INSURANCE COMMISSION
OF THE BAHAMAS

GUIDANCE ON
CYBERSECURITY RISK MANAGEMENT
OCTOBER 2025

TABLE OF CONTENTS

1. INTRODUCTION

1.0.1 The Insurance Commission of The Bahamas ("the Commission") is the independent regulatory authority established under the Insurance Act, 2005 and the External Insurance Act, 2009 to supervise and regulate all registrants and licensees (i.e. insurers, insurance intermediaries, and external insurers) operating in or from within The Bahamas. Its statutory objectives include safeguarding the soundness of the insurance sector, protecting policyholders, and maintaining public confidence in the jurisdiction's insurance market.

1.0.2 The Commission issues these Guidelines on Cybersecurity Risk Management ("Guidelines") under its mandate in the Insurance Act, 2005, to protect policyholders, uphold market integrity, and promote the safety and soundness of regulated entities. Cyber risk poses an increasingly material threat to the confidentiality, integrity, and availability of information assets and to the continuity of critical insurance functions. Robust cyber risk management is therefore a core element of good governance, prudent risk management, and operational resilience across the Bahamian insurance sector.

1.1 STATUTORY AUTHORITY AND SUPERVISORY ENFORCEMENT

1.1.1 These Guidelines are issued by the Commission pursuant to its powers under the Insurance Act, 2005, and the External Insurance Act, 2009. The Commission may issue rules, guidelines, and other regulatory instruments concerning the conduct of registrants and licensees.

1.1.2 Compliance with these Guidelines forms part of the Commission's supervisory expectations. In the course of inspections and ongoing supervision, the Commission will assess adherence to these requirements. Failure to comply may adversely affect the Commission's assessment of a registrant or licensee's fitness and propriety, governance standards, and overall risk profile. Where warranted, the Commission may exercise its statutory powers, including the imposition of conditions on a license, administrative penalties, or other enforcement measures under the Insurance Act, 2005.

1.2 PURPOSE

1.2.1 These Guidelines set out the Commission's expectations for the management of cybersecurity risk by our regulated entities, with the objective to:

- **Strengthen governance and accountability** – ensure Boards of Directors and Senior Management set cyber risk appetite, oversee strategy and resources, and embed cybersecurity into enterprise risk management (ERM) and decision-making.
- **Promote proportionate, risk-based controls** – require regulated entities to identify, assess, treat, and monitor cyber risks in line with their business model and risk profile, including risks arising from outsourcing arrangements with service providers including IT vendors, managed services and cloud service providers.
- **Enhance operational resilience** – integrate cyber scenario planning, continuity arrangements, disaster recovery, and tested incident response capabilities so that critical services are maintained or restored within defined tolerances.
- **Protect policyholder and confidential information** – implement data governance and protection measures consistent with applicable Bahamian law and sound practices across the information lifecycle.
- **Foster continuous improvement** – require ongoing monitoring, testing, training, and lessons-learned to adapt to the evolving threat landscape and technological change.

1.2.2 The Commission will review and update these Guidelines as needed to reflect emerging risks, supervisory experience, and developments in international practice.

1.2.3 These Guidelines are principles-based and intended to be applied proportionately. The Commission does not prescribe specific technologies or solutions but expects licensees and registrants to achieve effective risk management outcomes aligned with their individual risk profiles.

1.3 SCOPE

1.3.1 These Guidelines apply to all regulated entities under Bahamian insurance legislation, including:

- Domestic insurers (life, general, composite)
- External insurers operating in or from within The Bahamas
- Insurance intermediaries (agents, brokers, salespersons)
- Insurance managers and other entities providing outsourced insurance services to registrants and licensees

1.3.2 The Guidelines cover all information assets, systems, and processes that support or deliver regulated insurance activities, including but not limited to:

a. **Information Systems and Infrastructure** – hardware, software, networks, cloud environments, mobile devices, and any other technology components used in the conduct of insurance business.
b. **Data Assets** – personally identifiable information (PII), confidential commercial data, financial records, and any other sensitive or business-critical information processed, stored, or transmitted by the registrant or licensee or its service providers.
c. **Third-Party Arrangements** – all outsourced services, technology vendors, cloud service providers, and other external parties whose systems or services have the potential to affect the registrant or licensee's cyber risk profile.
d. **Operational Processes** – business processes reliant on technology or data that, if disrupted or compromised, could impact policyholder protection, market confidence, or financial stability.

1.3.3 The Commission expects each registrant and licensee to implement cybersecurity measures proportionate and scalable to its size, nature, complexity, and technological infrastructure, taking into account its risk exposures, including:

- The volume and sensitivity of information handled;
- The criticality of services provided;
- The nature of its business model and delivery channels; and
- The extent of its reliance on third-party or cloud-based systems.

1.3.4 These Guidelines apply to all relevant operations of the registrant or licensee, whether conducted directly, through branches, subsidiaries, or outsourced arrangements, to the extent those operations may impact the security and resilience of regulated insurance activities in The Bahamas.

1.3.5 In applying these Guidelines, registrants and licensees, particularly intermediaries and smaller entities, may adopt simplified or alternative controls where appropriate, provided that such controls achieve comparable risk management outcomes.

1.3.6 The Guidelines are intended to complement and not replace, applicable Bahamian law, particularly the Data Protection Act, 2008, as well as any relevant international obligations. Where more stringent requirements apply, registrants and licensees should adopt the higher standard.

1.4 TRANSITION AND IMPLEMENTATION

1.4.1 To facilitate orderly compliance with this guideline, the following transition arrangements apply:

1.4.2 All licensees and registrants, including insurers and intermediaries, will be allowed an implementation (transition) period of up to twelve (12) months. The Commission reserves the discretion to determine and vary the applicable transition period, having regard to the size, nature, and complexity of the relevant registrants and licensees within each category.

1.4.3 Certifications, declarations, and attestations required under these Guidelines shall not be mandatory until the first full reporting cycle following the conclusion of the transition period.

2. DEFINITIONS

For the purposes of these Guidelines, the following terms apply:

Access Control	Processes and technical measures for granting, restricting, and reviewing user and system access to networks, applications, and data according to least-privilege and need-to-know principles.
Business Continuity Plan	A documented plan that sets out procedures to ensure the continuation of critical business functions in the event of disruption, including cyber incidents.
Chief Information Security Officer	The senior officer responsible for leading the development, implementation, and oversight of the licensee's cybersecurity framework.
Cloud Service Provider	An external provider that delivers computing services (infrastructure, platform, or software) via the internet and is subject to contractual and regulatory risk management requirements.
Cyber Hygiene	Routine practices and safeguards that reduce exposure to common cyber threats, such as phishing, malware, outdated software, weak passwords, or misuse of elevated privileges.
Cybersecurity Incident Response Plan	A documented, tested plan outlining roles, responsibilities, procedures, and communications for detecting, escalating, containing, eradicating, and recovering from cybersecurity incidents, including post-incident review.
Cyber Resilience	The ability of systems and organizations to withstand cybersecurity events; practically, it is measured by the combination of mean time to failure and mean time to recovery.
Cyber Risk	The risk of financial loss, operational disruption, harm to policyholders, or reputational damage arising from the use of information and communication technologies, including risks to the confidentiality, integrity, and availability of electronic information and systems.
Cybersecurity	The strategies, policies, processes, and controls used to manage cyber risk, including threat reduction, vulnerability management, detection, response, recovery, and continual improvement.
Cybersecurity Incident	Any actual or suspected event that jeopardizes the confidentiality, integrity, or availability of information systems or the information they process, store, or transmit, or that breaches applicable security policy (e.g. malware infection, data breach, unauthorized access, denial-of-service, or disruptive system outage).
Cybersecurity Maturity Model	A staged framework used by the Commission and its registrants and licensees to assess and improve cybersecurity capability across progressive levels, supporting proportionate and risk-based implementation.

