bluezone | integrated compliance fabric

FINANCIAL
CYBER SECURITY

OSFI
COMPLIANCE

REGULATORY ALIGNMENT BRIEF

Apply unique methods of encryption and tokenization to facilitate OSFI Cyber Security guidance for financial institutions.

/// BLUEZONE

FACILITATE AND EXPEDITE OSFI COMPLIANCE

OSFI Background

Guidance for federally regulated financial institutions to assess the adequacy of their cyber security.

Office of the Superintendent of Financial Institutions (OSFI) is an independent agency of the Government of Canada, established to contribute to the safety and soundness of the Canadian financial system. OSFI supervises and regulates federally registered banks and insurers, trust and loan companies, as well as private pension plans subject to federal oversight. OSFI monitors the financial and economic environment to identify issues that may adversely affect these institutions, and takes further steps to assess each institution's material risks and the quality of its risk management and corporate governance practices. OSFI guidance continues to align with the international standards set out by the Basel Committee on Banking Supervision (BCBS).

The ever-increasing frequency and sophistication of 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 inter-connectedness of the financial sector, as well as the critical role that federally regulated financial institutions (FRFI) play in the overall economy.

OSFI thus expects FRFI senior management to review cyber risk mitigation policies and practices to ensure that they remain appropriate and effective in light of changing circumstances and risks. With this in mind, OSFI issued a template that summarized common cyber security criteria and was intended to serve regulated financial institutions as a guidance for their self-assessment activities.

Specification Overview

Cyber security practices for financial institutions and related critical infrastructure providers.

OSFI guidelines and the associated templates set out desirable properties and characteristics of cyber security practices for consideration by a regulated financial institution when assessing the adequacy of its information security control framework. FRFIs are encouraged to reflect the current state of their digital asset protection in their assessments, rather than their target state, and consider the outlined Cyber Security principles as a roadmap to compliance.

OSFI suggests that financial institutions rate their current degree of maturity on the following scale:

Maturity	Definition
4 - Fully	Fully implemented the principles across the enterprise, with evidence to substantiate the assessment and no outstanding issues identified.
3 - Largely	Largely, but not fully, implemented the principles; there may be some minor outstanding issues.
2 - Partially	Partially implemented the principles; major aspects of the implementation remain outstanding.
1 - None	Has not yet adopted the practice; the principles are under review for assessment consideration.

FRFIs are strongly advised to take notice of the OSFI guidance, as they may be requested to complete the Cyber Security assessment as part of the ongoing regulatory oversight of financial compliance.

The Cyber Security template identifies the following 6 high-level groups of self-assessment criteria:

- Organization and Resources
- Cyber Risk and Control Assessment
- Situational Awareness
- Threat and Vulnerability Risk Management
- Cyber Security Incident Management
- Cyber Security Governance

The included criteria relate to establishing the FRFI's accountability and ownership of its cyber security framework, threat landscape and risk assessment, enterprise-wide security knowledge management, deployment of information protection technologies, incident response practices and policy control.

Although the Cyber Security principles apply to the regulated financial institutions, their computing systems' vulnerability is dependent on material outsourcing partners and critical IT infrastructure providers. Given the trend of growing reliance on third-party technology operations and expanding use of cloud services, FRFIs are likely to look to their providers to conduct similar self-assessment and present the results to the institution, to ensure accuracy and completeness of the end-to-end cyber security framework implementation.

In addition, FRFI service providers may be asked to undertake more rigorous security reviews on an ongoing basis, and include more fullsome security terms and conditions in their contracts.

Threats can originate externally, from those seeking financial gain or trying to make a political statement. Equally, they can come from internal sources, such as employees or other parties that have legitimate direct or indirect access to financial assets, sensitive client information, and current or potential business transactions and trading algorithms. Despite the level and type of threats vary among organizations, OSFI raises awareness among smaller firms that they are as much a target of attacks as larger entities.

Implementation strategies and delivery plans that result from the Cyber Security assessment must be tailored to the specific risks and resources of each firm. Having a robust information security program and an architecture framework will not eliminate all cyber risks, or guarantee that a particular financial institution will not become a victim of cyber crime. It will however, allow the entity manage risks through an informed decision-making process.

