CYBERSHIELD
CYBER RESILIENCE ENHANCEMENT INITIATIVE
STATE BANK OF PAKISTAN

CYBER SHIELD

CYBER RESILIENCE STRATEGY FOR SBP REGULATED ENTITIES

2025-2030

CYBERSHIELD
CYBER RESILIENCE ENHANCEMENT INITIATIVE
STATE BANK OF PAKISTAN

CONTENTS

CHAPTER 1: CONTEXT 3

1.1. INTRODUCTION 3

1.1. THREAT LANDSCAPE 4

1.2. CHALLENGES 5

CHAPTER 2: STRATEGIC DIRECTION 7

2.1. VISION 7

2.2. MISSION 7

2.3. APPROACH 7

2.4. STRATEGIC PRINCIPLES 8

CHAPTER 3: STRATEGIC PRIORITIES 10

3.1. STRENGTHEN 11

3.2. MATURE 13

3.3. ENHANCE 14

3.4. DEVELOP 15

3.5. EVOLVE 16

CHAPTER 1: CONTEXT

1.1. INTRODUCTION

In today's hyper-connected global economy, digital transformation presents both unprecedented opportunities and complex risks. Across the financial system, advanced technologies—artificial intelligence, cloud computing, blockchain, and real-time payments—are redefining how economies operate and how people interact with money. This evolution is unfolding rapidly in both emerging and advanced markets, driven by customer demand for faster, more secure, and more inclusive financial services.

The Pakistan's banking sector, as a cornerstone of economic growth and financial stability, is engaged in this global transformation. The policy and infrastructure advancements, including instant payment systems, digital onboarding, and branchless banking have enabled strong digital adoption in recent years. The COVID-19 pandemic acted as a catalyst, accelerating technology-led operations that have since become embedded as the new normal, positioning Pakistan's banking ecosystem firmly within the interconnected, technology-dependent global economy.

This transformation, however, has amplified systemic risks. The sector's growing reliance on technology means that a single major disruption—whether from operational failure or a coordinated cyber-attack—could trigger cascading effects, eroding stability and public trust. The expanding digital footprint has also made banks a more attractive target for sophisticated cyber threat actors, many operating across borders. Yet, the speed of digitalization has outpaced the maturity of cybersecurity controls. The ready availability of cyber-attack tools and capabilities has lowered the barrier for malicious actors, contributing to a marked increase in both the volume and sophistication of cyber-attacks against financial institutions.

Safeguarding resilience in this environment demands that cybersecurity and operational risk management evolve in tandem with the digital growth. This requires coordinated regulatory frameworks, participation in threat intelligence sharing, and sustained investment in cybersecurity capabilities—priorities emphasized by leading international standard-setting bodies as essential to protecting financial stability while enabling innovation.

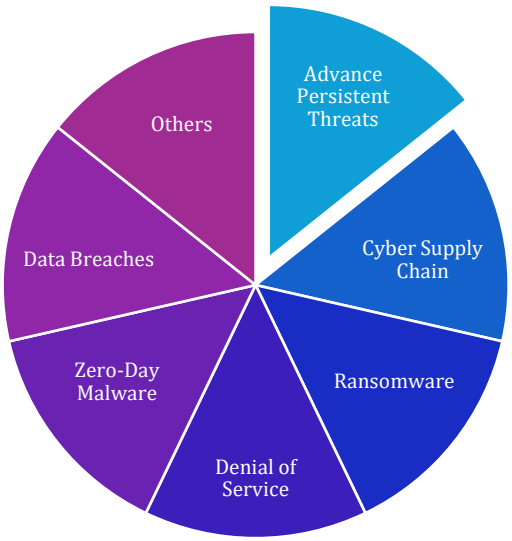
Accordingly, the purpose of this cyber resilience strategy is to ensure a comprehensive, holistic, and integrated approach that enables regulated entities to continuously adapt and respond to the constantly evolving cyber threat landscape, and to enhance the ability to protect systems from cyber-attacks, and to resume business operations quickly in case of a successful cyber-attack.

1.1. THREAT LANDSCAPE

The complexity of cyber threat landscape has been constantly evolving during the last couple of years. The changes in the cyber threat landscape entail enhancement in capability of the threat actors or interest of new threat actors in the regulated entities. In addition to the traditional website defacement and Denial of Service (DoS) attacks, there has been an increase in the number of Advance Persistent Threat (APT) and ransomware attacks which require some degree of technical capabilities. The use of zero-day malwares to institute cyber-attacks has also intensified. Further, the propensity of exploiting digital banking applications and services for reaping financial rewards has also seen a growth. Data security is another vital concern for regulated entities as there have been threat intelligence reports regarding availability of payment card data and user credentials of various regulated entities on the dark web.

