Consultation Paper

Principle-Based Guidelines on Cyber Security and Cyber Resilience for all Regulated Entities (REs) in IFSC

September 28, 2024

About IFSCA

1. International Financial Services Centres Authority (IFSCA) was established as a unified regulator for India's maiden international financial services centres i.e. GIFT IFSC under the International Financial Services Centres Authority Act, 2019. IFSCA has been entrusted with the development and regulation of financial products, financial services and financial institutions in the GIFT IFSCs in India, cutting across the realms of banking, capital markets, fund management, insurance, pensions, ancillary services and more.

Background

2. The Government of India notified the establishment of GIFT IFSC in the year 2015, with the aim of making India a global leader in the realm of international financial services. The GIFT IFSC jurisdiction was initially regulated by the Indian financial sector regulators like the Reserve Bank of India, the Securities and Exchange Board of India, the Insurance Regulatory and Development Authority of India, and the Pension Fund Regulatory & Development Authority. Entities set up in GIFT IFSC were following the regulations of the respective domestic regulators. On October 01, 2020, IFSCA became the sole unified regulator for all financial products and services in GIFT IFSC.

Entities in GIFT IFSC

3. In the short period of its existence, GIFT IFSC has evolved into a dynamic jurisdiction with several types of entities providing a wide gamut of financial, technological and ancillary services. Notably, GIFT IFSC hosts 29 banks, 5 market infrastructure institutions, 116 fund management entities, 12 IFSC insurance offices, 72 ancillary service providers and 3 global in-house centres, among a total of over 640 entities to whom registrations were granted by IFSCA till the end of June 2024[1].

4. The entities in GIFT IFSC perform a wide range of activities at different scales, leading to great variance in the information systems and technology deployed and cyber risk profile. Further, the entities in GIFT IFSC operate in different forms – as a branch of an overseas entity, as a wholly owned subsidiary incorporated in GIFT IFSC - with their parent entities belonging to different jurisdictions. Some of the entities which are operating in the form of a branch are also bound by the regulations of the regulators in their home jurisdiction.

Challenges

5. The diverse range of regulated entities and activities in GIFT IFSC has presented a unique challenge to IFSCA in the development of a uniform regulatory framework on cybersecurity and cyber resilience. In this backdrop, in order to develop an overarching framework on cyber security and cyber resilience and taking into account factors like ease of doing business and cost of compliance, IFSCA has deemed it prudent to adopt a principle-based approach to begin with. The rationale for the same is that such an approach is best suited to providing a consistent, proportional and risk-based regulatory framework, based on global best practices, for the management of cyber risk in GIFT IFSC.

[1] See IFSCA Bulletin for April-June 2024.

Approach

6. IFSCA has constituted the Cyber Security Advisory Committee (CSAC), chaired by Dr. Sanjay Bahl, Director General, Indian Computer Emergency Response Team (CERT-In) in August 2023, in order to provide recommendations, guidance and lend technical expertise to IFSCA, in fulfilling its mandate of improving the cyber resilience of entities in GIFT IFSC. CSAC comprises of eminent experts from the domains of cyber security, computer science, law, and seasoned officers with rich governmental and regulatory experience.

Objective

7. The objective of this consultation paper is to seek comments/ views from different stakeholders in GIFT IFSC to put in a principle based place framework on cyber security and cyber resilience.

Public comments

8. Comments and suggestions from the public are invited on the consultation paper on **"Guidelines on Cyber Security and Cyber Resilience for Regulated Entities in IFSC"** as placed at Annexure 1.

   Comments may be sent by email to Mr. Praveen Kamat, General Manager & Chief Information Security Officer at praveen.kamat@ifsca.gov.in , with a copy to Mr. Chintan Panchal, Manager at chintan.panchal@ifsca.gov.in and Mr. Abhinav Kadyalwar, Assistant Manager at abhinav.sk@ifsca.gov.in latest by October 19, 2024.

9. The comments may be provided in the following format (MS Word or MS Excel only)

Name and Details of the Person/ Entity [Organisation name (if applicable), Contact No., Email address]					
Sr. No.	Paragraph No. (as per Annexure 1)	Regulation No.	Comments/ Suggestions / Proposed Amendment	Detailed Rationale	Other Supporting Information

***

Annexure 1

Guidelines on Cyber Security and Cyber Resilience for all Regulated Entities in IFSC

1. As the international financial services centre continues to evolve as a global financial hub, the sophistication of cyber threats targeting financial entities is also expected to grow. In such an international jurisdiction, where institutions cater to a diverse global client base, maintaining robust cyber security becomes fundamental. The ability of financial entities to protect their IT systems from being compromised by threat actors—whether through fraudulent financial transactions, the exfiltration of sensitive data, or the disruption of critical IT infrastructure—directly impacts the trust placed in the jurisdiction.

2. Consequently, cyber security is not just a necessity but a foundational pillar for ensuring the stability, resilience, and credibility of the financial services offered within the GIFT IFSC. These Guidelines on cyber security and cyber resilience intend to serve as IFSCA's broad expectations from its Regulated Entities ("REs"). The implementation of these Guidelines shall be done in accordance with the **principle of proportionality**, considering the scale and complexity of operations, the nature of the activity the entity is engaged in, its interconnectedness to the financial ecosystem and the corresponding cyber risks the entity is exposed to. These major components of the guidelines are as follows.

   I. Governance
   II. Cyber security and cyber resilience framework
   III. Third Party Risk Management
   IV. Communication & Awareness
   V. Audit

I. Governance

3. The entity shall have adequate governance mechanism with clear set of roles and responsibilities to manage cyber risk. The cyber governance stakeholders may include the following.

   i. Governing Body (Governing Body may be in the form of Board of Directors (BoD)/Partners/ Dedicated officer in the case of branch).
   ii. IT Strategy Committees or different committee for the same purpose with different nomenclature
   iii. Chief Executive Officer (CEO)
   iv. Chief Information Security Officers (CISOs)
   v. Chief Technology Officers (CTOs)
   vi. IT Steering Committees (operating at an executive level and focusing on priority setting, resource allocation and project tracking)
   vii. Chief Risk Officer and Risk Committees
   viii. Any other committee as decided by the Governing Body

4. REs shall ensure that its Governing Body and senior management possesses sufficient expertise and knowledge to effectively understand and manage cyber risk. The Governing Body and senior management shall set the tone at the highest levels and cultivate a strong culture of cyber risk management and awareness at all levels of staff deployed within the entity.

5. REs shall designate a senior official as CISO or a senior official or management personnel (henceforth, referred to as the “Designated Officer”) whose function would be :

   a. to assess, identify and reduce cyber security risks,
   b. respond to cyber incidents,
   c. establish appropriate standards and controls, and

d. direct the establishment wherever deemed fit

e. oversee implementation of processes and procedures as approved by the Governing Body of REs.

6. REs should have a well-defined and coherent strategy to manage cyber risk, including third party risks, which is aligned with their overall business strategy. This strategy should define clear information security objectives.

II. <u>Cyber security and cyber resilience framework</u>

7. REs may formulate their cyber security and cyber resilience framework to maintain the <u>Confidentiality, Integrity and Availability</u> of their information assets. The said framework should cover the following:

   i. Prioritise the security and efficiency of its operations.

   ii. Define how the entity's cyber resilience objectives and cyber risks tolerance are determined.

   iii. Outline its people, process and technology requirements for managing cyber risks and timely communication to collaborate with relevant stakeholders.

   iv. Take an integrated and comprehensive view of the potential cyber threats it faces.

   v. The framework should aim to maintain and promote the entity's ability to anticipate, withstand, contain, and recover from cyber-attacks.

   vi. The framework should be reviewed and updated periodically to ensure that it remains relevant and in sync with ground reality.

The Governing Body shall ensure that the framework is aligned with the entity's overall risk management framework.

8. REs may formulate Information Security (IS) Policy as part of the Framework with the following basic principles.

   a) Identification and Classification of Information Assets

      i. REs shall maintain detailed inventory of information assets, including both logical (data, software) and physical (hardware) components, including system configurations their interconnections with internal and external systems, with distinct and clear identification of the asset.

      ii. REs shall carry out a risk assessment of those assets and classify assets based on their business criticality, sensitivity of data they hold, and potential impact on other systems if compromised.

      iii. REs shall identify and classify its business functions and supporting processes based on their criticality to overall operations and potential impact on performance. This classification shall guide the prioritization of security measures across protective, detective, response, and recovery efforts, focusing on mitigating risks associated with the most critical functions and processes.

   b) Protection

      REs shall implement appropriate security controls, aligned with best practices and cyber resilience standards, to minimize the likelihood and impact of cyberattacks on critical business functions, information assets, and data. These controls must be proportional to the entity's threat landscape, systemic role in the financial system, and risk tolerance. These controls shall be selected with cognizance of potential compromise of technology, people, and processes.

   c) Access Control

i. The REs shall manage access rights to information assets and their supporting systems on a 'need-to-know' basis following the principle of 'least privilege', i.e. to prevent unjustified access to a large set of data or to prevent the allocation of combinations of access rights that may be used to circumvent controls (principle of 'segregation of duties').

ii. The REs shall enforce authentication methods that are sufficiently robust to adequately and effectively ensure that access control policies and procedures are complied with.

d) Physical Security

The Confidentiality, Integrity, and Availability of information can be impaired through physical access and damage or destruction to physical components. REs are required to create a secure environment for physical security of IT Assets such as secure location of critical data, restricted access to sensitive areas like data center, etc.

e) Recovery

The REs shall have recovery policies and procedures to maximise their abilities to provide services on an ongoing basis and to limit losses in the event of severe business disruption.

f) Incident Management

The IS Policy should define what constitutes an incident. REs shall develop and implement processes for preventing, detecting, analysing and responding to information security incidents.

g) Audit trail

REs shall ensure that audit trails exist for IT assets satisfying its business requirements including regulatory and legal requirements, facilitating audit, serving as forensic evidence when required and assisting in dispute resolution.

9. The IS policy shall also include various other components including but not limited to hardening of devices, data classification, network security, data security, patch management, disposal of systems and any other policies that may help them to achieve the objectives of cyber security and cyber resilience framework and risk Management Framework.

III. Third Party Risk Management

10. The REs shall adopt a collaborative security approach by forging strong agreements with third-party vendor/external partner. REs should outline shared expectations for data security, incident reporting, and adherence to relevant security standards.

11. The REs shall conduct continuous vigilance of third-party vendor/external partner. REs should proactively monitor their partner network through various methods like audits, reviews, and feedback mechanisms to detect vulnerabilities or compliance gaps.

12. The REs should implement clear communication channels and escalation procedures for addressing any identified risks or non-compliance with partners promptly and effectively.

IV. Education & Communication

13. The REs shall provide regular cyber security training for employees on topics like phishing awareness, social engineering, password hygiene, and incident reporting procedures.

14. The REs shall establish clear and accessible channels for employees to report suspicious activity, vulnerabilities, and potential cyber incidents.

V. Audit

15. RE's governance, systems and processes for its cyber risks should be audited on a periodic basis by CERT-In empanelled auditors to provide independent assurance of their effectiveness to the Governing Body and the senior management. The auditors shall be independent from the REs. The frequency and focus of such audits should be commensurate with the relevant cyber risks the REs faces.

***