Cyber Security Self-Assessment Questionnaire

NOTE: This complete self-assessment may not be appropriate for use by all entities. It is not intended to function as a benchmark for all regulated entities, rather to be adaptable and tailored to fit the cyber security risk environment of a given entity.

Entities should rate their current individual cyber security framework components on a scale of 1 to 4 and provide sufficient justification in all circumstances. Below is a suggested definition of each of the ratings.

- **4 – Fully Implemented:** The entity has fully implemented the principles. There is evidence to substantiate the assessment. There are no outstanding issues identified.

- **3 – Largely Implemented:** The entity has largely, but not fully implemented the principles across its enterprise, or there may be some minor outstanding issues identified.

- **2 – Partially Implemented:** The entity has partially implemented the principle, major aspects of the implementation remain, and there may be some significant outstanding issues identified.

- **1 – Not Implemented:** The entity has not yet implemented this practice.

- **N/A:** If the entity determines the rating 1 to 4 is not applicable, the entity is encouraged to provide sufficient justification for this selection.

The self-assessment template can be found on the following pages.

1. Organization and Resources

Item	Criteria	Rating	Rating Rationale and Description (Control Design and Effectiveness)	Action Plan and Target Date(s) for Full Implementation
1.1	The entity has clearly established accountability and ownership of the cyber security framework.			
1.2	The entity has assigned responsibility for the management of cyber security.			
1.3	The entity has threat intelligence, threat management and incident response procedures.			
1.4	The entity has sufficient skilled staff for the management of cyber security.			
1.5	The entity has a plan to provide ongoing technical training for cyber security.			
1.6	Cyber security training and awareness is provided to new and existing employees.			

2. Cyber Risk and Control Assessment

Item	Criteria	Rating	Rating Rationale and Description (Control Design and Effectiveness)	Action Plan and Target Date(s) for Full Implementation
2.1	The entity has a process to conduct regular and comprehensive cyber risk assessments that consider people (i.e. employees, clients and other external parties), processes, data and technology.			
2.2	The entity assesses and takes steps to mitigate potential cyber risk arising from its critical IR service providers.			
2.3	The entity conducts vulnerability hardware and software scans and testing for client, server, and network infrastructure to identify security control gaps.			
2.4	The entity conducts penetration testing of the network to identify security control gaps.			

3. Situational Awareness (Identify)

Item	Criteria	Rating	Rating Rationale and Description (Control Design and Effectiveness)	Action Plan and Target Date(s) for Full Implementation
3.1	The entity maintains a current knowledge base of its users, devices, applications and their relationships, including but not limited to: - software and hardware asset inventory, Network maps; and - network utilization and performance data.			
3.2	The entity centrally stores a history of security event information.			
3.3	The entity monitors and tracks cyber security incidents in the financial services industry and more broadly as relevant, through participation in industry programs (e.g. Canadian Cyber Incident Response Centre).			
3.4	The entity subscribes to industry research and other relevant publications on cyber security.			

4. Threat and Vulnerability Risk Management (Protect and Detect)

Item	Criteria	Rating	Rating Rationale and Description (Control Design and Effectiveness)	Action Plan and Target Date(s) for Full Implementation
Data Loss Detection / Prevention				
4.1	The entity has implemented tools to: - prevent unauthorized data leaving the enterprise; - monitor outgoing high risk traffic to detect unauthorized data leaving the entity; - safeguard data in online and offline stores (e.g. desktop, laptops, mobile devices, removable devices, and removable media); and - safeguard data.			
Cyber Incident Detection & Mitigation				
4.2	The entity has implemented the following security tools and provides for their currency, automated updates, and enterprise-wide application: - intrusion detection / protection systems; web application firewalls; - anti-virus; - anti-spyware; - anti-spam; and - other (please describe).			