Data Protection	Administrative, technical, and physical safeguards to ensure lawful collection and processing and to protect personal and sensitive data throughout its lifecycle, including classification, minimization, retention, and secure disposal.
Disaster Recovery Plan	A documented plan focused on restoring IT systems, applications, and data after a disruption, including cyber events, within defined recovery objectives.
Encryption	Cryptographic techniques for protecting data at rest and in transit so that it is unintelligible to unauthorized parties.
Key Performance Indicators	Metrics that measure the effectiveness of cybersecurity processes, controls, and training programs.
Key Risk Indicators	Metrics that provide early warning signals of increasing risk exposures in cybersecurity.
Multi-Factor Authentication (MFA)	An authentication method requiring two or more independent factors (e.g. something you know, have, or are) to verify identity before granting access.
Penetration Testing	Authorized, simulated attacks by qualified, independent testers designed to identify and validate exploitable weaknesses in systems, networks, and applications.
Recovery Point Objective (RPO)	The maximum acceptable amount of data loss measured in time.
Recovery Time Objective (RTO)	The targeted duration to restore a system or process following disruption.
Risk Assessment	A process to identify cyber threats and vulnerabilities, analyze likelihood and impact, evaluate existing controls, and determine residual risk and treatment options.
Security Information and Event Management	A solution that aggregates, analyzes, and correlates security data from multiple systems to detect anomalous activities and threats.
Security Operations Centre (SOC)	An internal or outsourced function that centrally monitors, investigates, and responds to security events on a continuous basis.
Third-Party Risk	Risks to the registrant or licensee arising from service providers (including IT vendors, managed services, and cloud providers) and from broader supply chain dependencies.

3. CORPORATE GOVERNANCE

3.1 GOVERNANCE FOUNDATIONS

3.1.1 Cyber risk must be addressed not as a purely technical issue, but as a governance concern requiring informed oversight, cross-functional collaboration, and a culture of accountability.

3.1.2 Effective cyber risk management begins with strong corporate governance. The Board of Directors is ultimately accountable for ensuring that the registrant or licensee has the strategy, resources, and oversight mechanisms to safeguard information assets and maintain operational resilience.

3.1.3 The governance framework must clearly define roles, responsibilities, and reporting structures while aligning with applicable laws, regulatory expectations, and recognized industry standards. These may include relevant enterprise-wide committees, functions and/or designated officers with the requisite expertise to perform the responsibilities of a:

- Chief Information Officer (CIO) or equivalent[1]
- Chief Information Security Officer (CISO) or equivalent
- Cyber Incident Response & Recovery (CIRR) function or equivalent (Section 4.5.5)
- Project Management Office (PMO) or equivalent.

3.2 CYBER RISK-AWARE CULTURE

3.2.1 The registrant or licensee's governance framework must actively foster a cyber risk-aware culture across all levels of staff.

3.2.2 At a minimum, this must include:

- Mandatory training for all staff, delivered annually and more frequently for high-risk roles.
- Regular phishing simulations or awareness campaigns, and
- Mechanisms for the early reporting of suspicious activity without fear of reprisal.

3.2.3 In cultivating this culture, registrants and licensees are expected to adopt and apply the *Financial System Stability Committee (FSSC) Cyber Resilience Principles* (see Appendix 1). The first focus area under Principle 1 emphasizes the importance of cyber risk-aware culture as a foundation for resilience. Applying the 10 Principles is expected to:

- Build preparedness to withstand cyber threats and recover swiftly from incidents, thereby safeguarding financial stability.
- Foster collaboration across the financial sector and with public/private stakeholders to strengthen the resilience of the interconnected system.

3.3 BOARD OF DIRECTORS RESPONSIBILITIES

3.3.1 A registrant or licensee's Board of Directors holds ultimate responsibility for oversight of cyber risks and must:

- Embed cybersecurity into its overall business strategy and enterprise risk management (ERM) framework.
- Review and approve a cyber risk management framework that, at a minimum, incorporate *three lines of defense*.
- Define and periodically review the institution's cyber risk appetite and tolerance, ensuring alignment with critical operations and core business lines.

[1] In some cases, the Commission will allow a virtual equivalent and will assess all equivalencies in proportion to the level of development, including consideration of virtual options or the outsourcing of functions through service-level agreements.

- Monitor management's implementation of cybersecurity programs, providing challenge and direction where deficiencies are identified.
- Ensure that adequate budget, staffing, and technical expertise are dedicated to cybersecurity.
- Understand risks associated with IT outsourcing, cloud adoption, and other third-party arrangements, and ensure appropriate mitigation measures are in place.
- Maintain a program to address gaps in Board knowledge and expertise, including training and use of external advisors where necessary.

3.3.2 These responsibilities ensure the Board's oversight remains effective and consistent with principles of sound corporate governance.

3.4 SENIOR MANAGEMENT RESPONSIBILITIES

3.4.1 Senior Management is responsible for implementing the Board-approved cybersecurity strategy and ensuring day-to-day compliance with policies, laws, and regulations. Key responsibilities include:

- **Policy Implementation:** Translate Board directives into operational procedures, control frameworks, and measurable outcomes.
- **Operational Oversight:** Monitor outgoing cyber risk management and escalate material incidents to the Board in a timely manner.
- **Staff Competence:** Ensure all staff possess the necessary skills and training to execute cybersecurity responsibilities effectively.
- **Cross-Functional Coordination:** Promote collaboration across IT, risk, compliance, operations, and business units to manage risks comprehensively.

4. CYBER RISK MANAGEMENT FRAMEWORK

4.0.1 Registrants and licensees are required to establish and maintain an enterprise-wide Cyber Risk Management Framework that is aligned with internationally recognized cybersecurity standards (e.g. NIST, ISO, or other equivalent frameworks), as appropriate to the registrant's or licensee's business model and risk profile.

4.0.2 The framework should enable the effective identification, assessment, treatment, and oversight of cyber risks in a manner that supports the registrant or licensee's business objectives and meets the Commission's regulatory expectations.

4.0.3 The framework must assign clear accountability across the ***three lines of defense*** – operations, risk management, and internal audit – and be supported by approved policies, procedures, and reporting arrangements.

4.0.4 At a minimum, the framework must:

- Establish competent structures and resources
- Address third-party dependencies
- Identify and assess exposures
- Implement proportionate controls, and
- Provide continuous monitoring and reporting.

FIRST LINE OF DEFENSE: OPERATIONAL MANAGEMENT

4.1 RISK OWNERSHIP AND CONTROL IMPLEMENTATION

4.1.1 When implementing a robust framework for managing cyber risks, based on the aforementioned international standard, the framework must include, at a minimum, the following components:

- Risk Ownership: Senior management is responsible for establishing a cyber risk process and ensuring all internal controls and procedures deliver the reliability, resilience, and recoverability of critical technology and data assets. They must also maintain an effective threat intelligence process and participate in sector information-sharing arrangements.
- Control Implementation: Registrants and licensees must establish, maintain, and regularly test a formal, risk-based Information Security Program. This program should include layered, risk-based controls such as network and endpoint protection, multi-factor authentication (MFA) for critical systems, strict least-privileged access, and risk-based patch and vulnerability management. These controls must be reviewed and updated as threats and technologies change.

4.2 STRUCTURE AND RESOURCING

4.2.1 Senior Management must ensure an organizational construct with sufficient authority, skills, and budget to manage cyber risk.

4.2.2 Structures may include, as appropriate, enterprise committees and designated officers (e.g. CIO, CISO), a Cyber Incident Response and Recovery (CIRR) function, and a Project/Program Management Office (PMO).

4.2.3 Robust screening and due diligence for staff, contractors, and vendors must be performed to mitigate insider and IT-specific risks.

4.2.4 Mandatory, role-appropriate cyber awareness training must be delivered to all personnel, with periodic refreshers addressing prevailing threats (e.g. phishing, malware, credential abuse).

4.2.5 Licensees and registrants are not required to establish specific roles or titles (e.g. CIO, CISO), provided that the underlying responsibilities are clearly assigned and effectively performed.

4.3 ROLES AND ACCOUNTABILITIES

4.3.1 Registrants and licensees must clearly define and assign roles and responsibilities to ensure accountability, avoid duplication, and support effective governance of cyber risk. At a minimum, the following functions and responsibilities must be established.

