Office of the Superintendent of Financial Institutions Canada
Bureau du surintendant des institutions financières Canada

MEMORANDUM

Date: October 27, 2013

To: Federally Regulated Financial Institutions

Subject: Cyber Security Self-Assessment Guidance

The increasing frequency and sophistication of recent cyber-attacks has resulted in an elevated risk profile for many organizations around the world. As a result, significant attention has recently been paid to the overall level of preparedness against such attacks by these organizations, including financial institutions, critical infrastructure providers, regulatory bodies, the media and the public at large.

Cyber security is growing in importance due to factors such as the continued and increasing reliance on technology, the interconnectedness of the financial sector, as well as the critical role that federally regulated financial institutions (FRFIs) play in the overall economy. OSFI thus expects FRFI Senior Management to review cyber risk management policies and practices to ensure that they remain appropriate and effective in light of changing circumstances and risks.

OSFI recognizes that many FRFIs may have already conducted, or may be in the process of conducting, an assessment of their current level of preparedness. With this in mind, OSFI believes that they could benefit from guidance related to such self-assessment activities. Consequently, it is sharing the annexed cyber security self-assessment guidance to assist FRFIs in their self-assessment activities.

FRFIs are encouraged to use this template or similar assessment tools to assess their current level of preparedness, and to develop and maintain effective cyber security practices. OSFI does not currently plan to establish specific guidance for the control and management of cyber risk. Notwithstanding, and in line with its enhanced focus on cyber security as highlighted in its Plan and Priorities for 2013-2016, OSFI may request institutions to complete the template or otherwise emphasize cyber security practices during future supervisory assessments.

Further questions can be directed to Mohamad Al-Bustami, Managing Director, Technology Risk Division, at (416) 973 2088 or TRD@osfi-bsif.gc.ca.

Mark Zelmer
Deputy Superintendent

OSFI BSIF
255 Albert Street
Ottawa, Canada
K1A 0H2

www.osfi-bsif.gc.ca

Canada

Annex - Cyber Security Self-Assessment Guidance

This self-assessment template sets out desirable properties and characteristics of cyber security practices that could be considered by a FRFI when assessing the adequacy of its cyber security framework and when planning enhancements to its framework. FRFIs are encouraged to reflect the current state of cyber security practices in their assessments rather than their target state, and consider cyber security practices on an enterprise-wide basis. If a FRFI employs relevant practices that are not described in the template, it is encouraged to list them and their related assessments.

OSFI suggests that FRFIs rate their current degree of maturity on a 1 to 4 scale and provide sufficient justification in all circumstances. A suggested definition of each of the ratings is provided below.

4 – Fully Implemented	The FRFI has fully implemented the principles across its enterprise. There is evidence to substantiate the assessment. There are no outstanding issues identified (e.g. issues raised through self-assessment, or by groups such as operational risk management, Internal Audit, supervisors or other third parties).
3 – Largely Implemented	The FRFI has largely, but not fully implemented the principles across its enterprise, or there may be some minor outstanding issues identified (e.g. issues raised through self-assessment, or by groups such as operational risk management, Internal Audit, supervisors or other third parties).
2 – Partially Implemented	The FRFI has partially implemented the principle, major aspects of the implementation remain, and there may be some significant outstanding issues identified (e.g. issues raised through self-assessment or by groups such as operational risk management, Internal Audit, supervisors or other third parties).
1 – Not Implemented	The FRFI has not yet implemented this practice.
N/A	If the FRFI determines the rating 1 to 4 is not applicable, the FRFI is encouraged to provide sufficient justification for this selection.

The self-assessment template can be found below:

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 FRFI has clearly established accountability and ownership of, and financial resources for, the cyber security framework[1].			
1.2	The FRFI has assigned specific roles and responsibilities for the management of cyber security, and these individuals have sufficient delegated operational authorities.			
1.3	The FRFI has a centrally managed group of cyber security specialists that is responsible for threat intelligence, threat management and incident response.			
1.4	The FRFI provides 24/7 identification and response capabilities for the management of cyber security.			
1.5	The FRFI has sufficient number of skilled staff for the management of cyber security.			
1.6	The cyber security specialists are subject to enhanced background and security checks.			
1.7	The FRFI has a formalized plan to provide ongoing technical training to cyber security specialists.			
1.8	Cyber security training is provided to new and existing employees.			
1.9	Cyber security awareness is provided to all employees.			

[1] Cyber Security Framework: A complete set of organizational resources including policies, staff, processes, practices and technologies used to assess and mitigate cyber risks and attacks.

