Comments from Central Bank of Jordan

1. **CBJ supports the 46 effective practices mentioned in the document of CIRR. CBJ suggests adding the below practices for their value in cyber incident response and recovery:**

   - Conducting bilateral agreements with national law enforcement agencies specialized in forensic investigations to support extended cyber forensic investigations with legal mutual assistance, collaboration in organization capacity building and threat intelligence sharing.
   - Reporting criminal incidents to law enforcement. It is important that potential or actual cyber-crime is reported to relevant law enforcement agencies for the purpose of National Electronic Crime Law enforcement.
   - Conducting sessions to test real simulated cyber-attack scenarios of CIRR plan including all employee roles listed in the plan and figure out recommendations to enhance the response in real scenarios.
   - Planning information share with Media and Press in the case of Cyber incident and how news will be announced to public and at what stage in the way organization business operations and reputation are saved.

2. **CBJ answered Part1 in the section "Questions for public consultation", titled "General", in CIRR document. Kindly find the answers below.**

General

1.1. **Have you learnt any lessons from the COVID-19 pandemic and related cyber activity that will contribute to your cyber incident response and recovery practices?**

Pandemic scenario must be appended to the CIRR plan since this scenario may push work to be accomplished remotely making the attack surface of an organization a target for intensive threat and threat actors. Thus, staff must have procedures Witten down for forensic investigation while working remotely.

1.2. **To whom do you think this document should be addressed within your organisation?**

Information security and cyber security personnel.

1.3. **How does your organisation link cyber incident response and recovery with the organisation's business? Does your organisation follow international standards or common frameworks? If so, which international standards or common frameworks?**

International standards such as ISO 27000 series and NIST publications are the most relied on standards which are tailored to satisfy organization business needs and objects. Incident is categorized according to the targeted system and the criticality of its business operations.

1.4. **Does your organisation structure its cyber incident response and recovery activities along the seven components set out in the FSB toolkit? Please describe any additional components your organisation considers.**

Yes, Organization CIRR plan covers the 7 components of FSB toolkit. It does not cover all tools within one component.

1.5. Based on your organisation's experience, please provide any additional effective practice(s) for any of the tools. Please list the number of the tool (e.g. Tools 1 – 46) and describe the effective practice(s).

- **Governance**: Roles, responsibilities and accountabilities for CIRR, Human resources, Metrics.
- **Preparation**: Scenario planning and stress testing, Scenario planning and stress testing, Disaster recovery sites, Forensic Capabilities, Technology solutions and vendors.
- **Analysis**: Cyber incident taxonomy, System and transaction logs, Trusted information sources
- **Mitigation**: Containment, Eradication.
- **Restoration**: Data recovery
- **Improvement**: Exercises, tests and drills, External events and sources, Post-incident analysis.
- **Coordination and communication**: Trusted information sharing, Trusted communication channels, Cyber incident reporting.

1.6. Based on your organisation's experience, please provide additional examples of effective practices listed in the boxes (e.g. Boxes 1-6).

Box 1: Examples of metrics used by industry

- Metrics to measure impact of a cyber-incident: Time needed to restore business service

Box 3: Examples of CIRR taxonomies

- Information to be used when describing cyber incidents: Compromised system criticality

1.7. What role, if any, should authorities play in supporting an organisation's cyber incident response and recovery activities?

Mutual Legal Assistance, Information sharing.