Another important shift noted globally and domestically is the inclination of the threat actors to target the suppliers/ vendors of the financial institutions, as an easy means to achieve their objectives, i.e. cause harm to the financial institutions. Notable global and domestic software and other technology providers have been successfully targeted by the threat actors, which highlights the importance of cybersecurity posture of the third parties providing services to the regulated entities.

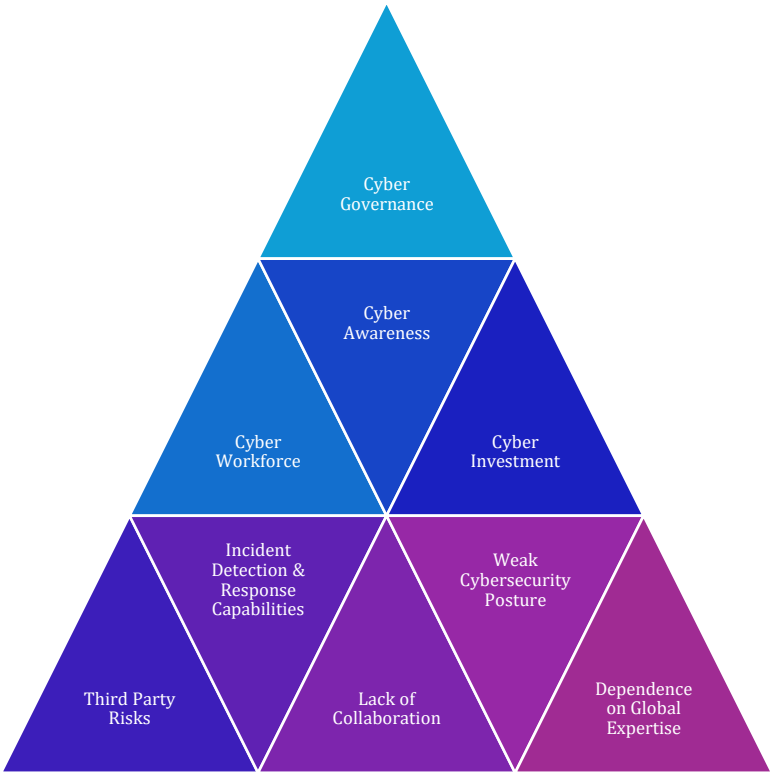
There has been increase in state sponsored cyber offensive activities, where nation state backed threat actors have been the source of aggressive cyber-attacks around the globe, using cyber operations for financial gain or to promote their own national interest. Considering the geopolitical circumstances, the cyber threats from nation states and state sponsored groups remain critical. With some of the adversary nations increasing their cyber offensive capabilities, there is potential for an increase in sophisticated cyber-attacks targeting systemic components of key national infrastructure. Globally, financial institutions and governments are also seeing a rise in the number and complexity of ransomware attacks. Trends include larger ransom payment demands and multifaceted attack tactics.



1.2. CHALLENGES

The cyber risks have significantly increased with rapid digitalization in the banking sector; however, the understanding of the said risks along with maturity of the cyber defense capabilities have not enhanced with the same pace, which has created a vulnerable cybersecurity posture. Considering the rapidly evolving threat landscape, it is vital for the regulated entities to improve their cyber defense capabilities.

Several challenges need to be addressed to considerably improve the cybersecurity posture of regulated entities. Cybersecurity governance needs to be improved at all levels. The boards and senior management of the regulated entities must have a clear understanding of their cyber risk posture, to take measures including investment in cyber defense, to enhance the cyber defense capabilities. Timely replacement/upgrade of systems and technologies is also challenging for some of the regulated entities which significantly increases the attack surface of these entities.



The trend and response to the cyber-attacks in recent past have revealed the need for improvement in cyber incident detection and response capabilities of the regulated entities. Hence, there is a need to significantly enhance incident detection and response capabilities on a priority basis. Further, collaboration among all the stakeholders is a prerequisite for quality cyber defense of any sector; however, the regulated entities need to improve collaboration on the subject including sharing of threat information, collaborative response, cyber workforce development, etc.

