connects CNI entities, enabling dynamic threat detection, prevention, and response.

This objective focuses on strengthening cybersecurity intelligence sharing and real-time monitoring to mitigate risks effectively. Integrating advanced technologies, such as AI and machine learning, into threat detection and response will be crucial for maintaining a resilient national cyber defense. These initiatives will strengthen national digital infrastructure security and reinforce confidence in its cybersecurity readiness.

Objective 03

Enhancing Crisis Management and Incident Response

Effective crisis management and incident response are crucial for maintaining digital infrastructure resilience, especially given the potential damage caused by cyberattacks, including those driven by geopolitical events. Organizations must implement comprehensive plans, procedures, and mechanisms for crisis management, incident response, business continuity, and disaster recovery to mitigate these risks. A coordinated national approach is necessary to contain cyberattacks, minimize their impact, and continuously improve response capabilities.

Priority will be given to developing and regularly testing crisis and incident response plans at both the sector-specific and national levels. Additionally, clear definitions of cyberattack levels, scenarios, and reporting procedures will be established. Cyber exercises will enhance stakeholder coordination, strengthening collective preparedness. Advanced technologies will enhance crisis detection and provide deeper insights, ensuring accurate event classification and effective countermeasures. Additionally, lessons learned from past incidents will shape future policies and procedures, while adopting international best practices will accelerate cyber mitigation efforts.

Pillar
02

Robust Cybersecurity Governance

Objectives

01 Enhancing Cybersecurity Regulations and Laws

02 Managing Cyber Risks at a National Level

03 Building on National Cybersecurity Policies and Standards

04 Maintaining Ongoing Cybersecurity Compliance

This pillar promotes a unified, proactive approach to securing the Kingdom's digital infrastructure and ecosystem. Effective governance is essential for mitigating cyber risks, strengthening resilience, and building trust in the digital economy. To enhance the Kingdom's cybersecurity governance framework, this pillar focuses on aligning with international best practices, enforcing cyber laws and regulations, and implementing risk management strategies. It also seeks to establish a structured approach to policy development, regulatory enforcement, continuous compliance, and risk assessment across CNI and SMEs.

Objective 01

Enhancing Cybersecurity Regulations and Laws

A comprehensive legal and regulatory framework is essential for effective national cybersecurity governance. It provides clear principles, defines roles and responsibilities, and establishes accountability measures. Enforceable regulations and cybersecurity laws mandate cybersecurity practices to protect digital infrastructure, safeguard national interests, and enhance cross-sector coordination.

Establishing and maintaining an adaptive legal framework is critical for standardizing cybersecurity practices and ensuring compliance. Regular updates will help keep pace with evolving threats and technologies. They will also help ensure cybersecurity policies remain aligned with emerging risks, technological advancements, and international best practices. This approach will strengthen national resilience and the Kingdom's ability to address evolving cyber challenges effectively.

Objective 02

Managing Cyber Risks at a National Level

Effective management of cyber risks at the national level requires fostering a risk-aware culture. This enables organizations to proactively identify, assess, and mitigate evolving threats while adhering to standardized risk management frameworks. A structured risk-based approach is essential to prioritize cybersecurity investments and implement measures that maximize protection within entities.

The established National Cyber Risk Management Framework is the guiding reference for assessing risks and evaluating potential impacts. It also helps assess threat likelihood, along with the effectiveness and cost of security measures. This framework aligns with international best practices, including the National Institute of Standards and Technology (NIST), Center for Internet Security (CIS), and International Organization for Standardization (ISO) standards. By leveraging the national framework, entities can apply structured risk assessment methodologies, gain critical insights into risk exposure, and identify mitigation priorities.

Objective 03

Building on National Cybersecurity Policies and Standards

Reliance on cybersecurity requires standardized governance guidelines to build public trust and help entities protect their digital assets. To broaden the scope of protection, unified governance frameworks must address sector-specific requirements and adapt to emerging trends and technological advancements. These frameworks will incorporate supply chain security requirements, security-by-design principles, and considerations for emerging technologies like AI, Internet of Things (IoT), and quantum computing. Additionally, a formal review process will ensure continuous improvement of existing frameworks and standards by integrating industry feedback.

Entities will be encouraged to adopt cybersecurity frameworks and controls. This approach will enable a phased implementation, allowing entities to enhance their security posture gradually. Additionally, a structured licensing processes for cybersecurity service providers will be developed to ensure proper implementation of cybersecurity controls and maintain the quality of services provided.

Objective 04

Maintaining Ongoing Cybersecurity Compliance

A continuous cybersecurity compliance procedure ensures that entities within CNI sectors adhere to national cybersecurity standards, keeping them aligned with emerging threats and evolving technologies. Regular compliance assessments are necessary to promote a security-conscious culture, enhance preparedness, and maintain business continuity.

A compliance framework will assess entities' adherence to cybersecurity standards through periodic audits and structured reporting mechanisms. Clear penalties and corrective measures for noncompliance will be defined to uphold the integrity and effectiveness of cybersecurity standards and reinforce accountability across all entities.

"

Secure Today,
Govern Wisely,
Lead Tomorrow

Pillar
03

Extended Collaboration and Partnerships

Objectives

01 Strengthening Domestic Cybersecurity Collaboration

02 Expanding Regional and Global Partnerships

Uniting domestic, regional, and global efforts is essential for strengthening cybersecurity resilience. In an interconnected digital landscape where cyber threats transcend borders, collaboration enhances collective defense. Strengthening information-sharing across CNI sectors fosters a unified cybersecurity strategy that integrates threat intelligence, resilience policies, and lessons learned while ensuring compliance with data protection and privacy regulations. Regional and international partnerships align with global standards, promote participation in cybersecurity exercises, and facilitate knowledge exchange through capacity-building initiatives. By promoting coordinated efforts, cybersecurity readiness improves, enabling more effective threat detection, response, and recovery.

Objective 01

Strengthening Domestic Cybersecurity Collaboration

Strengthening domestic collaboration mechanisms is critical to enhancing national cybersecurity defenses. Without structured frameworks, organizations struggle to leverage expertise and share critical information across sectors. Establishing coordinated collaboration frameworks improves cyber incident recovery, fortifies collective defenses, and promotes unified strategies for proactive preparedness.

A standardized framework will be developed to facilitate communication among entities. This framework will define roles, protocols, and processes for effective collaboration, ensuring the integration of expertise, knowledge, and cybersecurity initiatives. In addition, a dedicated communication model will streamline incident reporting and threat updates among stakeholders. By facilitating knowledge-sharing and incorporating lessons learned, the framework will strengthen defense strategies, fostering a resilient cybersecurity ecosystem capable of addressing both current and emerging threats.

Objective 02

Expanding Regional and Global Partnerships

International cybersecurity partnerships are essential in a borderless digital landscape where cyber threats originate from diverse global sources. Strengthening regional and global collaboration through bilateral and multilateral agreements provides deeper insight into emerging trends, evolving threats, and technological vulnerabilities.

These partnerships enable knowledge exchange and resource collaboration with international entities and organizations. They also support capacity-building initiatives through training programs and collaborative cybersecurity efforts. Engaging in regional and international cybersecurity exercises strengthens preparedness and keeps stakeholders informed about evolving threats. Additionally, participation in global cybersecurity conferences ensures alignment with international best practices, strengthening cybersecurity resilience and fostering a secure digital environment.