Role/ Function	Key Responsibilities
Senior Management	Establish enterprise-wide cyber risk processes aligned with risk appetite and regulatory requirements, approve and maintain a cybersecurity strategy, and ensure the reliability and resilience of critical assets. They are also responsible for embedding cyber hygiene and training across the organization, maintaining and testing CIRR plans, and escalating material incidents to the Board within five (5) days.
CIO	Provide strategic oversight of information technology and digital transformation programme. The Chief Information Officer (CIO) is responsible for overseeing technology services, driving digital enablement, and aligning IT with business objectives.
CISO	The Chief Information Security Officer (CISO) provides strategic oversight information security and overall cybersecurity programme, which includes the cyber risk awareness and strengthening cyber risk posture and maturity level. The CISO reports independently to the Board or a non-conflicted executive supporting business continuity and disaster recovery planning, monitoring emerging threats and enforcing cybersecurity controls.
CIRR	A cross-functional steering committee or equivalent that outline goals, objectives, and desired outcomes of activities related to the cyber incident response plan and any other related projects or initiatives that may arise. It should include at a designated incident coordinator and an executive sponsor to ensure timely incident reporting, effective response and recovery. (Section 4.5.5)
PMO	Coordinate technology, change initiatives, standardize security-by-design project delivery practices, and verify compliance with industry standards (Appendix 6).
Cyber Programs	Address areas such as critical infrastructure, applications, storage, cloud, information security, awareness and training, and continuity/recovery capabilities.

4.4 CYBERSECURITY PROGRAMME

4.4.1 A formal, risk-based program must be approved by Senior Management and aligned to applicable laws and international standards (e.g. ISO/IEC 27001). At a minimum, it must include:

- Access control and authentication (RBAC/least privilege, joiner-mover-leaver)
- Data protection and encryption
- Acceptable use
- Password/credential management (including MFA where appropriate), and
- Remote work and cloud security

- Data Loss Prevention
- Business Continuity and Disaster Recovery
- Physical Security Monitoring.

4.5 CYBER RISK LIFE CYCLE

4.5.1 Registrants and licensees must adopt a structured Cyber Risk Lifecycle that ensures risks are consistently identified, assessed, mitigated, monitored, and reported across the organization (Figure 1). This lifecycle must be embedded within the three lines of defense, with clear accountability for execution, oversight, and independent assurance.

Figure 1: Cyber Risk Life Cycle

4.5.2 **Risk Identification and Assessment**

- Registrants and licensees must maintain documented, ongoing processes to identify internal and external cyber threats [2] and vulnerabilities across technology, operations, and third parties.
- Identified risks must be analysed for likelihood and impact and prioritized against stated tolerances.
- The Commission may require submission of a Cybersecurity Risk Identification Form (Appendix 3).

4.5.3 **Risk Mitigation and Controls** must be mapped and harmonized with industry standards and frameworks for cybersecurity control (Appendix 6) to ensure effective mitigation treatment and adequate coverage of cyber risk exposures.

- **Risk register** must be maintained to document cyber risks, assigned owners, treatments, current status, and residual exposures.
- **Prioritization** must reflect high-impact threat/vulnerability pairings.
- **Cyber insurance** may be used where appropriate.

4.5.4 **Risk Monitoring and Reporting** must be continuous, systematic, and proportionate to the registrant or licensee's risk profile. High-severity risks should be subject to enhanced monitoring

[2] See *Appendix 2* for Common Cyber Attacks

and escalated through regular reporting. Metrics provided to Senior Management and the Board must incorporate incidents, vulnerabilities, testing results, and audit findings. Monitoring processes must be reviewed at least annually, or sooner in the event of material changes.

- **Penetration Testing:** Internet-facing systems must undergo annual penetration testing and after major changes; full-scope testing must occur at least biennially.
- **Scenario-based exercises** (e.g. tabletop, social engineering, cyber range, adversarial simulations) must be planned with clear objectives and rules of engagement and informed by relevant threat intelligence.
- **Attestation and Assurance**: Licensees and registrants must implement a structured approach to assessing and demonstrating the effectiveness of their cybersecurity framework.

  At a minimum:

  1. Management Self-Assessment and Certification
     - Licensees and registrants must perform an annual self-assessment of their cybersecurity controls against these guidelines. An annual attestation to the Commission is required, alternating between self-assessment (Appendix 4) and independent assessment (Appendix 5).
     - The results must be reviewed and approved by Senior Management and submitted to the Commission as part of the Annual Cybersecurity Certification.

  2. Independent Assessment
     - Licensees and registrants must periodically obtain an independent assessment of their cybersecurity framework to provide objective assurance on the design and operating effectiveness of controls.
     - Independent assessment may be performed by:
       - Internal Audit functions, provided they are independent of operational management, or
       - Qualified external third-parties with appropriate expertise in cybersecurity.
     - Independent assessments may include, as appropriate:
       - Cybersecurity audits
       - Control effectiveness reviews
       - Penetration testing and technical security assessments, or
       - Reviews aligned to recognized frameworks (e.g. ISO 270001, NIST)
     - The scope, depth, and frequency of independent assessments must be commensurate with proportionality.

  3. Evidence and Outcomes
     Licensees and registrants must maintain sufficient documentation to demonstrate:
     - The methodology and scope of assessments
     - Identified gaps and remediation plans, and
     - Progress against remediation actions.

4.5.5 Attestations and assessments may be conducted by:

- Senior Management or designated internal personnel (self-assessment)
- Internal Audit functions, or
- Independent external assessors, depending on the size, complexity, and risk profile of the licensee or registrant.

Intermediaries and smaller entities may adopt proportionate attestation approaches, subject to supervisory expectations.

4.5.6 **Incident Response and Recovery**- The role of the Cyber Incident Response and Recovery (CIRR) function or equivalent encompasses but not limited to:

- Outline goals, objectives, and desired outcomes of activities related to the cyber incident response plan and any other related projects or initiatives that may arise.
- Serve as the steering committee for the various projects/initiatives geared towards the establishment and maintenance of the cyber incident response plans, playbooks, protocols and procedures, to ensure alignment and compliance with the relevant laws, regulations and international standards.
- Designate an incident coordinator and an executive sponsor to ensure timely incident reporting, effective response and recovery.
- Monitoring and ensuring adherence to the relevant legislative, regulatory and industry standards, in collaboration with lines of defence.
- Make recommendations on policy, resource allocation, and prioritization of cyber incidents response related projects/initiatives.
- Co-ordination of activities outlined in the CIRP in response to an actual cyber incident. This includes attending meetings at very short notice at the onset of the incident, and giving undivided attention during same to inform timely and effective response to the incident.
- Participate in cyber related scenario simulations, table top test exercises and other related activities to ensure effective maintenance of the cyber incidence response plan.
- Review progress reports, evaluate milestones, and ensure timely and effective implementation of action items/initiatives coming out of cyber related scenario simulations or tabletop test exercises.

4.6 THIRD-PARTY & CLOUD RISK MANAGEMENT

4.6.1 Licensees and registrants must remain fully accountable for all outsourced services, including cloud service providers and managed IT and security providers. To manage these risks, registrants and licensees must have:

Key Area	Expectation
Governance	All outsourced services must be governed within the Cyber Risk Management Framework.
Pre-Engagement Due Diligence	Before engaging any provider, conduct a thorough due diligence process to assess governance, controls, and operational resilience. For material cloud services, this also includes assessing data sensitivity, operational impact, and legal obligations, obtaining Board approval, and reviewing relevant certifications (e.g., ISO/IEC 27001, SOC 2).
Contractual Clarity	All contracts must clearly define responsibilities and mandate breach notification, audit rights, data security, and compliance with legal and regulatory expectations. For cloud, this also addresses security/availability SLAs and data localization.
Ongoing Oversight	Maintain continuous oversight through periodic reviews and performance monitoring. This includes implementing cybersecurity controls such as encryption, strong identity, access management, data protection and privacy policy measures integrated into Business Continuity/Disaster Recovery Plans (BCP/DRP) and the development of exit strategies.

4.6.2. Where outsourcing arrangements involve cross-border data transfers, licensees and registrants must ensure compliance with the Data Protection Act, including the implementation of safeguards to ensure a level of protection comparable to that required under the Act.