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 FRFI has a process to conduct regular and comprehensive cyber risk assessments that consider people (i.e. employees, customers and other external parties), processes, data, technology across all its business lines and geographies.			
2.2	The FRFI assesses and takes steps to mitigate potential cyber risk arising from its outsourcing arrangements deemed material under OSFI's Guideline B-10.			
2.3	The FRFI assesses and takes steps to mitigate potential cyber risk arising from its critical IT service providers.			
2.4	The FRFI's change management risk assessment and due diligence processes consider cyber risk.			
2.5	The FRFI conducts regular vulnerability hardware and software scans and testing for client, server, and network infrastructure to identify security control gaps.			
2.6	The FRFI conducts regular penetration testing of the network boundary (e.g. open network entry and exit points) to identify security control gaps.			
2.7	The FRFI conducts regular testing with its third party cyber mitigating services.			
2.8	The FRFI conducts regular cyber-attack (including Distributed denial-of-service (DDoS)) and recovery simulation exercises.			
2.9	The FRFI considers in its risk assessment the impact of an Internet outage across Canada for an extended period of time.			

3. Situational Awareness

Item	Criteria	Rating	Rating Rationale and Description (Control Design and Effectiveness)	Action Plan and Target Date(s) for Full Implementation
3.1	The FRFI maintains a current enterprise-wide knowledge base of its users, devices, applications and their relationships, including but not limited to • software and hardware asset inventory; • network maps (including boundaries, traffic and data flow); and • network utilization and performance data.			
3.2	The FRFI centrally stores a history of security event information.			
3.3	The FRFI normalizes, aggregates, and correlates security event information.			
3.4	The FRFI conducts automated analysis of security events to identify potential cyber-attacks including DDoS attacks.			
3.5	The FRFI supplements automated analysis of security events by conducting additional expert analysis on security events to identify potential cyber-attacks.			
3.6	The FRFI 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).			
3.7	The FRFI subscribes to industry research on cyber security.			

4. Threat and Vulnerability Risk Management

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 FRFI has implemented tools to • prevent unauthorized data leaving the enterprise; • monitor outgoing high risk traffic to detect unauthorized data leaving the FRFI (e.g. by geography, size, volume, information type); • safeguard data in online and offline stores (e.g. desktop, laptops, mobile devices, removable devices, and removable media); and • safeguard data at rest and in motion.			
4.2	The FRFI has implemented the above controls on an enterprise-wide basis.			
Cyber Incident Detection & Mitigation				
4.3	The FRFI 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; • DDoS protection; and • other (please describe).			
4.4	The FRFI has implemented the above security tools using enhanced detection techniques (e.g. reputation-based and/or behaviour-based).			
Software Security				
4.5	The FRFI has a process to obtain, test and automatically deploy security patches and updates in a timely manner based on criticality.			
4.6	The FRFI considers and mitigates cyber risk arising from use of any unsupported software.			

Item	Criteria	Rating*	Rating Rationale and Description (Control Design and Effectiveness)	Action Plan and Target Date(s) for Full Implementation
4.7	The FRFI has a process to confirm successful deployment of security patches and resolve update failures.			
4.8	The FRFI's internally or externally developed software is subject to secure system design, coding and testing standards that incorporate appropriate cyber security controls.			
4.9	The FRFI implements the above controls on an enterprise-wide basis.			
Network Infrastructure				
4.10	The FRFI has implemented network boundary monitoring and protection.			
4.11	The FRFI segments the enterprise network into multiple, separate trust zones.			
4.12	The FRFI's network infrastructure has multiple layers of defence (e.g. cloud based, ISP, on premise) to mitigate against DDoS attacks.			
4.13	The FRFI is able to rapidly and remotely isolate, contain or shut down compromised operations.			
4.14	The FRFI has implemented processes and tools to secure mobile devices and wireless networks.			
4.15	The FRFI implements the above controls on an enterprise-wide basis.			
Standard Security Configuration and Management				
4.16	The FRFI uses standard secure Operating System images for client, server and network devices.			
4.17	The FRFI follows a formal change management process for security configuration management for all network hardware and software assets on its networks.			
4.18	The FRFI documents, implements and enforces security configuration standards to all hardware and software assets on the network.			
4.19	The FRFI restricts the use of unauthorised/unregistered software and hardware through policy and automated tools, including mobile devices.			

Item	Criteria	Rating*	Rating Rationale and Description (Control Design and Effectiveness)	Action Plan and Target Date(s) for Full Implementation
4.20	The FRFI implements the above controls on an enterprise-wide basis.			
Network Access Control & Management				
4.21	The FRFI has the ability to automatically detect and block unauthorised network access (e.g. including wired, wireless and remote access).			
4.22	The FRFI applies strong authentication mechanisms to manage user identities and access.			
4.23	The FRFI tightly controls and manages the use of administrative privileges.			
4.24	The FRFI implements the above controls on an enterprise-wide basis.			
Third Party Management				
4.25	The FRFI considers cyber security risk as part of its due diligence process for material outsourcing arrangements and critical IT service providers, including related subcontracting arrangements.			
4.26	Contracts for all material outsourcing arrangements and critical IT service providers include the provision for safeguarding the FRFI's information.			
4.27	The FRFI has a process in place to monitor the level of cyber risk preparedness for material outsourcing arrangements and critical IT service providers.			
4.28	The FRFI has processes in place to ensure the timely notification of a cyber incident from service providers with whom the FRFI has one or more material outsourcing arrangements, or critical IT service providers.			
Customers and Clients				
4.29	Cyber security awareness and information is provided to customers and clients.			
4.30	The FRFI has taken additional actions to protect its customers and clients.			