A cyber security framework is necessary to provide senior management a means to assess, prioritize and manage the FRFI's specific risk exposure, which includes regulatory, legal, operational, reputational and environmental elements. The framework should cover specific information channels, security policies and decision-making workflows to ensure safety of critical digital assets. That is when security tools and automated solutions come to the rescue, taking on the burden of information protection.

Regulatory Alignment

Protecting financial data with bluezone ensures simplified OSFI compliance assessment.

An industry-leading bluezone solution tremendously reduces the footprint of your critical financial data, therefore minimizing compliance delivery costs and simplifying the overall OSFI / BCBS oversight process. The exposure of your sensitive digital assets is limited to the on-premise or hosted bluezone environment, eliminating your own information systems and applications from the scope of Cyber Security assessment.

The value of bluezone is apparent in helping financial institutions implement effective cyber security measures fairly quickly while meeting their OSFI compliance, and is realized through the following built-in capabilities:

OSFI Cyber Security Principle	Capabilities and Benefits
2 Cyber Risk and Control Assessment	
2.1 Conduct regular cyber risk assessments that consider people, processes, data and technology for all business lines and geographies.	♦ Facilitates critical digital asset identification and security classification ♦ Minimizes personnel exposure to sensitive financial and other records ♦ Eliminates the requirement to inspect and redesign business processes that involve confidential data management
2.2 Mitigate potential cyber risk arising from material outsourcing arrangements.	♦ De-sensitizes real-time transactions and archived records, which makes outsourcing of technology delivery and operations a threat-safe activity ♦ Secures data exchange between financial partner networks
2.3 Mitigate potential cyber risk arising from critical IT service providers.	♦ Implements best practices of cyber security industry standards that address service provider related risks, including PKI and RSA cryptography ♦ Critical cyber assets are protected with data-centric security controls that "travel" with the data to service provider networks and platforms
2.4 Change management risk assessment and due diligence processes consider cyber risk.	♦ Facilitates strict control of changes to operational environment ♦ Fully supports segregation of duties to prevent digital asset misuse ♦ Supports parallel deployment and operation for pilot service provisioning
2.8 Conduct regular cyber-attack, including Distributed denial-of-service (DDoS) and recovery simulation, exercises.	♦ Denial-of-service function is embedded in bluegrid security edge node ♦ DDoS simulations can be run on demand against staging environments ♦ Monitoring and alerting functions are available to test the effectiveness of DDoS attack detection and remediation procedures
2.9 Consider the impact of an Internet outage for an extended period of time.	♦ Each bluezone instance functions as an isolated secure environment, which is not dependent on the method of access, including via public Internet ♦ Provides remote system administration option via a private network
3 Situational Awareness	
3.2 Centrally store a history of security event information.	♦ Invalid and successful digital asset access attempts are logged ♦ Includes a central SYSLOG server to collect and store critical security events
3.3 Normalize, aggregate and correlate security event information.	♦ Includes a central, dedicated security event management system ♦ Critical events are detected based on the event management configuration, with notifications triggered and instantly delivered over various transports
3.4 Conduct automated analysis of security events to identify potential cyber-attacks, including DDoS attacks.	♦ Equipped with multiple technologies that identify and act upon security attacks, including intrusion prevention system and denial-of-service module ♦ Public Internet access is monitored with embedded web application firewall ♦ Security events are analyzed based on the monitoring and alerting rules
3.5 Supplement automated analysis of security events by conducting additional expert analysis on security events to identify potential cyber-attacks.	♦ Expert event analysis is available as additional service as part of an SLA ♦ Security personnel operating a bluezone environment is qualified and trained to undertake periodic security event reviews, aside from automated alerting ♦ Security advisories are monitored and factored into the operational environment, including from WASC and OWASP communities
3.6 Monitor and track cyber security incidents occurred internally and in the financial services industry.	♦ Includes packaged security event monitoring and incident management ♦ Supports SNMP and SMTP alerts based on critical security event detection ♦ Integrates with standard enterprise logging and monitoring systems