The cyber workforce is the most sought-after globally. The situation is more grave domestically. Not only is there scarcity of cyber workforce but also the quality and required skills are not available. The regulated entities heavily rely on the third-party service providers for a wide range of technology related functions including cybersecurity related responsibilities. These encompass not only the procurement of software and hardware solutions but also the outsourcing and insourcing of critical services such as

security operations, incident response, and digital forensics. Given that these entities fall outside the direct regulatory purview of SBP, ensuring their adherence to robust cybersecurity standards present a persistent challenge. This risk is further heightened in case of the international vendors, where oversight complexities and jurisdictional limitations can further impede effective governance and risk management.

Owing to the limited domestic capacity of Information Technology (IT) firms capable of delivering the specialized products and services demanded by the regulated entities, a substantial portion of these third-party providers operate from foreign jurisdictions—amplifying both the dependency risk and the need for enhanced due diligence mechanisms.

CHAPTER 2: STRATEGIC DIRECTION

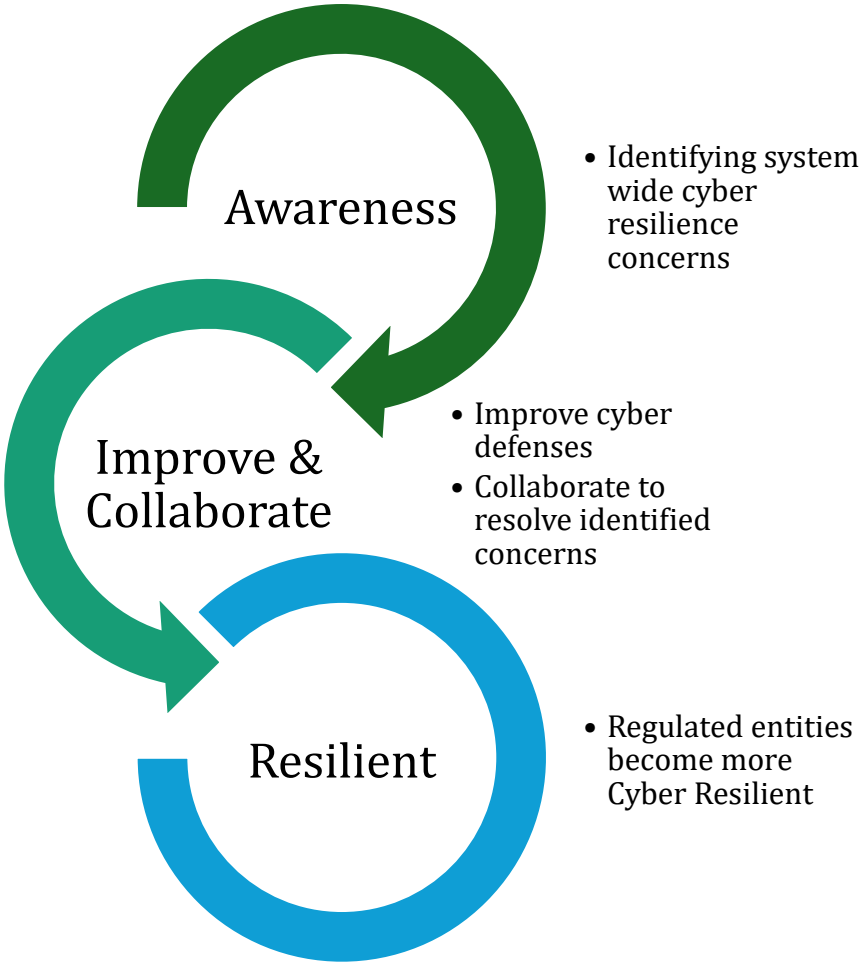
2.1. VISION

To ensure safe, reliable, and resilient financial services by strengthening cyber resilience of regulated entities against evolving cyber threats.

2.2. MISSION

To enhance the safety, efficiency, and stability of regulated entities through strong cybersecurity capabilities, shared knowledge, and comprehensive supervision.