Item	Criteria	Rating	Rating Rationale and Description (Control Design and Effectiveness)	Action Plan and Target Date(s) for Full Implementation
Software Security				
4.3	The entity has a process to obtain, test and automatically deploy security patches and updates in a timely manner based on criticality.			
4.4	The entity considers and mitigates cyber risk arising from use of any unsupported software.			
4.5	The entity has a process to confirm successful deployment of security patches and resolve update failures.			
4.6	The entity’s internally or externally developed software is subject to secure system design, coding and testing standards that incorporate appropriate cyber security controls.			
Network Infrastructure				
4.7	The entity has implemented network monitoring and protection.			
4.8	The entity is able to rapidly and remotely isolate, contain or shut down compromised operations.			
4.9	The entity has implemented processes and tools to secure mobile devices (including personal cell phones and tablets) and wireless networks.			

Item	Criteria	Rating	Rating Rationale and Description (Control Design and Effectiveness)	Action Plan and Target Date(s) for Full Implementation
Standard Security Configuration and Management				
4.10	The entity documents, implements and enforces security configuration standards to all hardware and software assets on the network.			
Network Access Control & Management				
4.11	The entity has the ability to automatically detect and block unauthorized network access (e.g. including wired, wireless and remote access).			
4.12	The entity applies authentication mechanisms to manage user identities and access.			
4.13	The entity controls and manages the use of administrative privileges.			
Third Party Management				
4.14	The entity considers cyber security risk as part of its due diligence process for material outsourcing arrangements and critical IT service providers, including related subcontracting arrangements.			
4.15	Contracts for all material outsourcing arrangements and critical IT service providers include the provision for safeguarding the entity’s information.			

Item	Criteria	Rating	Rating Rationale and Description (Control Design and Effectiveness)	Action Plan and Target Date(s) for Full Implementation
4.16	The entity has processes in place to ensure the timely notification of a cyber-incident from service providers with whom the entity has one or more material outsourcing arrangements, or critical IT service providers.			
Customers and Clients				
4.17	Cyber security awareness and information is provided to customers and clients.			
4.18	The entity has taken additional actions to protect its customers and clients confidential personal information.			

5. Cyber Security Incident Management (Respond and Recover)

Item	Criteria	Rating	Rating Rationale and Description (Control Design and Effectiveness)	Action Plan and Target Date(s) for Full Implementation
5.1	The entity is able to respond rapidly to cyber security incidents.			
5.2	The entity has documented procedures for monitoring, analyzing and responding to cyber security incidents.			
5.3	The entity has an internal communication plan to address cyber security incidents that includes communication protocols for staff and other key internal stakeholders.			
5.4	The entity has an external communication plan to address cyber security incidents that includes communication protocols and draft pre-scripted communications for key external stakeholders (i.e. customers, media, critical service providers, etc.).			
5.5	The entity’s incident management process is designed to ensure that the following tasks are fully completed before an incident can be formally closed: - Recovery from disruption of services from the cyber security incident; - Assurance of systems’ integrity following the cyber security incident; and - Recovery of lost or corrupted data due to the cyber security incident.			
Item	**Criteria**	**Rating**	**Rating Rationale and Description (Control Design and Effectiveness)**	**Action Plan and Target Date(s) for Full Implementation**

5.6	The entity has an established post incident review process that: - is completed for material cyber security incidents; includes appropriate cyber forensic investigations; - chronicles the events leading up to, during and following the cyber security incident; - identifies the root cause and highlights control deficiencies; - assesses any breakdowns in the incident management process; and - establishes a plan of action to address identified deficiencies.			

6. Cyber Security Governance

Item	**Criteria**	**Rating**	**Rating Rationale and Description (Control Design and Effectiveness)**	**Action Plan and Target Date(s) for Full Implementation**
Cyber Security Policy & Strategy				
6.1	The entity has established an cyber security policy with supporting procedures in place that set forth how the entity will identify and manage its cyber security risks.			
6.2	The roles and responsibilities are clearly described within the cyber security policy.			
Second Line of Defence (e.g. Risk Management)				
6.3	The entity has utilized scenario analysis to consider a material cyber attack, mitigating actions, and identify potential control gaps.			
Compliance/Internal Audit				
6.4	The frequency of cyber security audits is determined by and is consistent with the risk of a cyber attack.			
6.5	The entity assess both the design and effectiveness of the cyber security framework annually.			
External Benchmarking				
6.6	The entity has conducted an external benchmarking review of its cyber security framework.			