OSFI Cyber Security Principle	Capabilities and Benefits
4 Threat and Vulnerability Risk Management	
Data Loss Detection / Prevention	
4.1 Implement tools to prevent unauthorized data leaving the enterprise, monitor outgoing high-risk traffic, and safeguard data in online and offline stores, at rest and in motion.	♦ Creates a secure "bubble" around FRFI's IT systems and channels ♦ Integration with other networks will fail unless explicitly allowed ♦ Restricts monitoring to outbound connections only (SNMP etc.) ♦ Restricts inbound administrative access to VPN and SSH only ♦ Sensitive data is encrypted and/or tokenized prior to storage
Cyber Incident Detection and Mitigation	
4.3 Implement the following security tools and provide for their currency, automated updates and enterprise-wide application: intrusion detection / prevention systems, web application firewalls, anti-virus, anti-spyware, anti-spam, DDoS and other.	♦ Provides next-generation firewall with embedded intrusion prevention and denial-of-service capabilities engaged at the edge of a bluezone instance ♦ Includes web application firewall configured to detect industry-recognized security attack patterns and cyber defense best practices ♦ Each bluegrid node is a hardened appliance at all network layers
Software Security	
4.5 Have a process to obtain, test and automatically deploy security patches and updates in a timely manner based on criticality.	♦ Provides secure and convenient upgrade and patch tools and processes ♦ Minimizes the impact on partner service changes on FRFI's IT systems via configurable service mediation gateway acting as an integration broker ♦ Includes fully managed bluezone private cloud option, where patches and software updates are performed by the authorized operational personnel
4.6 Consider and mitigate cyber risk arising from use of any unsupported software.	♦ Unsupported software is not allowed on engineered bluegrid systems ♦ Provides signature verification of product packages for authenticity
4.7 Establish a process to confirm successful deployment of security patches and resolve update failures.	♦ Security patching and update processes are well documented and subject to security policies defined for each specific bluezone instance
4.8 Internally or externally developed software is subject to secure system design, coding and testing standards that incorporate appropriate cyber security controls.	♦ Software components included in bluegrid are developed and tested using secure coding techniques and common vulnerability detection methods ♦ Uses engineering principles and guidelines for IT security endorsed by PCI, NIST, ISO/IEC, ISF, WASC, TOGAF and other industry consortiums
Network Infrastructure	
4.10 Implement network boundary monitoring and protection.	♦ Bundles next-generation firewall node to protect the network edge ♦ Includes reverse proxy module with TLS termination on the traffic management node to prevent direct public access to core services
4.11 Segment the enterprise network into multiple, separate trust zones.	♦ Employs a DMZ model with NAT and explicitly allowed cross-VLAN routing ♦ Operates segregated platform clusters in a private IP space
4.12 Network infrastructure has multiple layers of defense (e.g. cloud based, ISP, on premise) to mitigate against DDoS attacks.	♦ Supports message level and transport layer encryption ♦ Designed for location neutrality, where any particular bluezone instance can be deployed as a secure hybrid / private cloud, or launched on premise
4.13 Have an ability to rapidly and remotely isolate, contain or shut down compromised operations.	♦ Supports active-active data center deployment and clustering architecture ♦ Supports 24 × 7 operation which accommodates both scheduled shutdown activities and real-time unexpected node failures
4.14 Implement processes and tools to secure mobile devices and wireless networks.	♦ Manages and secures traffic between cellular and conventional data networks ♦ Secures data entry on smartphones, tablets and other mobile devices with pre-emptive encryption and tokenization prior to FRFI backend integration
Standard Security Configuration and Management	