“

Together
We Defend,
United We
Secure

Pillar
04

Sustainable Awareness and Workforce Development

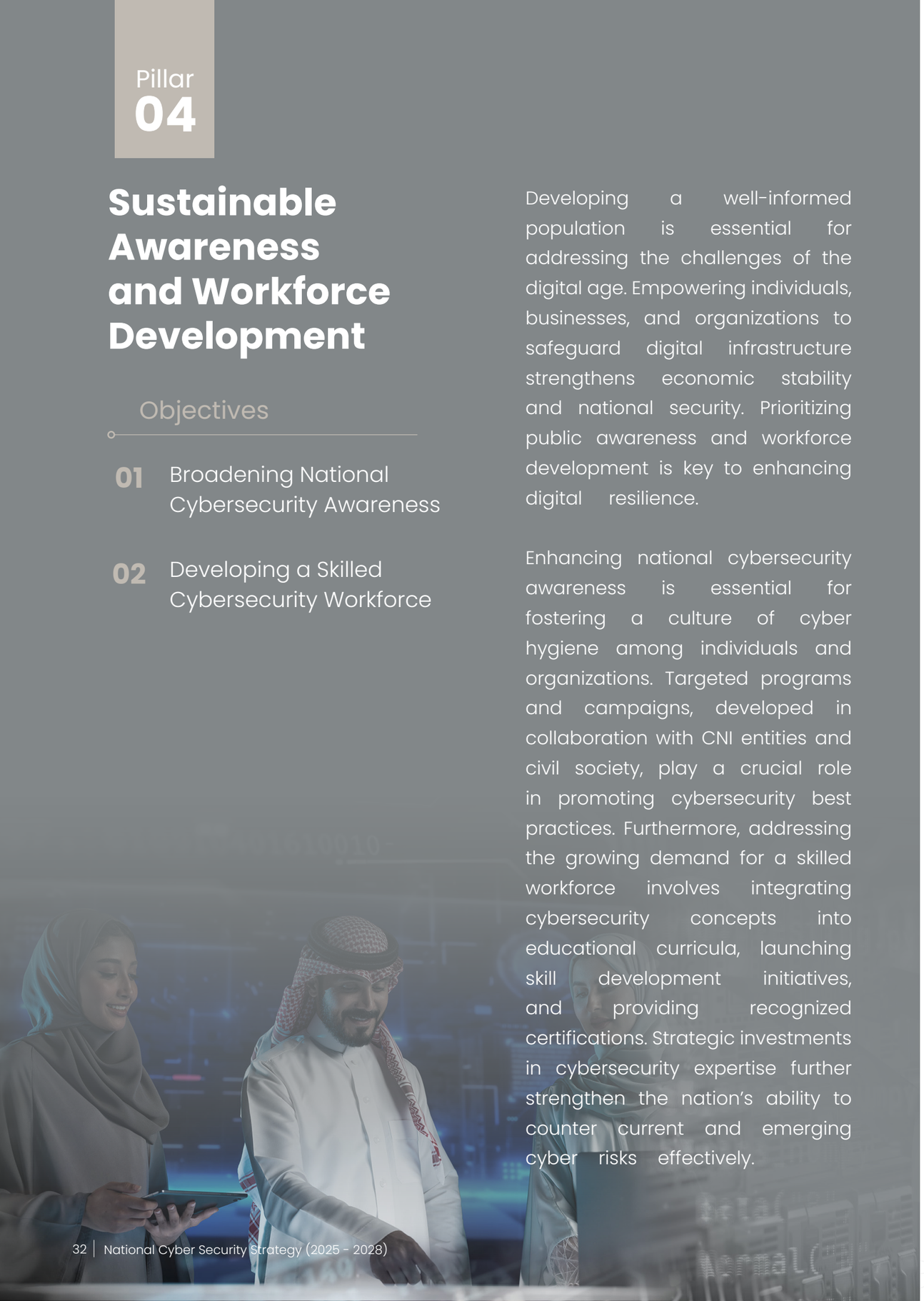
Objectives

01 Broadening National Cybersecurity Awareness

02 Developing a Skilled Cybersecurity Workforce

Developing a well-informed population is essential for addressing the challenges of the digital age. Empowering individuals, businesses, and organizations to safeguard digital infrastructure strengthens economic stability and national security. Prioritizing public awareness and workforce development is key to enhancing digital resilience.

Enhancing national cybersecurity awareness is essential for fostering a culture of cyber hygiene among individuals and organizations. Targeted programs and campaigns, developed in collaboration with CNI entities and civil society, play a crucial role in promoting cybersecurity best practices. Furthermore, addressing the growing demand for a skilled workforce involves integrating cybersecurity concepts into educational curricula, launching skill development initiatives, and providing recognized certifications. Strategic investments in cybersecurity expertise further strengthen the nation's ability to counter current and emerging cyber risks effectively.



Objective 01

Broadening National Cybersecurity Awareness

Raising cybersecurity awareness is critical to strengthening the nation's digital resilience. Targeted initiatives will educate individuals, businesses, SMEs, and industry professionals on best practices for securing digital assets and mitigating cyber risks. To ensure sector-specific relevance, awareness programs will be developed in collaboration with CNI regulators, entities, and civil society organizations.

Maximizing outreach requires utilizing various communication channels and digital media to effectively deliver cybersecurity guidance. The CyberWiser program will expand to support multiple languages, providing accessible resources, practical tools, and insights into emerging threats. Enhancing public understanding of cyber risks and promoting responsible digital behavior will strengthen national cybersecurity resilience and foster a more secure digital environment.

Objective 02

Developing a Skilled Cybersecurity Workforce

Building a skilled and adaptable cybersecurity workforce is essential for addressing the increasing complexity of cyber risks and ensuring a secure digital transformation. Enhancing cybersecurity expertise protects digital infrastructure and promotes economic growth, establishing the nation as a leader in secure digital infrastructure. Integrating cybersecurity concepts into education at all levels, from early childhood to higher education, enhances foundational knowledge and prepares future professionals. Partnerships with national and international organizations will further support these efforts. Additionally, upskilling programs aligned with global cybersecurity standards will equip professionals and new entrants with the expertise needed to navigate evolving cyber risks effectively.