4.6.2 Licensees and registrants must ensure that data storage and cross-border data processing arrangements comply with the Data Protection Act and any applicable legal or regulatory requirements. Where data is stored or processed outside The Bahamas, licensees and registrants must assess associated risks, including data sovereignty, legal enforceability, and access by foreign authorities.

SECOND LINE OF DEFENSE: RISK MANAGEMENT

4.7 RISK MANAGEMENT & COMPLIANCE FUNCTION

4.7.1 The risk management and compliance function must monitor cybersecurity as part of overall operational risk, oversee and challenge control practices, and ensure adherence to applicable laws and regulatory requirements. It must propose risk tolerances for Board approval, integrate cybersecurity into governance, risk, and compliance processes in coordination with the CISO, report risk and compliance information, and maintain treatment plans. The assessment approach should align with the enterprise risk management (ERM) framework and use impact-driven metrics (e.g., critical service downtime, affected accounts, customers impacted, lost revenue, SLA breaches), updating as the business and regulatory environment evolves.

THIRD LINE OF DEFENSE: INDEPENDENT ASSURANCE

4.8 INTERNAL AUDIT

4.8.1 Internal Audit is expected to provide independent and objective assurance on the adequacy, design, and operating effectiveness of the organization's cybersecurity governance, risk management, and control environment. Internal Audit is expected to:

- Report findings directly to the Board or Audit Committee, independent of management influence.
- Assess whether cybersecurity risks are identified, monitored, and managed in line with the risk appetite and regulatory requirements.
- Verify that policies, procedures, and controls are consistently applied across business units, outsourced providers, and cloud arrangements.
- Ensure that deficiencies and recommendations are tracked to remediation, with unresolved issues escalated to the Audit Committee.
- Establish a risk-based audit plan, reviewed and approved annually by the Audit Committee, to determine the scope and frequency of cybersecurity audits.
- Conduct periodic thematic or ad-hoc reviews in response to emerging risks, material incidents, or regulatory directives.

4.9 REGULATORY REPORTING AND COMPLIANCE

4.9.1 Licensees and registrants must demonstrate ongoing compliance with these cybersecurity guidelines through regular reporting and supervisory engagement.

4.9.2 At a minimum, licensees and registrants must:

- Submit an *Annual Cybersecurity Certification* to the Commission, signed by the CEO or equivalent senior executive, attesting to compliance with these Guidelines.
- Be subject to supervisory assessments, which may include targeted reviews, onsite examinations, and independent third-party evaluations of the effectiveness of their cybersecurity framework.

4.9.3 Failure to comply with these requirements may result in regulatory action, including the use of enforcement powers and sanctions under the *Insurance Act, 2005*, and the *Data Protection Act, 2008*, to protect policyholders and maintain market integrity.

5. SUPPORTING FRAMEWORKS AND PROGRAMS

5.0.1 Licensees and registrants must establish and maintain supporting frameworks and programs that complement the Cyber Risk Management Framework. These programs are necessary to ensure resilience, preparedness, and compliance across the organization, and must, at a minimum, address incident response, business continuity and disaster recovery, data protection and privacy, and training and awareness.

5.1 CYBER INCIDENT RESPONSE AND NOTIFICATION

5.1.1 Incident response capabilities must be integrated into the registrant or licensee's broader risk management framework, supporting operational continuity, regulatory compliance, and the protection of stakeholders' interests.

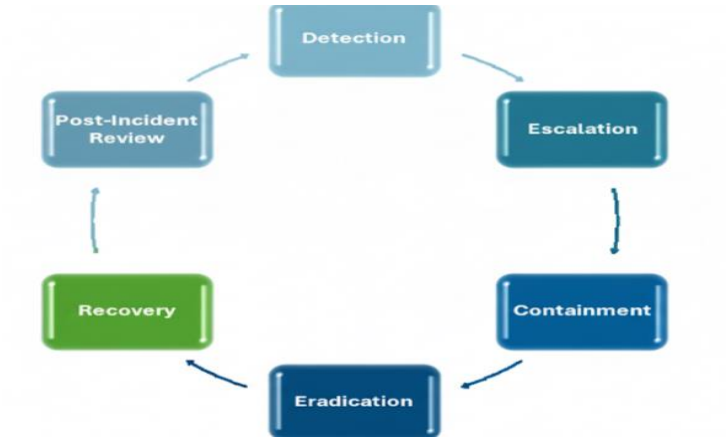
5.1.2 At a minimum, licensees and registrants are required to:

- **CIRR Function and Cyber Incident Response Plan:** Licensees and registrants must establish a Cyber Incident Response and Recovery (CIRR) function or equivalent that oversees, guide, maintains, and regularly test a Cyber Incident Response Plan (CIRP) to ensure an effective and coordinated response to cybersecurity incidents.
- **Regulatory Notification:** Notify the Commission **within 72 hours** of detecting any significant cybersecurity incident that may disrupt operations, compromise critical systems, expose policyholder or sensitive data, or create potential regulatory non-compliance. Failure to notify within the prescribed timeframe may result in regulatory action.
- **Testing and Exercises:** Conduct at least annual incident response exercises (e.g. tabletop simulations) to validate the effectiveness of the CIRP, ensure staff readiness, and identify areas for improvement.

5.1.3 The CIRP must clearly define roles, responsibilities, escalation procedures, external communications, and recovery steps to enable a rapid and structured approach to incident management, including detection, escalation, containment, eradication, recovery and lessons learned (Figure 1).

- Detection– to detect incidents as early as possible and to effectively assess the nature and severity of the incident.
- Escalation – to promptly notify appropriate stakeholders based on incident severity and impact to enable timely and coordinated response.
- Containment – to isolate compromised systems.
- Eradication – to eliminate the threats from affected systems.
- Recovery – to return operations to normal and ensure no threat remains.
- Post-incident review– to analyse incident logs, capture lessons learned, update response plan and complete incidents related documentation.

Figure 2: Incident Response Cycle



5.2 MONITORING, DETECTION, AND TESTING

5.2.1 Licensees and registrants must establish a monitoring and detection framework that enables the timely identification, assessment, and response to cybersecurity threats. The following requirements must be implemented in a manner proportionate to the licensee's or registrant's size, complexity, and technological environment.

5.2.2 Monitoring controls must be commensurate with the size, nature, complexity, and risk profile of the licensee or registrant and the criticality of its operations.

5.2.3 At a minimum, licensees and registrants must implement capabilities to:

- Collect and retain relevant security logs
- Detect anomalous or suspicious activity
- Investigate and respond to security events in a timely manner.

5.2.4. A range of solutions may be utilized to achieve these outcomes, including:

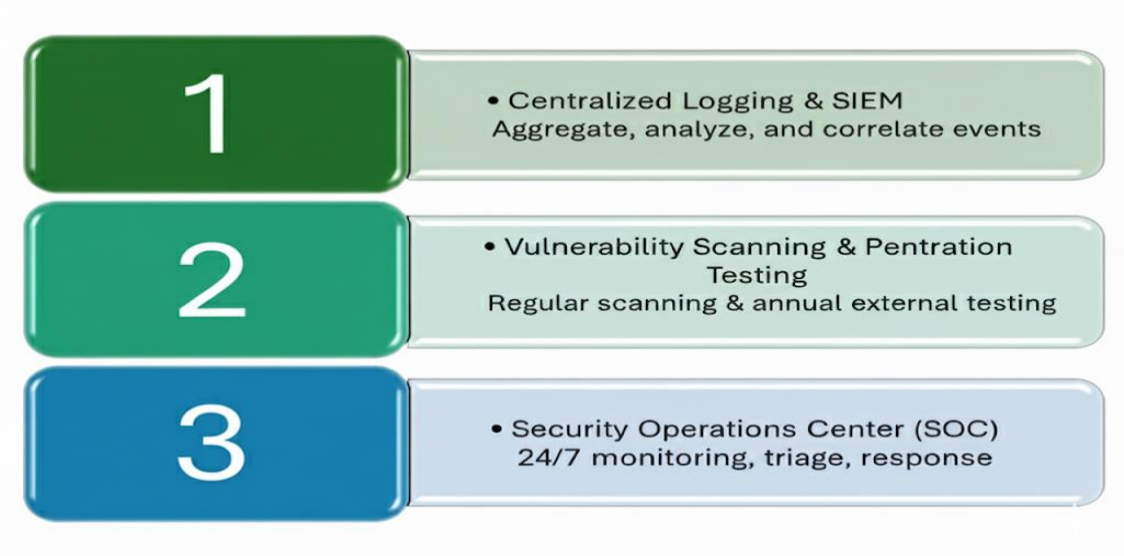
- Centralized logging and event correlation tools (e.g. SIEM or equivalent solutions)
- Managed security service providers (MSSPs)
- Outsources or shared Security Operations Centre (SOC) capabilities, or
- Other proportionate monitoring arrangements.