OSFI Cyber Security Principle	Capabilities and Benefits
4.16 Use standard secure OS images for client, server and network devices.	♦ Embeds hardened and tested secure OS images on all bluegrid nodes ♦ Employs runtime containerization to protect the underlying host-level infrastructure and independent core functions from vulnerability spread
4.17 Follow a formal change management process for security configuration management for all network, hardware and software assets.	♦ Each bluezone instance is fully isolated and separately managed ♦ User and system authentication and access controls are 100% resident in the bluezone environment, with no risk of dependency on external systems ♦ Implements centralized network device and system level access control
4.18 Document, implement and enforce security configuration standards to all hardware and software assets.	♦ All bluezone components are protected with centralized authentication, authorization and accounting (AAA) security control and enforcement ♦ Software and hardware security configuration is compliant with PCI DSS, NIST FIPS, ISO/IEC ISMS, Common Criteria and other industry standards
4.19 Restrict the use of unauthorised / unregistered software and hardware through policy and automated tools, including mobile devices.	♦ Unregistered or unauthorized software is not allowed on bluegrid systems ♦ Each bluezone instance is subject to strict policy compliance and rigorous security procedures around operation, administration and maintenance
Network Access Control and Management	
4.21 Have and ability to automatically detect and block unauthorized network access.	♦ Employs firewalls, IPS modules, VPN gateways, private subnets and other standard methods to prevent unauthorized network access ♦ Enforces TLS security for external HTTP and FTP access
4.22 Apply strong authentication mechanisms to manage user identities and access.	♦ Supports single sign-on and user/system identity federation ♦ Supports username/password and X.509 certificate based sign-on, and role-based access control (RBAC) over business services and system resources
4.23 Tightly control and manage the use of administrative privileges.	♦ Restricts inbound administrative access to the recognized endpoints that require VPN-based SSH connectivity and two-factor authentication ♦ Centrally manages administrative roles in the supplied LDAP directory
Third Party Management	
4.25 Consider cyber security risk part of the due diligence process for material outsourcing arrangements and critical IT service providers, including related subcontracting arrangements.	♦ Protects cyber assets themselves vs. their perimeter, which allows safe distribution across partner and supplier networks ♦ Applies centralized data protection measures that reduce the overhead of third-party specific security management
4.26 Contracts for all material outsourcing arrangements and critical IT service providers include the provision for safeguarding the FRFI's information.	♦ Each bluezone instance is a tamper-resistant environment which meets and exceeds nine prevalent information security compliance standards ♦ Supports cloud service SLA options to safeguard FRFI cyber assets with the highest level of information protection and environment perimeter defense
4.27 Have a process in place to monitor the level of cyber risk preparedness for material outsourcing arrangements and critical IT service providers.	♦ Assists in risk ranking and mitigation in the context of critical system data protection, retention and privileged access control ♦ Simplifies third-party security management process with the data-centric security and masking techniques, where de-sensitized cyber assets bear no risk of data loss or theft on the service provider network
4.28 Have 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.	♦ Automates the process of cyber incident notification from outsourcing partners and service providers via event management and alerting ♦ Hosted data facility security protocol includes automated incident response with notification of authorized operations and management personnel
Customers and Clients	
4.29 Cyber security awareness and information is provided to customers and clients.	♦ Maintains currency with the industry-recognized security threat classifications ♦ Provides continuous compliance with the information security regulations
4.30 Take additional actions to protect customers and clients.	♦ Protects customer data privacy in compliance with PII / PIPEDA ♦ Ensures secure processing of payment credentials and other sensitive data

OSFI Cyber Security Principle	Capabilities and Benefits
5 Cyber Security Incident Management	
5.1 Incident management framework is designed to respond rapidly to material cyber security incidents.	♦ Includes event management tools and monitoring dashboards ♦ Fully managed bluezone service supports proximity hosting, 24 × 7 monitoring, and rapid-fire incident response to service outages
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.	♦ Provides out-of-the-box multi-channel incident notification controls ♦ Offers an SLA option of security operation center (SOC) based response
5.3 Document procedures for monitoring, analyzing and responding to cyber security incidents.	♦ Each bluezone instance provides documented incident response procedures, which alleviate any uncertainty over critical digital asset issue management
5.4 Change management process has been designed to allow for rapid response and mitigation to material cyber security incidents.	♦ Reduces the overall impact of changes in financial data processing via service mediation within or outside of the FRFI's technology environment ♦ Facilitates business flexibility by releasing IT systems from security overhead ♦ Delivers high-availability and fault-tolerance via clustering, which also allows change provisioning without interruption of service
5.5 The incident management framework includes escalation criteria aligned with its cyber security taxonomy.	♦ Simplifies incident alignment with FRFI's cyber security control classification ♦ Each operated bluezone instance supplies well-defined escalation procedures enforced via event management automation
5.6 Have an internal communication plan to address cyber security incidents that includes communication protocols for key internal stakeholders.	♦ Facilitates internal security risk and control management via critical data identification and masking implementation effort ♦ An absence of the "trusted network" in bluezone promotes identification and mandatory authorization of the FRFI's key internal stakeholders who require access to incident or business related operational information
5.7 Have an external communication plan to address cyber security incidents that includes communication protocols and draft scripted communications for key external stakeholders	♦ Financial partner network mediation gateway facilitates the identification and documentation of the responsible party communication information ♦ Security zone operational personnel maintains high availability of critical FRFI services via rapid issue response based on well-defined communication plans
5.8 Incident management process is designed to ensure that the following tasks are fully completed: recovery from disruption of service, assurance of system integrity, and recovery of lost or stolen data due to incidents.	♦ Supports industry standard log entries to facilitate audit trail ♦ Provides alerting for critical cyber asset access violation incidents ♦ Protects financial records using tamper-resistant algorithms and devices ♦ Real-time replication of data for simplified backup, restore and failover ♦ Minimizes the scope of disaster recovery planning and validation testing
5.9 Establish post incident review process that is: completed for material cyber security incidents, includes appropriate cyber forensic investigations, chronicles the events throughout security incident lifecycle, identifies the root cause and highlights control deficiencies, assesses breakdowns in the incident management process, and establishes a plan of action.	♦ Includes security event storage facility for incident reviews and investigations ♦ Provides event correlation and search capabilities for issue root cause analysis ♦ Supports configurable log retention policies for regulatory and legal purposes ♦ Facilitates incident tracking across service providers and financial partners
6 Cyber Security Governance	
Cyber Security Policy and Strategy	

OSFI Cyber Security Principle	Capabilities and Benefits
6.1 Establish an enterprise-wide cyber security policy with supporting procedures in place to identify and manage cyber security risks.	♦ Provides simplified data retention policy compliance process ♦ Simplifies user and system authentication policy enforcement ♦ Supports privilege-based resource access control policy ♦ Facilitates provisioning of policy-based data security controls
6.3 The cyber security policy applies to all of the bank's operating groups and entities, including subsidiaries, joint ventures and geographic regions.	♦ Simplifies policy compliance across FRFI subsidiaries and partners by implementing data-centric security techniques and enforcement controls
6.4 Have a defined and consistent common taxonomy for cyber security risk.	♦ Assists in establishing security risk management framework for an on-premise or cloud-based financial service delivery in alignment with common threats
Second Line of Defense - Risk Management	
6.8 Relevant risk and control assessments address cyber security risk and mitigating controls.	♦ Reduces probability and impact of business process interruption ♦ Facilitates expedient and controlled risk assessment process ♦ Facilitates quick identification and documentation of regulatory requirements and their scope of applicability to IT systems
6.9 Key risk and performance indicators, as well as thresholds, have been established for the key inherent cyber security risks and controls.	♦ Provides secure zone implementation based on the industry best practices ♦ Expedites identification and documentation of performance indicators and thresholds while adapting bluezone event management to the FRFI's needs
6.10 Utilize scenario analysis to consider a material cyber-attack, mitigating actions, and identify potential control gaps.	♦ Simplifies information security assessments and gap analysis ♦ Eliminates tedious remediation measures for modern and legacy applications deemed in scope of OSFI / BCBS compliance assessment
6.11 Appropriately assess cyber security risk within the change management process.	♦ Lowers the risk assessment effort via the endorsement of data-centric security ♦ Simplifies change management process via reduced secure zone footprint
6.12 Responsibilities relating to cyber security assessments have been assigned to an independent control group with cyber risk expertise.	♦ Simplifies independent risk assessments via sensitive data taxonomy definition and automated access control procedures ♦ Reduces security gap analysis and risk remediation effort
6.13 Regularly provide an independent challenge to the various cyber security risk assessments conducted by the first line of defense.	♦ Promotes segregation of duties and more accurate risk assessments via the isolation of sensitive data in a hardened security zone ♦ Simplifies recurring independent risk assessment challenge procedures with pre-defined automated security controls and event monitoring rules
6.14 Monitor and challenge the identification, appropriateness and remediation of actions resulting from cyber security incidents and risk assessments.	♦ Facilitates the identification and enforcement of security controls resulting from cyber security incident management and risk assessment activities ♦ Assists in establishing a discipline of information security governance spanning the complete risk lifecycle, from recognition to mitigation
Third Line of Defense - Internal Audit	
6.18 The frequency of cyber security audits is determined by, and is consistent with the risk of a cyber-attack.	♦ Minimizes the footprint of confidential financial assets ♦ Significantly lowers the risk of successful cyber-attacks on the critical systems ♦ Reduces the cost of the initial and follow-up cyber security audits
6.19 Internal audit has assessed, or is planning to assess both the design and effectiveness of the cyber security framework.	♦ Implements data-centric security in financial environment, therefore excluding the majority of FRFI's technology systems from the audit scope ♦ Removes the need to assess complex application integration scenarios and sophisticated security methods and procedures
6.20 Internal audit has sufficient resources and expertise to audit the cyber security framework implementation.	♦ Results in reduced internal audit budgets and assessment timelines ♦ Lowers the requirements for auditors' subject matter expertise and extensive background in the IT domain and FRFI's specific systems and processes