One of the primary objectives is enhancing cybersecurity and IT competencies through targeted training and capacity-building programs. These programs will develop a comprehensive skill set, covering both foundational and advanced levels, ensuring participants acquire the technical expertise required for success in cybersecurity and IT roles. Moreover, promoting gender diversity through specialized programs will empower women, increase their representation, and strengthen their contributions to the cybersecurity sector.

Collaboration with academic institutions and industry leaders will facilitate workshops, conferences, networking opportunities, and knowledge-sharing initiatives. Investing in workforce development strengthens national cybersecurity capabilities, increases resilience across sectors, and ensures long-term preparedness in an ever-evolving cyber landscape.

> "With Knowledge, Skills Grow and **Cybersecurity Advances**

Pillar
05

Cyber Research, Development, and Innovation

Objectives

01 Promoting National Research, Development, and Innovation Capabilities

02 Elevating the Cybersecurity Industry

This pillar promotes the Kingdom's cybersecurity research, development, and innovation (RDI) through collaboration among government, CNI sectors, industry, and academia. It identifies and prioritizes emerging cyber challenges, advances defensive capabilities, and promotes industry growth through national RDI initiatives. By supporting startups, developing a skilled workforce, and encouraging local cybersecurity solutions, the Kingdom aims to build a resilient, innovative, and competitive cybersecurity ecosystem.

Objective 01

Promoting National Research, Development, and Innovation Capabilities

Encouraging national cybersecurity RDI is necessary to address the current cybersecurity challenges and strengthen the defensive capabilities of national infrastructure. This effort requires the development of national RDI plans that promote collaboration between key stakeholders. By implementing a coordinated approach, these plans will identify emerging challenges, prioritize critical cybersecurity topics, and direct national resources to high-impact areas.

The plans will outline specific activities, competitions, and programs, such as stakeholder-focused sessions and hackathons. They will also encourage active participation from organizations, companies, and academic institutions to develop research-driven and practical solutions for addressing cybersecurity challenges in a controlled environment.

Objective 02

Elevating the Cybersecurity Industry

The Kingdom aims to strengthen cybersecurity by supporting startup growth and innovating technologies. A strong domestic cyber industry will enhance public trust in digital platforms, establish a secure digital environment, attract international investments, and boost the national economy.

Through conferences and industry events, startups will have opportunities to connect and collaborate with key stakeholders, including potential partners, investors, and customers. These engagements will facilitate knowledge exchange, promote best practices, and build startups' credibility and reputation. Additionally, they will help stakeholders better understand the nature and demands of the cybersecurity industry. Furthermore, a key priority is promoting the adoption of locally developed cybersecurity products and services to strengthen the domestic market. Organizations will be encouraged to source local cybersecurity solutions.

> "Innovation Shapes Cyberspace

Conclusion

07

Bahrain's National Cyber Security Strategy (2025–2028) establishes a comprehensive, forward-looking approach to safeguarding the Kingdom's digital ecosystem. As the Kingdom advances its digital transformation and adopts emerging technologies, cybersecurity remains a national priority. This strategy ensures the resilience of CNI, secures economic stability, and fosters public trust in the digital landscape. This strategy builds on previous initiatives and introduces a structured, proactive framework to address evolving cyber threats while aligning with global best practices.

The strategy is built on five pillars that collectively strengthen the Kingdom's cybersecurity resilience. The first pillar enhances national digital infrastructure and defenses against cyber threats, ensuring CNI and SMEs have strong security measures. The second pillar aims to establish a legal and regulatory foundation, develop and implement policies and standards, ensure compliance, and enforce the risk management framework. The third pillar strengthens national, regional, and international cooperation and partnership to enhance cybersecurity resilience. The fourth pillar focuses on advancing cybersecurity awareness and workforce development. The fifth pillar fosters cybersecurity advancements and industry growth by focusing on research, development, and innovation.

This strategy addresses immediate and long-term cybersecurity challenges, ensuring the Kingdom remains adaptable to future technological advancements. By prioritizing proactive cybersecurity measures and aligning with global standards, the Kingdom will cultivate a secure, resilient, and innovative digital environment that supports national priorities and strengthens global competitiveness.

ncscbh

ncsc_bh

www.ncsc.gov.bh