5.2.5. Licensees must maintain centralized logging and, where appropriate, utilize Security Information and Event Management (SIEM) or equivalent monitoring solutions. An internal or outsourced monitoring capability must be established, which may include a Security Operations Center (SOC) or equivalent arrangements appropriate to the entity's risk profile. Solutions must demonstrate:

- Effective coverage of key systems and risks
- Timely detection and escalation of incidents, and
- Adequate response and recovery capabilities.

5.2.6. The Commission will assess the adequacy of monitoring arrangements based on outcomes achieved, rather than the specific technologies deployed.

Figure 3: Monitoring, Detection & Testing Layers



5.3 BUSINESS CONTINUITY AND DISASTER RECOVERY

5.3.1 Registrants and Licensees must explicitly incorporate multiple scenarios into their Business Continuity Plans (BCPs) and Disaster Recovery Plans (DRPs) including IT outages and various type of cyberattacks (Appendix 2) to ensure resilience and the continuity of critical functions in the event of a cyber incident.

5.3.2 At a minimum, BCPs and DRPs must include:

- Clearly defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)
- Strategies for ransomware detection, containment and recovery
- Documented procedures for failover to secondary or backup systems.

5.3.3 Regular testing of cyber resilience must be conducted to validate the effectiveness of these plans. Such testing must include:

- Tabletop or live simulations of ransomware scenarios
- Exercises addressing data loss, system compromise, and extended service disruption.

5.3.4 Testing scenarios may be combined where appropriate, provided that cyber-related risks (including ransomware and data loss) are adequately covered within broader business continuity and disaster recovery exercises.

5.4 DATA PROTECTION AND PRIVACY

5.4.1 Licensees must establish and enforce a data protection framework aligned with the *Data Protection Act, 2008*, and consistent with recognized international principles, particularly where cross border data transfers are involved.

5.4.2 At a minimum, the framework must provide for:

- Controls include data classification and minimization, encryption of data at rest and in transit, and secure handling, storage, and disposal.
- Compliance obligations under the *Data Protection Act, 2008* and applicable international privacy standards.
- Procedures for prompt detection and escalation of data breaches, timely notification to affected individuals and the Commission where required, and ongoing review of privacy and data handling practices.

- Privacy-by-design principles embedded across cybersecurity and data governance to ensure protection of personal and sensitive information through its lifecycle.

5.4.3 Compliance with the *Data Protection Act, 2008* must be treated as both a legal obligation and a core operational priority.

5.5 DATA PROTECTION AND PRIVACY

CROSS-BORDER DATA STORAGE AND PROCESSING

5.5.1. Registrants and licensees may store or process personal data outside The Bahamas, provided that such arrangements comply with the *Chapter 324A, Data Protection* and do not compromise the confidentiality, integrity, or availability of data.

5.5.2. Licensees and registrants remain fully accountable as data controllers for personal data processed on their behalf, regardless of where such data is stored or processed.

MINIMUM EXPECTATIONS

5.5.3. Ensure Compliance with Data Protection Principles

- Ensure that personal data is collected, processed, retained, and disclosed in accordance with the principles set out in the Chapter 324A, including lawful processing, purpose limitation, data minimization, retention, and security.
- Implement appropriate technical and organizational security measures to protect against unauthorized access, loss, or disclosure.

5.5.4. Conduct Risk Assessments for Cross-Border Transfers

Assess risks associated with transferring data outside The Bahamas, including:

- The legal and regulatory framework of the destination jurisdiction
- The ability to enforce contractual rights, and
- Risk of unauthorized access or disclosure, including by foreign authorities.

Consider whether the transfer could result in harm, damage, or distress to data subjects.

5.5.5. Implement Contractual or Legal Safeguards

Ensure that third-party service providers (including cloud providers) are subject to contractual or other legal arrangements that provide a level of protection comparable to that required under the Data Protection Act.

Contracts must, at a minimum, address:

- Data protection and confidentiality obligations
- Security controls and incident management
- Breach detection and notification
- Audit and access rights
- Data location, transfer, retention, and secure deletion.

5.5.6. Maintain Ongoing Oversight

Monitor third-party providers on an ongoing basis to ensure continued compliance with contractual and regulatory requirements.

Ensure that data remain accessible, recoverable, and protected in line with business continuity and regulatory expectations.

5.5.7. Ensure Regulatory Access and Accountability

Ensure that data can be accessed and produced to the Commission in a timely manner, regardless of where it is stored.

Maintain clear accountability for data protection obligations, including where processing is outsourced.

5.5.8. The Commission does not prescribe specific data localization requirements. However, consistent with the Data Protection Act, cross-border transfers may be restricted where the licensee or registrant is unable to demonstrate that adequate or comparable levels of protection are in place.

Licensees and registrants must be able to demonstrate that appropriate safeguards, whether contractual, technical, or organizational, are in place to protect the rights and interests of data subjects.

5.6 TRAINING AND AWARENESS

5.6.1 Licensees and registrants must establish and maintain a comprehensive cybersecurity training and awareness program to foster a culture of security throughout the organization. The program must ensure that all employees, contractors, and third-party personnel understand their responsibilities in protecting the organization's information assets.[3]

5.6.2 At a minimum, the program must include:

- Mandatory training at onboarding, annually, and upon significant policy, procedural, or threat-related changes.
- Role-based modules tailored to specific responsibilities, with heightened focus on individuals with privileged access or elevated cybersecurity duties.
- Core topics covering data protection, secure technology use, phishing awareness, incident reporting, and relevant legal and regulatory obligations.

5.6.3 Training effectiveness must be regularly evaluated and updated to reflect emerging threats, technologies, and regulatory changes. Records of completion must be maintained and made available for inspection by the Commission as part of supervisory oversight.

[3] Emerging technologies, including Artificial Intelligence (AI), introduce new dimensions of cyber and operational risk. While this Guideline establishes the baseline requirements for cyber resilience, the Commission will issue separate guidance specific to the governance, ethical use, and risk management of AI and other emerging technologies.

6. DOCUMENTATION AND ESCALATION

6.0.1 Licensees and registrants must ensure that accountability and escalation processes are clearly documented and regularly tested to support timely decision-making and effective oversight of cybersecurity risks.

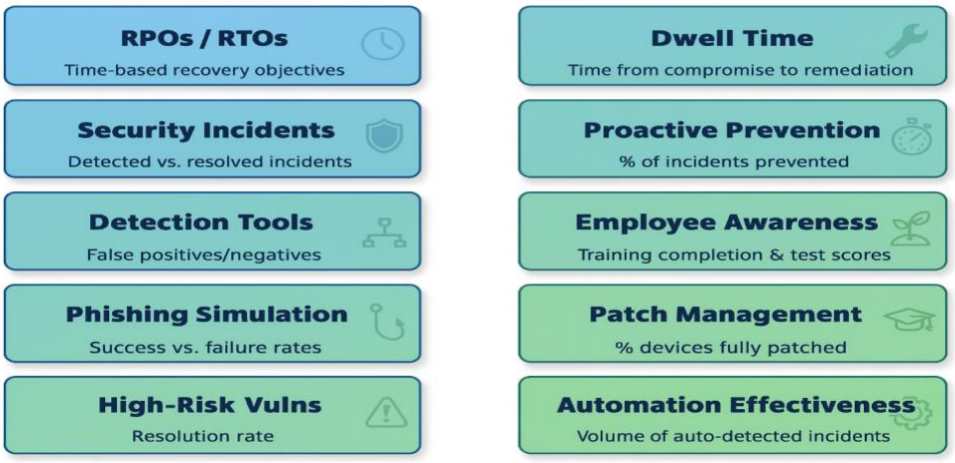
6.0.2 At a minimum, licensees and registrants must:

- **Accountability Documentation:** Define and record all cybersecurity roles, responsibilities, and reporting lines in policies and procedures.
- **Escalation Procedures:** Establish and test clear escalation pathways to ensure prompt communication and resolution of cybersecurity concerns.