5. Cyber Security Incident Management

Item	Criteria	Rating	Rating Rationale and Description (Control Design and Effectiveness)	Action Plan and Target Date(s) for Full Implementation
5.1	The FRFI's Incident Management Framework is designed to respond rapidly to material cyber security incidents.			
5.2	An appropriate 'command and control' structure with the requisite delegated expenditure authority has been established within the Incident Management Framework to support rapid response to all levels of cyber security incidents.			
5.3	The FRFI has documented procedures for monitoring, analyzing and responding to cyber security incidents.			
5.4	The FRFI change management process has been designed to allow for rapid response and mitigation to material cyber security incidents.			
5.5	The FRFI's Incident Management Framework includes escalation criteria aligned with its cyber security taxonomy.			
5.6	The FRFI has an internal communication plan to address cyber security incidents that includes communication protocols for key internal stakeholders (e.g. relevant business units / call centres, senior management, risk management, Board of Directors, etc.).			
5.7	The FRFI 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.).			
5.8	The FRFI'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
5.9	The FRFI 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 FRFI has established an enterprise-wide cyber security policy[2], with supporting procedures in place that set forth how the FRFI will identify and manage its cyber security risks.			
6.2	The roles and responsibilities of each of the three lines of defence and other stakeholders are clearly described within the cyber security policy.			
6.3	The cyber security policy applies to all of the FRFI's operating groups and entities, including subsidiaries, joint ventures and geographic regions.			
6.4	The FRFI has a defined and consistent common taxonomy for cyber security risk.			

[2] Cyber Security Policy: A set of documented and authorized principles that set out how the Cyber Security Program is to be governed and executed.

Item	Criteria	Rating	Rating Rationale and Description (Control Design and Effectiveness)	Action Plan and Target Date(s) for Full Implementation
6.5	The FRFI's cyber security policy is linked to other relevant Risk Management policies including Information Security, Business Continuity Management, Outsourcing, New Initiatives and Change Management, etc.			
6.6	The FRFI has established a cyber security strategy that is aligned with the FRFI's business strategy.			
6.7	The FRFI has a strategic and tactical cyber security implementation plan that outlines key initiatives and timelines.			
Second Line of Defence (e.g. Risk Management)				
6.8	Relevant risk and control assessments (RCAs) address cyber security risk and mitigating controls.			
6.9	Key risk and performance indicators as well as thresholds have been established for the FRFI's key inherent cyber security risks and controls.			
6.10	The FRFI has utilized scenario analysis to consider a material cyber-attack, mitigating actions, and identify potential control gaps.			
6.11	The second line of defence appropriately assesses cyber security risk within the FRFI's change management process.			
6.12	The second line of defence responsibilities relating to cyber security assessments have been assigned to an independent control group with cyber risk expertise.			
6.13	The second line of defence regularly provides an independent challenge to the various cyber security risk assessments conducted by the first line of defence (e.g. risk assessments within RCSAs, scenario analysis, change management processes, KRIs, threat risk assessments, etc.).			
6.14	The second line of defence monitors and challenges the identification, appropriateness and remediation of actions, resulting from cyber security incidents and risk assessments.			
6.15	The FRFI's operational risk appetite and tolerance considers cyber security risk.			

Item	Criteria	Rating	Rating Rationale and Description (Control Design and Effectiveness)	Action Plan and Target Date(s) for Full Implementation
6.16	The FRFI has considered cyber risk insurance coverage that provides financial mitigation to cyber risk incidents and impacts.			
Internal Audit – Third Line of Defence				
6.17	Internal Audit coverage includes, but is not limited to, all aspects of cyber security within this questionnaire.			
6.18	The frequency of cyber security audits is determined by and is consistent with the risk of a cyber-attack.			
6.19	Internal Audit has assessed or is planning to assess both the design and effectiveness of the cyber security framework.			
6.20	Internal Audit has sufficient resources and expertise to audit the cyber security framework implementation.			
Senior Management Oversight				
6.21	A Senior Management committee has been established that is dedicated to the issue of cyber risk, or an alternative Senior Management committee has adequate time devoted to the discussion of the implementation of the cyber security framework.			
6.22	Senior Management provides adequate funding and sufficient resources to support the implementation of the FRFI's cyber security framework.			
6.23	Processes are in place to escalate breaches of limits and thresholds to Senior Management for significant or critical cyber security incidents.			
6.24	The FRFI's Internal Control Framework[3] comprises its cyber security framework and implementation plan, including the adequacy of existing mitigating controls.			
External Benchmarking				
6.25	The FRFI has conducted an external benchmarking review of its cyber security framework.			

[3] Refer to the Corporate Governance Guideline for additional guidance in this area.