OSFI Solution Summary

Limit the exposure of financial data within or outside your organization IT infrastructure.

A unique, innovative bluezone solution reduces the footprint of critical financial data, leaving only benign, non-sensitive business information behind. A self-contained, engineered environment becomes your lightweight secure inter-connect, with privacy controls applied to sensitive data elements.

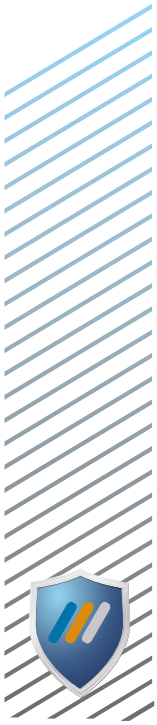
The solution allows you to centrally and uniformly manage all traffic of financial interest, whether it is exchanged internally within your organization, or with your partners and customers involved in the automated business process flow. In a secure, integrated bluezone environment you can quickly and safely manage your financial data with minimal administration and maintenance effort. As a result, the cost and timeline to prepare for your OSFI / BCBS compliance audit are significantly reduced.

Such substantial benefits have become possible due to a concept of capturing sensitive data at the network perimeter, preventing it from ever entering and "contaminating" the computing systems and network devices in your IT environment.

The encrypted and tokenized digital assets are no longer in the scope of OSFI compliance audit, or at risk of being lost or compromised. The complex business processes and inter-connected information systems no longer require redesign.

In the era of cloud computing having evolved as a model for enabling ubiquitous and convenient access to a pool of digital resources, the bluezone solution managed to combine both elasticity of the cloud and security of financial data. A "zero trust" approach, where the so called "trusted network" no longer exists, was laid in the foundation of a small-footprint data protection environment with access to components strictly on a need-to-know basis.

In a nutshell, your applications and infrastructure have been eliminated from the exposure to cyber-threat. Those systems and processes remaining on the OSFI cyber security radar have been reduced to carefully engineered and validated zone, safely accessed regardless of who initiates the network communication and where it originates.



Reliable, simple, affordable. Certified.

An instance of the zone is powered by bluegrid, the industry's first integrated security system engineered to address the complexity and cost of OSFI, among other regulatory standards.

The compact, portable cloud service is based on a high-density component architecture covering network, servers, storage and applications which support large transaction volumes and carrier-grade communication throughput.

Every component of bluezone provides built-in redundancy to meet continuous service availability, fault tolerance and scalability for growth. OSFI compliance is now simple and sustainable.

Contact

Phone 1.888.414.5739
E-mail info@bluezonex.com
Web www.bluezonex.com

bluezone

10 Four Seasons Place, Fl. 10
Toronto, Ontario M9B 6H7