6.0.3 In addition, licensees and registrants must provide the Board of Directors with regular reporting on cybersecurity effectiveness to ensure oversight and accountability. At a minimum:

- Reports on vulnerability testing must be submitted at least annually, or more frequently where risk exposure warrants.
- Senior Management must establish, track, and analyse key performance indicators (KPIs) and key risk indicators (KRIs) to provide high-visibility reports to the Board.
- As shown in Figure 4, metrics should include, where applicable:
    - RPOs and RTOs
    - Dwell time (time from compromise to full remediation)
    - Number of security incidents detected and resolved
    - Percentage of incidents prevented through proactive measures
    - Effectiveness of detection tools (false positives/false negatives)
    - Employee security awareness levels and training frequency
    - Results of simulated phishing exercises
    - Patch management coverage across devices
    - Resolution rate of high-risk vulnerabilities
    - Systems failing vulnerability scans
    - Volume of incidents detected and responded to through automation.

Figure 4: Cybersecurity KPI/KRI Dashboard



6.0.4 These documentation and escalation requirements form an integral part of the cyber risk governance and reporting framework, ensuring that material risks are visible at the highest levels of the organization and addressed in a timely manner.

7. INTERMEDIARY REQUIREMENTS

7.0.1 Insurance intermediaries licensed under the Act (including agents, brokers, and salespersons) are critical participants in the Bahamian insurance market. While insurance intermediaries may operate at a smaller scale than insurers, their role in handling sensitive policyholder data and facilitating market transactions requires the implementation of sound cybersecurity practices.

7.0.2 The requirements in this section constitute the primary cybersecurity obligations applicable to intermediaries. Other sections of these Guidelines apply to intermediaries only where explicitly stated or where relevant on a proportionate basis.

7.0.3 Intermediary obligations must be interpreted and applied proportionately, taking into account their scale, infrastructure, and reliance on third-party systems.

7.1 GOVERNANCE AND ACCOUNTABILITY

7.1.1 Intermediaries must designate a senior individual, partner, or officer with explicit responsibility for cybersecurity oversight. For larger intermediaries, cyber risk must be reported to the insurer(s) with whom it may be contracted to do business.

7.1.2 Governance frameworks must ensure accountability for policyholder data protection, incident escalation, and compliance with regulatory obligations.

7.2 CYBER RISK MANAGEMENT FRAMEWORK

7.2.1 Intermediaries must establish a documented cyber risk management program that identifies, assesses, and mitigates risks to confidentiality, integrity, and availability of data.

7.2.2 At a minimum, the framework must cover:

- Information security policies (passwords, access control, data handling).
- Threat and vulnerability assessments updated at least annually.
- Incident response and reporting procedures.
- Proportionate monitoring and review of cyber risks.

7.3 DATA PROTECTION AND PRIVACY

7.3.1 Intermediaries must comply with the *Data Protection Act, 2008* and ensure that customer information is collected, stored, transmitted, and disposed of securely.

7.3.2 Sensitive or personal data must be encrypted at rest and in transit, with access restricted to authorized personnel under the principle of least privilege.

7.3.3 Third-party service providers (e.g. IT vendors, cloud services) must be subject to appropriate due diligence, contracts, and ongoing oversight.

7.4 INCIDENT RESPONSE AND REPORTING

7.4.1 Intermediaries must maintain an incident response plan tailored to their scale of operations.

7.4.2 Any material cybersecurity incident that could impact policyholder data, business continuity, or regulatory compliance must be reported to the Commission **within 72 hours** of detection.

7.4.3 Records of all cyber incidents, investigations, and remedial actions must be maintained for supervisory review.

7.5 BUSINESS CONTINUITY AND RESILIENCE

7.5.1 Intermediaries must adopt proportionate business continuity and disaster recovery arrangements that include cyber scenarios (e.g. ransomware, data loss, system disruption).

7.5.2 Periodic testing of backups, failover procedures, and recovery objectives (RPO, RTO) must be carried out and documented.

7.6 TRAINING AND AWARENESS

7.6.1 Intermediaries must ensure that all staff receive annual cybersecurity training, with enhanced training for individuals handling sensitive data or possessing elevated system access.

7.6.2 Training must cover cyber hygiene, phishing awareness, secure data handling, and incident reporting responsibilities.

7.7 SUPERVISORY ENGAGEMENT AND CERTIFICATION

7.7.1 Intermediaries are required to complete the Commission's *Annual Cybersecurity Self-Certification* (Appendix 4).

7.7.2 The Commission may require intermediaries to submit self-assessments, undergo targeted supervisory reviews, or obtain independent assurance over their cybersecurity controls.

7.7.3 Failure to comply with intermediary cybersecurity requirements may result in enforcement measures under the Act, including conditions on licenses, administrative penalties, or suspension/revocation of registration.

7.8 ASSURANCE AND ATTESTATION

7.8.1. Intermediaries must implement proportionate processes to assess and demonstrate the effectiveness of their cybersecurity controls.

7.8.2. At a minimum:

- Intermediaries must complete an annual self-assessment (Appendix 4) and submit a certification of compliance to the Commission.
- Independent assessments are not expected to follow the same frequency or depth as insurers, but may be required where:
    - The Intermediary handles significant volumes of sensitive or personal data
    - There is material reliance on outsources or cloud-based systems, or
    - The Commission identifies elevated risk.
- Where appropriate, intermediaries may satisfy independent assurance expectations through:
    - Reliance on service provider assurance (e.g. SOC 2 reports)
    - Targeted external reviews, or
    - Other proportionate validation mechanisms.

7.8.3. The Commission will assess intermediary assurance arrangements based on risk exposure and outcomes, rather than prescriptive requirements.

8. CYBER HYGIENE

8.1 CYBER HYGIENE

8.1.1 Cyber hygiene refers to the routine practices and safeguards that reduce exposure to common cybersecurity threats. Weak hygiene practices increase the likelihood of:

- Security breaches from phishing, malware, and viruses.
- Data loss through hacking, corruption, or system compromise.
- Exploitation of outdated or unpatched software.
- Ineffective protection from outdated antivirus and malware tools.
- Misuse or abuse of elevated user privileges.

8.1.2 The Board must ensure that policies and procedures are established and enforced to embed cyber hygiene best practices across the organization. At a minimum, these must include:

- Regularly backing up important data, ensuring backups are encrypted, offline, and securely stored offsite.
- Enforcing strong, complex passwords that re updated regularly.
- Requiring connection only to secure and trusted Wi-Fi networks.
- Enabling multi-factor authentication (MFA) where possible.
- Applying the latest software patches from trusted sources.
- Restricting user permissions to the minimum necessary for each role.
- Installing reputable antivirus and anti-malware software and updating it regularly.
- Training users to recognize and report phishing, suspicious communications, and anomalous system activity.
- Exercising caution when sharing personal or sensitive information via phone, email, social media, or public channels.
- Encrypting messages, storage media, and devices that contain sensitive or confidential data.
- Reviewing and managing application privacy and security settings, including permissions to access device features and data.
- Securely deleting data from desktops and mobile devices before disposal, repurposing, donation, resale, or recycling.
- Ensuring that the use of Artificial Intelligence (AI) tools complies with internal data protection and cybersecurity policies. Users must avoid entering confidential, personal, or proprietary information into public or unverified AI systems, and any AI-enabled tools deployed within the organization must be formally approved, secured, and monitored for compliance.

8.1.3

8.1.4 Board members, Senior Management, IT administrators, and other privileged users must exercise heightened caution when reviewing incoming emails, text messages, or other electronic communications. Suspicious messages must not be opened, and links, attachments, or embedded content must not be accessed.