2.3. APPROACH

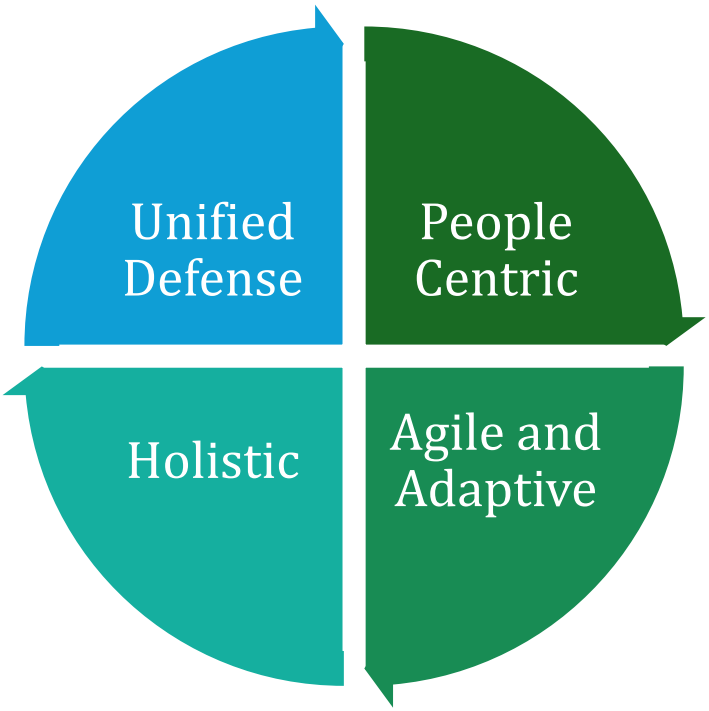


2.4. STRATEGIC PRINCIPLES

This strategy defines four principles of action to deliver the vision. This will require a collaborative approach among the regulated entities working together to achieve the vision that is guided by the below defined strategic principles.

2.4.1. Unified Defense

This principle recognizes that the scale and pace of the threats demand a more comprehensive and unified response. The availability of cyber offensive tools and information, and threat intelligence pertaining to the threat actors reveals that one of the strengths of these actors is collaboration among themselves, which helps them to build their capabilities in a short span of time. Accordingly, the level of collaboration for cyber defense among the regulated entities needs enhancement on a priority basis.



2.4.2. Holistic

The principle of holistic approach to cybersecurity is based on the philosophy that people, processes, and technology should work together to create a layered defense against cyber threats. This is to establish that systems are designed to protect confidentiality, integrity and availability of data by reducing cyberattack surface, improving the information security design of the systems, enhancing cybersecurity processes, and inculcating cybersecurity culture.

2.4.3. Agile and Adaptive

The prominent characteristics of cyber risks which differentiate it from other types of risks are dynamism and velocity. The said risks change constantly and continue to evolve, which makes its treatment challenging. Therefore, agility and adaptiveness are the essential prerequisites for treating the said risks.

2.4.4. People Centric

The human element remains one of the most exploitable vulnerabilities in the cyber threat landscape, frequently serving as the entry point for sophisticated attacks. Technical controls, no matter how advanced, can be rendered ineffective in the absence of an ingrained culture of cyber resilience. Embedding this culture requires sustained efforts to enhance cyber awareness and accountability across all levels of an institution—an imperative that must be treated as a core pillar of any comprehensive cybersecurity framework.

CHAPTER 3: STRATEGIC PRIORITIES

The strategic principles are supported by five strategic priorities. Each strategic priority represents a significant focus area and line of effort that provides an essential component required to achieve the ultimate vision which leads to a cohesive and comprehensive framework for creating a secure and trusted cybersecurity posture of the regulated entities.

3.1. STRENGTHEN

PRIORITY # 1

Strengthening Cyber Resilience of the Regulated Entities

Develop and implement measures to strengthen cyber resilience of regulated entities

One of the fundamental priorities of this strategy is to strengthen cyber defense and improve the cyber resilience of the regulated entities. It is aimed to raise the cybersecurity readiness and protect the systems and networks of the regulated entities. This can be accomplished by developing modern and advance cybersecurity defenses that enhance mechanisms to address and detect potential cyber-attacks and threats in a comprehensive and accurate manner. The systemically important infrastructure of the banking system remains vital focus area to enhance the cyber resilience capabilities. Improving cyber defense capabilities may involve incurring significant financial outflows which may be challenging for smaller regulated entities. Therefore, a risk-based approach to cyber defense would be adopted, where investment in such capabilities would be risk-based. Further, appropriate cyber hygiene would be a must for all regulated entities.

Actions	**Outcomes**
✓ Develop and implement a cyber-testing framework that simulates real-world threats through controlled cyber-attacks.	➢ Improvement in cyber resilience of the regulated entities.
✓ Enhance, update and consolidate cybersecurity regulations by using tiers to characterize the rigor of cybersecurity risk governance and management practices	➢ Regulated entities' efforts / investment in cyber defense based on their cyber risk exposures.
✓ Develop and implement a cybersecurity maturity assessment mechanism for the regulated entities.	➢ Development of cyber defense capabilities of the regulated entities with respect to the evolving threat landscape.
✓ Enhance the disaster recovery plans of the regulated entities to incorporate cyber risk scenarios.	➢ Preparedness of the regulated entities against cyber-attack scenarios.
✓ Prepare a roadmap for implementation of Zero Trust Architecture for critical infrastructure of the banking system.	

Improve Cyber Resilience of Financial Market Infrastructures

Improve the Cyber Resilience of systemically important payment systems and Financial Market Infrastructures

Safe and efficient functioning of the systemically important payment systems and Financial Market Infrastructures (FMIs) are essential for financial stability and economic growth. Due to the significant interconnectedness and dependency of the banking system on these entities, they are often target of choice for the sophisticated threat actors who want to bring systemic disruptions to the banking system. Further, these entities could themselves become propagation channels for malware infiltration into other entities of the ecosystem. Therefore, it is essential for these entities to always maintain an elevated cybersecurity posture.

Actions	**Outcomes**
✓ Define risk-based cybersecurity regulatory expectations for the FMIs	➢ Improvement in cybersecurity posture of systemically important FMIs
✓ Designate systemically important payment systems and assess their cyber resilience	➢ FMIs' efforts / investment in cyber defense based on their cyber risk exposures.
✓ Enhance FMIs business continuity plans to achieve two-hour recovery time objective and align with international standards for FMIs and guidance on their cyber resilience	
✓ Assess all critical service providers of the FMIs	

PRIORITY # 2

3.2. MATURE

Mature Cybersecurity Governance of the Regulated Entities

One of the prime reasons for a weak cybersecurity posture is ineffective cyber governance practices. Cyber risks are relatively new types of risks for the board of directors and senior management of the regulated entities. Further, the dynamic nature, high velocity and technical characteristics make it difficult for the stakeholders to properly understand its gravity and necessity of required actions. Resultantly, the limited deliberations on the said risks are noted at senior forums of some regulated entities. Furthermore, the gravity and vitality of the said risks are often understood when the entities are subject to high impact cyber incidents. Without effective cyber governance, appropriate cyber resilience capabilities would never be achieved. Cyber risks have now become a significant part of the risk profile of regulated entities, and the share of the said risks is increasing with the passage of time. Therefore, it is vital for regulated entities to improve their cyber governance practices to achieve cyber resilience capabilities.

Actions	**Outcomes**
✓ Strengthen regulatory cybersecurity governance expectations including role of the Chief Information Security Officer (CISO) and Chief Information/Technology Officer (CIO/CTO)	➢ Improvement in cybersecurity governance
✓ Enhance cyber risk understanding of the board of directors and senior management of the regulated entities	➢ Better understanding of the board of directors and senior management of the regulated entities regarding cyber risks

3.3. ENHANCE

PRIORITY # 3

Enhance Collaborations and Partnerships

Enhance Collaboration and Partnerships among regulated entities and related stakeholders for improving cyber resilience

The cyber resilience of the regulated entities could never be effective if its stakeholders do not collaborate. An effective cyber risk management strategy would be incomplete without situational and threat awareness. Therefore, it is vital for the regulated entities and the related stakeholders to timely share the threat intelligence among themselves for mitigation. Some progress has been made in this area including incident response support by the SBP for cyber incidents occurring at the regulated entities; however, there is a need for further enhancement. Often similar tactics are being used to conduct cyber offensive activities against different entities. Therefore, it is important to leverage partnerships with other domestic and international regulators and agencies to improve cyber resilience of the regulated entities. Timely reporting of cyber incidents to the regulatory authorities helps in timely containing system wide risks and improved response and recovery of the affected entity.

Actions	**Outcomes**
✓ Develop and implement a threat intelligence and information sharing platform for the regulated entities	➢ Improved response of the regulated entities after cyber-attacks
✓ Develop and implement a standardized IT/cyber incident reporting framework for the regulated entities	➢ Ability to analyze and correlate IT/cyber incident data for improvement in cyber resilience of the regulated entities
✓ Develop and implement a multi-year cyber exercising program for the regulated entities	➢ Enhancement in system-wide incident response capabilities
✓ Establish FinCERT after implementing the threat intelligence and information sharing platform	

PRIORITY # 4

3.4. DEVELOP

Develop Cyber Workforce

Developing Cyber Workforce for the Regulated Entities

The investment in cyber defense would be futile in the absence of a quality cyber workforce. The availability of cybersecurity human resources is a global challenge, which also echoes among regulated entities. There is a dearth of skilled cybersecurity workforce in the country. The regulated entities are significantly dependent on the third-party cybersecurity firms for provision of cyber related services. These firms are not regulated by the SBP, which makes delivery of quality services challenging. With the increase in digital footprint of the regulated entities and advent of additional players, the requirement of cyber workforce would only increase. However, so far neither any consolidated formal assessment of required skills was carried out nor any program / mechanism exists to bridge the widening gap in future.

Actions	**Outcomes**
✓ Conduct a survey to quantify the cyber skills gap of the regulated entities	➢ Information about the cyber skills gap of the regulated entities
✓ Develop competency roadmap and training program to address the cyber skills gap	➢ Reduction in cyber skills gap of the regulated entities

3.5. EVOLVE

PRIORITY # 5

Evolve the Cybersecurity Strategy and Programs

Evolving the Cybersecurity Strategy and Programs in Response to External Trends

Cyber risks are dynamic and complex, with high velocity and adaptability. With the enhancement in the cyber defense, the threat actors rapidly change their tactics, tools and techniques. Therefore, it is vital for an effective cybersecurity strategy to continuously evolve with the focus on threat landscape and other changing dynamics. A static cybersecurity strategy and program would never be effective in providing the required deterrence and response capabilities. The adaptability of the cyber programs of the regulated entities needs to be further enhanced to be more effective. There has been a considerable change in the threat landscape where the threat actors are now increasingly targeting the third party service providers of regulated entities, as a means to infiltrate the cyber defenses of other stakeholders of the industry. Therefore, there is a need to enhance the third party risk management of the regulated entities.

Actions	**Outcomes**
✓ Establish regular review of the cybersecurity strategy to be responsive to emerging threats	➢ Effective cybersecurity strategy
✓ Assess the need for futureproofing with advisories on emerging technologies	➢ Awareness of opportunities and risk pertaining to emerging technologies
✓ Strengthening oversight and supervisory expectations for third-party risk management	➢ Improved third-party risk management practices of the regulated entities
✓ Develop an annual cyber threat landscape report of the regulated entities	➢ Improved awareness regarding changing cyber threat landscape

Glossary[1]

Advance Persistent Threat (APT): A threat actor that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple threat vectors. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to execute its objectives.

Cyber Incident: A cyber event that adversely affects the cyber security of an information system or the information the system processes, stores or transmits whether resulting from malicious activity or not.

Cyber Resilience: The ability of an organization to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents.

Cyber Risk: The combination of the probability of cyber incidents occurring and their impact.

Cyber Security: Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.

Cyber Threat: A circumstance with the potential to exploit one or more vulnerabilities that adversely affects cyber security.

Denial of Service (DoS): Prevention of authorized access to information or information systems; or the delaying of information system operations and functions, with resultant loss of availability to authorized users.

Distributed Denial of Service (DDoS): A denial of service that is carried out using numerous sources simultaneously.

Financial Market Infrastructures (FMIs): an FMI is defined as a multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions.

FinCERT: Financial sector Computer Emergency Response Team of appropriately skilled and trusted members that handles incidents during their life cycle.

Malware: Software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to entities or their information systems.

Ransomware: Malware that is used to commit extortion by impairing the use of an information system or its information until a ransom demand is satisfied.

Regulated Entities: Entities regulated by the State Bank of Pakistan including Banks, Digital Banks, Microfinance Banks, Electronic Money Institutions, Payment System Operators and Payment Service Providers, Credit Bureaus etc. as updated from time to time.

Supply chain attack: Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software,

[1] A number of key definitions of relevance to the Strategy are taken from the FSB Cyber Lexicon (2023)

operating systems, peripherals (information technology products) or services at any point during the life cycle.

Threat Actor: An individual, a group or an organization believed to be operating with malicious intent.

Vulnerability: A weakness, susceptibility or flaw of an asset or control that can be exploited by one or more threats.

Zero Trust Architecture: An evolving set of cybersecurity paradigms that move defenses from static, network- based perimeters to focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned).

Zero-day vulnerability: A previously unknown vulnerability within an information system.