8.1.5 All user devices – including those used by Board members, Senior Management, IT administrators, or other privileged account holders – must be subject to controls that prevent unauthorized access to the financial institution's core network. As a default, portable storage media, personal computers, and internet-of-things devices must be blocked unless formally approved for use. Any approved devices or media must undergo routine security scanning.

9. APPENDIX

APPENDIX 1 – CYBER RESILIENCE PRINCIPLES (FSSC)[4]

Cyber resilience is essential for safeguarding financial stability. Financial institutions are expected to adopt these **10 Cyber Resilience Principles**, which serve as guiding concepts to manage cyber risks and enhance each institution's ability to safeguard its operations, assets, and reputation in an increasingly digital and interconnected financial system.

No.	Principle	Description	Focus Areas
1	**Not Just an IT Issue**	Cyber resilience must extend beyond information technology operations to include people, processes, data, and facilities	• Cyber Risk-Aware Culture • Integration with Business Strategy • Remote Working
2	**Legal Basis**	Boards and management must understand the legal implications of technology and cyber incidents, including data privacy, in relation to their specific circumstances.	• Legal and Regulatory Compliance
3	**Adequate Attention on Agenda**	Cyber risk must receive due attention at the board level, with adequate discussion time in meeting agendas to reduce exposure to direct losses, legal claims, reputational damage, ICT disruption, and misuse of technology. (See Appendix 2: 60 Must-Ask Questions at the Next Board Meeting to Strengthen Cybersecurity)	• Cybersecurity Strategy • Regular Reporting
4	**Accountability with Expertise**	An enterprise-wide Cyber Risk Governance framework must be integrated into organizational operations, supported with sufficient staffing, budgets, training, and recovery capabilities.	• Clear Roles and Responsibilities • Training and Awareness
5	**Transparent, Thorough and Targeted**	Board and management discussions should cover cyber risks to avoid, accept, mitigate, or transfer (e.g., through insurance), with specific plans aligned to each approach.	• Transparency • Performance Metrics • Threat Information Sharing
6	**Defence in Depth**	Multiple layers of security controls must be implemented, ensuring that if one layer is breached, others still provide protection	• Incident Response & Recovery
7	**Need-to-Know**	Access to information and resources must be restricted to individuals with a legitimate and specific need, reducing exposure to unauthorized access or data breaches.	• Risk Assessment and Mitigation
8	**Least Privilege**	Users and systems must be granted only the minimum access rights necessary to perform their tasks, limiting potential misuse or damage.	• Continuous Permissions Right Sizing
9	**Segregation of Duties**	Critical responsibilities should be divided among individuals or systems to prevent a single point of failure, conflict of interest, fraud, or unauthorized actions	• Sufficient Resources
10	**Security by Design**	Security must be integrated from the outset into software, systems, and product development, emphasizing proactive rather than reactive measures.	• Third-Party Management • Privacy as the Default

[4] Financial System Stability Committee. 2024. *Cyber Resilience Principles.* Financial System Stability Committee. Retrieved September 21, 2025 from: https://www.fscjamaica.org/wp-content/uploads/2024/03/Cyber-Resilience-Principles.pdf

APPENDIX 2 – COMMON CYBER ATTACKS[5]

ATTACK TYPE	DESCRIPTION	EXAMPLE TECHNIQUES
PHISHING	Mass emails sent to trick recipients into revealing sensitive information or visiting malicious sites.	Fake websites, credential theft emails.
WATERING HOLE	Fake or compromised websites designed to infect visitors' systems.	Malicious code injected into legitimate sites.
RANSOMWARE	Malware that encrypts files or systems and demands payment for decryption.	Disk-encrypting extortion malware.
SCANNING	Automated probing of large parts of the internet to find exploitable systems.	Network scanning, vulnerability scanning.
SPEAR-PHISHING	Targeted phishing aimed at specific individuals with tailored malicious emails.	Malicious attachments, Trojanised documents.
BOTNET / DDOS	Network of compromised devices used to flood targets with traffic.	Distributed Denial of Service attacks.
SUPPLY CHAIN ATTACK	Compromise of software, hardware, or service providers to infiltrate organizations.	Malicious updates, tampered components.
INSIDER THREATS	Employees/contractors intentionally or accidentally compromising security.	Misuse of access, social engineering.
BRUTE-FORCE ATTACK	Automated trial-and-error attempts to guess passwords or encryption keys to gain unauthorized access.	Password cracking, credential stuffing.
SQL INJECTION	Inserting malicious SQL commands into application input fields to manipulate or extract database information.	Injecting SQL queries into login or search fields
ZERO-DAY EXPLOIT	Exploitation of software vulnerabilities before a security patch or fix is available.	Exploiting unpatched operating systems or applications.
MALWARE	Malicious software designed to damage, disrupt, or gain unauthorized access to systems or data.	Trojans, ransomware, spyware, worms
MAN-IN-THE-MIDDLE (MITM)	Intercepting and altering communication between two parties without their knowledge.	Session hijacking, rogue Wi-Fi hotspots.
WHALE-PHISHING ATTACK	Targeted social-engineering attacks aimed at senior executives or high-profile users	CEO fraud emails, fake invoice requests.
DRIVE-BY ATTACK	Infection of devices when users visit compromised or malicious websites.	Malicious ads (malvertising), exploit kits.
DISTRUBUTED DENIAL-OF-SERVICE (DDOS)	Flooding systems or networks with traffic from multiple compromised devices to disrupt availability.	Botnet traffic floods, amplification attacks.
CLOUD CONFIGURATION ATTACKS	Exploiting misconfigured cloud services or storage leading to unauthorized access or data exposure.	Publicly exposed files, overly broad access, default cloud settings.
AI-ENABLED OF DEEPFAKE ATTACKS	Use of artificial intelligence to create realistic fake voices, images, or communications to deceive users.	Synthetic CEO voice calls, deepfake video impersonation.

[5] National Cyber Security Center. 2016. *Common Cyber Attacks: Reducing the Impact*. HM Government. Retrieved September 21, 2025, from: https://www.ncsc.gov.uk/files/common_cyber_attacks_ncsc.pdf

APPENDIX 3 – CYBER RISK IDENTIFICATION FORM

CYBER RISK IDENTIFICATION FORM

Section 1: General Information

- **Risk ID:** _____
- **Date Identified:** _____
- **Business Unit / Department:** _____
- **Risk Owner:** _____
- **Reviewer / Approver:** _____

Section 2: Risk Description

- **Risk Title:** _____
- **Risk Category (select one):**
  - ☐ Information Security
  - ☐ Data Privacy
  - ☐ Third-Party / Vendor Risk
  - ☐ IT Infrastructure
  - ☐ Business Continuity / Resilience
  - ☐ Regulatory / Compliance
  - ☐ Other: _____
- **Detailed Risk Description:**
  (Describe the cyber risk, potential causes, and how it could impact operations, assets, or reputation.)

Section 3: Threat & Vulnerability Assessment

- **Threat Source(s):**
  - ☐ External (hackers, cybercriminals, nation states)
  - ☐ Internal (employees, contractors)
  - ☐ Environmental (natural disasters, power outages)
  - ☐ Other: _____

- **Vulnerabilities Exploited:**
  (e.g., outdated software, weak access controls, inadequate training, supply chain gaps)

Section 4: Impact & Likelihood Assessment

- **Potential Impact Areas:**
  - ☐ Financial Loss
  - ☐ Reputational Damage
  - ☐ Operational Disruption
  - ☐ Legal / Regulatory Penalties
  - ☐ Data Loss / Breach
  - ☐ Customer Trust
- **Impact Level (select one):**
  - ☐ Low
  - ☐ Medium
  - ☐ High
  - ☐ Critical
- **Likelihood (select one):**
  - ☐ Rare
  - ☐ Unlikely
  - ☐ Possible
  - ☐ Likely
  - ☐ Almost Certain

Section 5: Risk Rating

- **Inherent Risk Score:** _____
  (Based on Impact × Likelihood before controls)
- **Current Controls in Place:**
  (List security measures, policies, or technologies mitigating this risk.)
- **Residual Risk Score:** _____
  (Risk remaining after applying current controls)

Section 6: Mitigation & Action Plan

- **Recommended Additional Controls:**
  (e.g., enhanced monitoring, training, patching, vendor assessment)
- **Responsible Party:** _____
- **Target Completion Date:** _____

- **Monitoring / Reporting Method:** _____

Section 7: Sign-Off

- **Risk Owner Signature:** _____
- **Reviewer Signature:** _____
- **Date:** _____

APPENDIX 4 – CYBERSECURITY SELF-ASSESSMENT FORM

INSURANCE COMMISSION OF THE BAHAMAS

CYBERSECURITY SELF-ASSESSMENT FORM

Organization Name: _____

Assessment Date: _____

Assessor(s): _____

Reviewed By: _____

SECTION 1: GOVERNANCE & CULTURE

1.1 Board Oversight

- ☐ The board regularly reviews cyber risk reports.
- ☐ Cyber risk is a standing item on the board agenda.
- ☐ Roles and responsibilities for cyber risk management are clearly defined.

1.2 Cyber Risk Culture

- ☐ Staff receive regular cybersecurity awareness training.
- ☐ Policies encourage reporting of suspicious activity without fear of reprisal.
- ☐ Senior management promotes cyber-risk aware behaviour.

Self-Assessment Rating (circle one):

1 – Not in place | 2 – Ad-hoc | 3 – Developing | 4 – Established | 5 – Optimized

---

SECTION 2: RISK MANAGEMENT & COMPLIANCE

2.1 Risk Identification

- ☐ Cyber risk assessments are conducted at least annually.
- ☐ Threat intelligence is incorporated into risk analysis.

2.2 Legal & Regulatory Compliance

- ☐ The organization complies with all applicable data protection and privacy laws.
- ☐ A legal review of cyber obligations is conducted regularly.

Self-Assessment Rating: 1 | 2 | 3 | 4 | 5

SECTION 3: SECURITY CONTROLS

3.1 Access Management

- ☐ User access follows “least privilege” principles.
- ☐ Access rights are reviewed periodically.
- ☐ Multi-factor authentication is enforced for critical systems.

3.2 Segregation of Duties

- ☐ Critical functions are split across multiple individuals/systems.
- ☐ High-risk transactions require dual authorization.

3.3 Security by Design

- ☐ Security requirements are integrated into system development lifecycle.
- ☐ Vendor risk assessments include cybersecurity criteria.

Self-Assessment Rating: 1 | 2 | 3 | 4 | 5

SECTION 4: RESILIENCE & INCIDENT RESPONSE

4.1 Defence in Depth

- ☐ Multiple security layers are in place (network, endpoint, application, data).
- ☐ Incident response and recovery procedures are documented and tested.

4.2 Business Continuity

- ☐ Cyber resilience is integrated into business continuity planning.
- ☐ Backups are performed, tested, and secured regularly.

Self-Assessment Rating: 1 | 2 | 3 | 4 | 5

SECTION 5: MONITORING & REPORTING

5.1 Performance Metrics

- ☐ Cyber risk metrics are defined and tracked.
- ☐ Reports are regularly shared with management and the board.

5.2 Threat Information Sharing

- ☐ The organization participates in industry cyber threat sharing groups.
- ☐ External threat intelligence feeds are integrated into monitoring.

Self-Assessment Rating: 1 | 2 | 3 | 4 | 5

SECTION 6: OVERALL RATING

Average Score: _____

Cyber Resilience Level (based on average):

- 1–2 = Initial / Ad-hoc

- 2–3 = Developing
- 3–4 = Established
- 4–5 = Leading / Optimized

- **Section 7: Action Plan**
- **Top 3 Priority Gaps Identified:**
    1. _____
    2. _____
    3. _____
- **Recommended Actions:**
    - _____
    - _____

- **Responsible Party:** _____

- **Target Completion Date:** _____

APPENDIX 5 – ANNUAL CYBERSECURITY SELF- CERTIFICATION

ANNUAL CYBERSECURITY SELF - CERTIFICATION

Date: _____

Licensee/Registration Name: _____

Registration Number: _____

Reporting Period: _____

Certification Statement:

As an authorized officer of _____, I certify that the information provided below accurately reflects the cybersecurity practices and conditions of the organization during the reporting period, including any areas where requirements have not been fully met.

1. We have taken reasonable steps to identify and manage cybersecurity risks appropriate to the size, nature, and complexity of our business.
2. We have a basic Information Security Policy in place covering:
    - Password protection and access control,
    - Employee awareness of cyber risks,
    - Procedures for reporting suspicious cyber activity.
3. We have identified critical third-party providers (if any) and taken reasonable steps to verify their cybersecurity practices.
4. To the best of my knowledge, no material cybersecurity incident has occurred during the reporting period that has not been reported to the Insurance Commission of The Bahamas.
5. We have performed a cyber security self-assessment against and currently operate at:
   Cyber Resilience Level: _____
6. Explanation of Non-Compliance (if applicable):

   If the licensee/registrant has not fully met any of the certification items above, please provide a brief explanation below, including:

    - The specific item(s) not met
    - The reasons for non-compliance
    - Any mitigating measures in place
    - The planned actions and timeline for achieving compliance

_____

_____

_____

Declaration

I, the undersigned, hereby certify that the information provided in this self-assessment is accurate and complete to the best of my knowledge. This assessment reflects the organization's current state of implementation of cybersecurity measures in accordance with the guidelines set forth by the Insurance Commission of The Bahamas.

Title: _____

Signature: _____

APPENDIX 6 – INDUSTRY STANDARDS & CONTROL FRAMEWORKS

1. NIST Cybersecurity Framework (CSF) 2.0[6]

The NIST CSF 2.0 provides organizations with a flexible and voluntary framework to identify, assess, and manage cybersecurity risks. It is widely adopted across industries and governments as a baseline for building resilient cybersecurity programs. The framework is organized into three key components:

- **CSF Core** – A taxonomy of high-level cybersecurity outcomes organized into six **Functions**:
  - **Govern (GV):** Establish and oversee cybersecurity risk management strategy, policies, and supply chain considerations.
  - **Identify (ID):** Maintain awareness of assets, vulnerabilities, threats, and organizational risks.
  - **Protect (PR):** Implement safeguards such as access control, training, data protection, and resilient infrastructure.
  - **Detect (DE):** Monitor systems continuously to identify anomalies, compromises, and incidents.
  - **Respond (RS):** Contain and mitigate cybersecurity incidents, coordinate communication, and conduct incident analysis.
  - **Recover (RC):** Restore impacted systems, services, and data, ensuring continuity of operations.

- **Profiles** – Represent an organization's **Current Profile** (existing posture) and **Target Profile** (desired state). Profiles enable organizations to perform gap analyses, prioritize improvements, and communicate risk management strategies internally and externally.

- **Tiers** – Characterize the maturity of an organization's cybersecurity governance and practices, ranging from **Tier 1 (Partial)** to **Tier 4 (Adaptive)**. Higher tiers reflect formalized, continuously improving practices integrated with enterprise risk management.

2. Integration with Other Standards and Practices

The CSF references and aligns with global standards and best practices, including:

- **NIST SP 800-53** (*Security and Privacy Controls for Information Systems and Organizations*) for control selection.
- **NIST Risk Management Framework (SP 800-37 and SP 800-30)** for structured risk assessment.
- **ISO/IEC 27001** for international information security management systems (ISMS).
- **Supply Chain Risk Management (SP 800-161r1)** for managing third-party and vendor risks.
- **Privacy and Emerging Technologies Frameworks**, including the NIST Privacy Framework and AI Risk Management Framework, to address evolving areas such as data protection and artificial intelligence.

3. Practical Applications

- Provides a **common language** for cybersecurity across technical and executive teams.
- Enables **benchmarking and maturity assessments** via Profiles and Tiers.
- Supports **regulatory compliance** and industry-specific adaptation.
- Encourages continuous improvement and resilience against evolving cyber threats.

[6] National Institute of Standards and Technology. 2024. *The NIST Cybersecurity Framework (CSF) 2.0*. (NIST Cybersecurity White Paper, NIST CSWP 29). US Department of Commerce. Retrieved September 22, 2025, from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf