# NATIONAL RESERVE BANK OF TONGA

## Prudential Banking Standard No. 15 - 2021

## Cybersecurity

**Contents**

## INTRODUCTION

### General stipulations

This Prudential Banking Standard is issued under Section 20(3) of the Banking Act 2020 and forms part of the [National Reserve Bank of Tonga] standards governing the conduct of Banks in Tonga.

In preparing the requirements of this Prudential Banking Standard, reference has been made to the recommendations of international financial sector supervisory standard setters and international sound practices and standards on cybersecurity.

### Objectives and key requirements

This Prudential Banking Standard aims to ensure that Banks have in place a cybersecurity governance and risk management framework commensurate with the Bank's inherent cybersecurity risk, so as to ensure the business impact from the occurrence of cybersecurity vulnerabilities or cybersecurity incidents are kept to a minimum and are within the Bank's risk tolerance levels.

Key requirements of this Prudential Banking Standard are that the Board of an LFI is ultimately responsible for ensuring prudent and comprehensive cybersecurity risk management of the institution, and that the LFI must:

- establish and maintain a comprehensive and effective cybersecurity risk management framework;
- clearly define the cybersecurity-related roles and responsibilities of the Board, senior management, governing bodies and individuals;
- maintain a cybersecurity capability commensurate with the size and extent of threats to its information assets;
- implement controls to protect its information assets commensurate with the criticality and sensitivity of those information assets, and undertake systematic testing and assurance regarding the effectiveness of those controls; and
- minimise the likelihood and impact of cybersecurity incidents on the confidentiality, integrity or availability of information assets, including information assets managed by related parties or third-parties.

### Applicability

This Prudential Banking Standard applies to all entities licensed under the National Reserve Bank Act

### Definition of terms

*availability* - timely and reliable access to and use of information

*confidentiality* - access being restricted only to those individuals, entities or processes authorised

*criticality* - the degree of importance to potential loss of availability

*cybersecurity* – controls and processes to preserve the confidentiality, integrity and availability of information assets

*cybersecurity capability* - the totality of resources, skills and controls which provide the ability and capacity to maintain information security;

*cybersecurity control* - a prevention, detection or response measure to reduce the likelihood or impact of an information security incident;

*cybersecurity incident* – an actual or potential compromise of the confidentiality, integrity or availability of an institution's system or data

*cybersecurity policy framework* - the totality of policies, standards, guidelines and procedures pertaining to information security;

*cybersecurity threat* - a circumstance or event that has the potential to expose an information security vulnerability;

*cybersecurity vulnerability* - weakness in an information asset or information security control that could be exploited to compromise information security;

*data at rest* - data held or stored on some form of storage system

*data in transit or motion* - means data being transferred over some form of communication link.

*data in use* - means data that is being accessed or used by a system at a point in time.

*firewall* **-** system or combination of systems that enforces a boundary between two or more networks typically forming a barrier between a secure and an open environment such as the Internet;

*information asset* - information and information technology, including software, hardware and data (both soft and hard copy);

*integrity* - completeness, accuracy and freedom from unauthorised change or usage;

*sensitivity* - the potential impact of a loss of confidentiality or integrity.

*malware* - a collective term used to describe a variety of malicious programs (including viruses, worms, Trojan horses, ransomware, spyware, adware, shareware etc.) designed to spread and replicate from computer to computer through communications links or through sharing of electronic files to interfere with or damage computer operation.

*material activities* - activities of such importance that have a significant impact on the banking institution's business operations or its ability to manage risks effectively should such activities be disrupted;

*need to know basis* - the restriction of sensitive data using a tight security method in which information is only given to those who need it, to do a particular task

*penetration testing* - the practice of testing a computer system, network or web application for security weaknesses or vulnerabilities that might potentially be exploited

*Software System End of Life* – with respect to a software product, indicating that the product is in the end of its useful life

*vulnerability assessment* - the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system

**References**

This Prudential Banking Standard should be applied in conjunction with the Operational Risk Management Prudential Banking Standard

**GOVERNANCE**

**Cybersecurity risk management**

1. Banks must have in place a framework for cybersecurity risk management (CSRMF) and this should be an integral part of the Bank's enterprise risk management framework. A comprehensive and effective CSRMF must at a minimum include:
    a) clear definition of the elements of cybersecurity governance such as organisation structures, roles and responsibilities and reporting lines;
    b) a formally documented statement of the Board's cybersecurity risk tolerance;
    c) cybersecurity risk assessment methodology and tools;
    d) cybersecurity processes which considers identification, protection, detection, response and recovery functions;
    e) process for reviewing the effectiveness of the framework, and continuous improvement and learning process; and
    f) three lines of defense risk management for cybersecurity.

2. A~~n~~ Bank's CSRMF must be documented and approved by the Board. The CSRMF must be reviewed regularly.

3. Banks must have a designated cybersecurity risk management function, that, at a minimum:
    a) is responsible for assisting the Board, board committees and senior management of the institution to maintain CSRMF;
    b) is appropriate to the size, business mix and complexity of the LFI;
    c) has independent reporting lines to the Board, board committees and senior management of the institution, so to conduct its risk management activities in an effective and independent manner;

d) is resourced with staff who possess appropriate experience and qualifications to exercise their responsibilities;
e) is headed by a person designated as the Chief Information Security Officer (CISO) or an equivalent senior officer of the LFI;
f) includes a formally documented statement of the Board's cybersecurity risk tolerance;
g) includes risk assessment methodology and tools;
h) includes cybersecurity processes which considers identification, protection, detection, response and recovery functions;
i) includes process for reviewing the effectiveness of the framework, and continuous improvement and learning process; and
j) includes three lines of defense risk management for cybersecurity.

4. Banks which are subsidiaries or branches may adopt the CSRMF of their parent, but the minimum requirements of this standard must be complied with on a standalone entity basis.

**Cybersecurity strategy**

5. Banks must develop and document an enterprise wide cybersecurity risk strategy, approved by the Board.

6. The strategy must:
   a) outline the cybersecurity risk concept and the cybersecurity challenges facing the LFI;
   b) explain the Bank's overall approach to cybersecurity risk management and how this aligns to the Bank's business strategy;
   c) include key elements of the Bank's cybersecurity risk management objectives, principles and implementation;
   d) be aligned with the Board's established and documented cybersecurity risk tolerance;
   e) establish a plan for cybersecurity risk management to identify, assess and control cybersecurity threats covering people, process, technologies and policies.

7. Banks must conduct regular reviews of its cybersecurity strategy to ensure the strategy remains relevant and current to the Bank's overall business strategy and risk tolerances.

**Policy framework**

8. Banks must have in place a cybersecurity policy framework commensurate with its exposures to vulnerabilities and threats, covering policies and procedures for cybersecurity risk identification, measurement, monitoring and control.

9. Cybersecurity policies and procedures must cover requirements arising from the Bank's business strategy, regulatory framework and the current and projected cybersecurity threat environment.

10. The cybersecurity policy framework should cover, inter alia:

a) information asset management;
b) access control;
c) physical and environmental security;
d) end user management;
e) cryptography;
f) operations security;
g) communication;
h) system development;
i) third-party relationships;
j) incident management;
k) business continuity; and
l) regulatory compliance.

11. Banks should review and update cybersecurity policies and procedures at least annually or when major changes occur in its security environment.

**Roles and Responsibilities**

12. The Board and senior management of an LFI must ensure that a sound and robust CSRMF is established and maintained.

13. The Board of an LFI is ultimately responsible for the institution's CSRMF and is responsible for the oversight of its operation by management, and must, inter alia:
    a) approve the CSRMF;
    b) approve the institution's cybersecurity strategy (CSS);
    c) set and formally document the cyber security risk tolerance;
    d) approve cyber security policies and procedures;
    e) ensure receipt of information on the cyber security risk profile of the institution, including significant cyber security incidents; and
    f) ensure the CSRMF is subject to effective and comprehensive audits and testing.

14. Senior management of an LFI is responsible for implementing and maintaining the CSRMF consistent with the Board's cybersecurity risk tolerance, and must, inter alia:
    a) ensure sufficient resources are available for effective operation of the cyber security risk management framework;
    b) develop and maintain a comprehensive cyber security policy framework, and ensure that policies and procedures are clearly communicated throughout the institution;
    c) maintain a process of continuous assessment of the institution's cyber security risk profile and associated periodic reporting;
    d) periodically review, assess and enhance the effectives of the CSRMF; and
    e) establish the institution's cybersecurity strategy (CSS).

15. The Chief Information Security Officer (CISO) (or equivalent) of an LFI is responsible for:

a) managing the CSRMF;
b) developing and enhancing the CSRMF;
c) ensuring the consistent application of policies and standards across all technology projects, systems and services;
d) providing leadership to the Bank's cybersecurity organization;
e) partnering with business stakeholders across the company to raise awareness of cybersecurity risk management concerns;
f) assisting with the overall Bank's technology planning, providing a current knowledge and future vision of technology and systems.

16. The internal auditor of an LFI is responsible for conducting periodic cybersecurity risk assurance audit of the LFI and this should include testing of the cybersecurity environment of the LFI.

17. The compliance manager of an LFI is responsible for conducting compliance assessment on the cybersecurity risk policy framework of the LFI.

## HUMAN RESOURCES

### Screening and background checks

18. Banks must have a comprehensive screening and background checking process for prospective employees and contractors, that covers relevant laws, regulations and ethics.

19. Banks must have in place documented policy and controls regarding recruitment and hiring of personnel (including employees and suppliers), identity and access management, and segregation of duties, employee mobility, transfer and leave.

20. The screening and background checking process of the LFI should be proportional to the business requirements, sensitivity of the information to be handled and the perceived risks.

### Necessary competence

21. Banks must have employment guidelines to ensure that all employees hired for cybersecurity related roles have the necessary skills and experience to perform the role in a trusted, competent manner.

### Security awareness program

22. Banks must have a cybersecurity awareness and training program to ensure that all employees and contractors are aware of their responsibilities for cybersecurity and how those responsibilities are to be discharged.

23. The cybersecurity awareness and training program must encompass the entire range of target audiences, including employees, managers, developers, system and infrastructure administrators, external entities, suppliers and customers.

24. Cybersecurity awareness training should be conducted at least annually.

25. The cybersecurity awareness and training should be conducted when employees are transferred to a new position or roles with substantially different cybersecurity requirements and during the onboarding of employees.

### Contractors

26. Banks must have a policy and associated written guidelines on engaging contractors to critical information technology operations and cybersecurity functions. The guidelines at a minimum must include:
    a) screening and background checks;
    b) communication protocols;
    c) terms and conditions of the engagement;
    d) compliance to FI's code of conduct;
    e) confidentiality and non-disclosure agreements; and
    f) fit and proper criteria.

## ASSET MANAGEMENT

### Asset inventory and ownership

27. Banks must ensure that all information, information processing and communication assets are identified and inventoried. The inventory of these assets should be drawn up, maintained accurately and kept up to date.

28. Ownership of information assets maintained in the inventory must be appropriately assigned. The asset owners should:
    a) define protection requirements for the assets owned, be accountable for these protection requirements and ensure regular review[1]; and
    b) identify assets critical to the continued operation of the institution to ensure commensurate protection.

### Information classification

29. Banks must define and have in place a Board approved information asset classification scheme. The classification scheme, at a minimum, must:
    a) include confidentiality, integrity, and availability requirements for each category; and
    b) have institution wide applicability.

30. Information assets that are in the highest protection category, at a minimum, should be labelled regardless of their format (physical or electronic).

[1] For information assets, at a minimum, protection must be defined in terms of confidentiality, integrity, and availability requirements.

### Media handling

31. Banks must have appropriate policies and procedures in place to prevent unauthorised access, modification, removal or destruction of media used for the storage of information assets.

## ACCESS CONTROL

### Principles of access control

32. Banks must establish, document and implement relevant policies and procedures to control access to information assets and information processing and transmitting facilities.

33. The policies must align to international best practice standards and at a minimum include:
    a) information dissemination and authorisation (for example the "need to know" and "default deny" principles, information security levels and classification of information);
    b) application of segregation of duties principles commensurate with the size and complexity of the institution and the risk level of the operations and functionalities involved; and
    c) clearly defined roles and responsibilities.

### User access management

34. Banks must establish, document and implement relevant policies, and procedures to address the following:
    a) user identification (ID) (account) lifecycle management including creation, modification, suspension and deletion of user identities;
    b) access rights lifecycle management, including requesting, approving, granting, changing and revoking access rights;
    c) appropriate recording of audit trails for all access rights related activities;
    d) user IDs and access rights activities must be regularly (at least annually) reviewed and any discrepancy with policies promptly followed up, resolved and appropriately reported;
    e) requirements for secret authentication information for all user IDs compliant with defined and enforced complexity requirements and expiration times, that effectively mitigate the risk of uncovering them;
    f) requirements for privileged access rights assigned to user IDs different from those used for regular business or ICT related activities must include:
        i. the number of user IDs with privileged access rights must be kept at the minimum possible;
        ii. to the extent possible privileged user ID must be set up with strong (i.e. two-factor or three-factor) authentication; and
        iii. activities performed using privileged access rights should be subject to close monitoring.
    g) requirements for the use of generic administration user IDs limiting usage to the extent possible.

## CRYPTOGRAPHY

### Use of cryptography to protect sensitive data

35. Banks must have a comprehensive policy on the use of cryptography for protection of confidentiality, authenticity and integrity of information. The policy at a minimum must include:
    a) senior management's approach towards the use of cryptographic controls across the institution;
    b) use of encryption (e.g. end-to-end encryption) and authentication measures on a risk-based basis to safeguard data during transmission across open and public networks as per the institution's classification scheme on criticality and sensitivity of information;
    c) the use of encryption for protection of information transported through devices and equipment;
    d) methods to deal with the protection of cryptographic keys and the recovery of encrypted information in the case of lost, compromised and damaged keys; and
    e) vetting functions involving cryptographic algorithms and crypto-key configurations for deficiencies and loopholes.

### Key management

36. Banks must have a key management policy to ensure that cryptographic Keys are secure through their whole life cycle. The policy at a minimum to include:
    a) methods for generating keys for different cryptographic systems and different applications and disposal of materials used in the generation of Keys;
    b) hardware security modules and keying materials are physically and logically protected;
    c) procedures for issuing and obtaining public Key certificates;
    d) storing Keys, including how authorised users obtain access to Keys;
    e) procedures on exchanging or updating Keys upon expiry, including rules when Keys should be changed and how this will be done;
    f) dealings with compromised Keys, revoking Keys, lost Keys and backing up or archiving Keys; and
    g) when cryptographic Keys are being used or transmitted, the FI should ensure that these keys are not exposed during usage and transmission.

37. Cryptographic Keys should be used for a single purpose to reduce the impact of an exposure of a Key.

38. Banks should consider and decide the appropriate lifetime (validity period) of each cryptographic Key[2].

[2] The sensitivity of data and operational criticality should determine the frequency of Key changes.

## PHYSICAL AND ENVIRONMENTAL CONTROLS

### Physical security of information processing facilities

39. Banks must define security perimeters to protect areas that contain sensitive or critical information and information processing facilities.

40. Physical and logical access to data centre and systems should be permitted only for individuals who are identified and authorised, and authorisation should be limited only to those with a legitimate business need for such access according to job responsibilities.

41. Physical access of staff to the data centre should be revoked immediately if it is no longer required.

42. Banks must ensure that there is proper notification of and approval for third-parties who requires temporary access to the data centre to perform maintenance or other approved work.

43. Banks must ensure that visitors or third-parties are accompanied at all times by an authorised employee while in the data center.

44. Banks must ensure that the data centre building, facility, and equipment room are physically secured and monitored at all times and deploy security systems and surveillance tools, as appropriate.

### Physical entry controls

45. Banks must ensure secure areas are protected by effective entry controls that only allow access to authorised personnel at all times.

46. Banks must maintain a physical log book for recording physical movements in the data centre for all personnel access, including information technology personnel, visitors and third-parties.

47. The log book should be reviewed regularly for suspicious access.

48. The access rights to data centre should be regularly reviewed and updated and revoked when necessary.

49. Banks should conduct spot checks on the physical security of the information processing facilities of the institution.

50. Banks must verify that adequate physical security measures are implemented at third-party payment kiosks, which accept and process the Bank's payment cards.

### Equipment protection

51. Banks must have adequate controls in place for equipment and devices issued to employees to prevent loss, damage, theft or compromise of equipment and devices and interruption to the institution's operations.

52. Banks should also have adequate controls in place for:
    a) maintenance of the equipment and devices;
    b) removal of equipment and devices;
    c) security of equipment and devices off-premises;
    d) secure disposal or re-use of equipment and devices; and
    e) unattended user equipment and devices.

### Clear desk policy

53. Banks must have and implement a clear desk policy for all personnel, that includes papers and removable storage media.

54. Banks must have a clear screen policy for at least the information processing facilities.

## OPERATIONS SECURITY

### Operational procedures and responsibilities

55. Banks must have formal documented procedures for operational activities relating to information processing and communication facilities; including:
    a) computer start-up and close-down procedures;
    b) equipment maintenance;
    c) operation and management of media; and
    d) mail management.

56. Operational procedures should clearly identify management responsibilities and controls over all changes relating to information processing and communication facilities[3].

57. Banks must implement appropriate monitoring systems for the use of all information technology resources, to ensure effective operational control of information processing and communication facilities.

58. To ensure sufficient operational capacity, Banks must monitor the volume of use of information processing and communication facilities and project and manage future capacity requirements.

[3] In this regard, Banks should maintain a register of these changes.

59. Commensurate to the level of risks inherent in an information system, Banks must ensure that there is an adequate segregation and separation of duties for systems development, testing and operational environments.

**Malware protection**

60. Banks must ensure that all information processing and communication facilities have up-to-date malware protection mechanisms.

**Backup**

61. Banks must maintain information backup facilities ensuring that significant information and software can be recovered following an operational failure, disruption or disaster.

62. Banks must ensure backup duplicates of data, applications, and system images are taken and tested regularly in accordance with documented and approved backup policy and procedures.

63. Banks must ensure that the backup policy and procedures are based on defined data loss tolerances and recovery requirements and address retention and protection requirements.

64. Banks' backups must be accessible at a remote location that is unlikely to be affected by the same operational failure, disruption or disaster event as the main processing site.

65. In cases of critical assets, backups must cover all information necessary for a comprehensive recovery in the event of an operational failure, disruption or disaster.

**Logging and monitoring**

66. Banks must keep and regularly review event logs that record user activities (including system administrators), exceptions, faults and information security events.

67. Event logs must:
    a) be protected against unauthorised access, tampering, and data loss (including by system administrators); and
    b) be subject to privacy controls.

68. Banks must ensure all clocks of data processing and communication services are automatically synchronized to a single reference time source.

**Software installation**

69. Banks must have in place documented policies and procedures to control changes to software on operational systems.

70. All installation and systems upgrades and updates must be assessed, approved, implemented and reviewed in a controlled manner, in accordance with documented policies and procedures.

71. Banks must have stated strategies and plans for Software System End of Life in the institution.

72. Banks must adopt and enforce policies to control types of software and updates users may install.

**Vulnerability management**

73. Information about technical vulnerabilities of information systems must be obtained in a timely fashion.

74. Banks' exposure to such security vulnerabilities are to be evaluated and appropriate measures are to be implemented to address the associated security risks.

75. Banks must establish the roles and responsibilities associated with vulnerability management, including vulnerability monitoring, vulnerability risk assessment and the installation of security updates.

76. Banks should install all relevant security updates to software on operational systems without undue delay and prioritizing high risk systems.

77. Banks must test and evaluate security updates before installation on critical systems for effectiveness and undesired side effects.

78. If installing a security patch would result in side effects that cannot be tolerated, or a security update is not available, then compensating controls must be implemented to mitigate the resulting exposure.

**COMMUNICATIONS SECURITY**

79. Banks must have in place controls to ensure the security of information in networks and the protection of connected services from unauthorised access, including:
    a) documented and approved responsibilities and procedures for the management of networks;
    b) controls to ensure confidentiality and integrity of data transmitted over networks not controlled by the institution, or wireless networks;
    c) restrictions on system connections to the networks; and
    d) authentication of systems on the network.

80. Network services' security mechanisms, service level requirements and required management services, must be identified and be subject to documented service level agreements, whether services are provided internally or outsourced.

81. Banks deploying Wireless Local Area Networks (WLAN) within the institution must take measures to mitigate the risks associated in this environment, such as having secure communication protocols for transmissions between access points and wireless clients.

82. Groups of users and information systems must be segregated based on an assessment of the security requirements of each group.

83. Access between such segregated groups and between the institution's network and any third-party network must be controlled and restricted on a business need basis.

84. Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities, in particular electronic messaging.

**SYSTEMS ACQUISITION AND DEVELOPMENT LIFECYCLE**

85. Banks must ensure that information security related requirements are considered when acquiring new information systems or enhancing existing information systems.

86. Banks must have in place effective controls to ensure that information (such as payments, internet banking or mobile banking apps) are protected from fraudulent activities, contract dispute and unauthorised disclosure and modification.

87. Rules for the development of software and systems, including mandatory security requirements, must be established by the Banks and applied to developments within the institution.

88. Secure system engineering principles, coding standards and programming techniques must be adopted by the Banks and used in the system development process.

89. Banks must ensure that changes to systems within the development lifecycle are controlled by the use of formal change control procedures and the modifications to software packages are limited to necessary changes under a strict control environment.

90. Banks should establish and appropriately protect secure development environments that cover the entire system development lifecycle. In addition, Banks should supervise and monitor outsourced system development activities.

91. During the systems development phase, testing of security functionality should be carried out.

**THIRD-PARTY RELATIONSHIPS**

92. The use of third-party services must not in any way result in any weakening of the cybersecurity control environment of the institution or the assurance over its effectiveness.

93. Banks must develop and implement a third-party relationship policy that mandates cybersecurity controls to address the risk posed by third-party access to its information assets.

94. Banks must review the security policies, procedures and controls of third-parties that have access to its information assets, on a regular basis, including commissioning or obtaining periodic expert reports on the adequacy of the cybersecurity control environment and compliance to applicable regulation.

95. The third-party relationship policy must, at the minimum include:

    a) appropriate due diligence processes for the appointment of a third-party service provider to determine its viability, reliability, credential and financial position;
    b) limited third-party access with time limitations[4]; and
    c) management of changes to the provision of services by third-parties taking it into account the criticality of business information, systems and processes involved and reassessment of risks.

96. Banks must establish an effective service level agreement for any services provided by third-parties that in any way requires or provides access to the Bank's information assets.

97. The service level agreement must include provisions in relation to cybersecurity that ensures the effectiveness of the Bank's cybersecurity controls are maintained.

98. Third-party agreements must include clauses that reserves the right of the LFI and the [Authority] to conduct audits, including on-site inspections of the activities, systems, sites, and facilities that are relevant to the provision of the contracted services.

**INCIDENT MANAGEMENT**

99. Banks must have a cybersecurity incident management process governed by documented policy and procedures with the objective of restoring normal service as quickly as possible following an incident, and with minimal impact to the its business operations.

100. The cybersecurity incident management policy and procedures must at a minimum:
    a) define what constitutes a cybersecurity incident and the criteria for incident categorization, including criteria for categorizing an incident as a crisis;
    b) prioritize resolution based on defined severity levels;

[4] Such access must be monitored and periodically reviewed.

c) address clear accountability and communication strategies to limit the impact of information security incidents[5];
d) address evidence collection and preservation;
e) address the testing of the incident management process;
f) address employees' requirements to notify on incidents or indicators of possible incidents; and
g) clear and effective coordination with supervisory body, police and national cybersecurity organizations.

**SECURITY AUDIT AND TESTING**

101. Banks are required to ensure that its approach to managing information security and its implementation, including the objectives, controls, policy, processes and procedure for information security, are reviewed independently at planned intervals or when significant changes occur.

102. Banks must ensure that an operationally independent and adequately resourced internal audit function covers review of the CSRMF.

103. To ensure that cybersecurity is implemented and operated in accordance with the Banks policies and procedures, the following minimum security audit and testing requirements are to be observed:
a) conduct security audits and tests, including vulnerability scans and penetration tests at regular intervals at a minimum for high risk systems and processes, and before such systems are introduced (put in production);
b) internal audit function to perform or commission security audits and tests at regular intervals (at least annually) according to their independent risk assessment; and
c) ensure that the internal audit function is sufficiently resourced, at a minimum to effectively assess the audits' and tests' planning, execution and reporting.

**CYBERSECURITY CONSIDERATIONS OF BUSINESS CONTINUITY MANAGEMENT**

104. Information security continuity must be embedded in the Banks business continuity management system and at a minimum should include the following requirements:
a) determine their requirements for cybersecurity and the continuity of cybersecurity risk management in adverse situations, e.g. during a crisis or disaster; and
b) establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for cybersecurity during an adverse situation.

[5] This to include escalation and reporting requirements to senior management, the board, external stakeholders and dealing with the mass media where appropriate.

## REGULATORY REPORTING

105. Banks are required to provide the following reports on cybersecurity:
- Quarterly reporting on all cybersecurity incidents in the format prescribed attached as Appendix I

106. Banks must notify the [National Reserve Bank of Tonga] as soon as possible but not later than sixty minutes after becoming aware of an information security incident that materially affects or has the potential to materially affect financially or non-financially the institution or the interests of depositors.

## COMPLIANCE WITH PRUDENTIAL BANKING STANDARD 15

107. This statement is effective from **1st July 2021** "Non-compliance with the requirements of this Prudential Banking Standard will be subject to corrective actions as provided under section 39 of the Banking Act 2020 and the administrative penalties outlined in Prudential Banking Standard No.3 Administrative Penalties.

## EFFECTIVE DATE

**108.** This guideline applies to Banks licensed under the Act and will be effective from **1st July, 2021.**

**Appendix I**

Form QCR **Quarterly Reporting on Cybersecurity Risk Incidents**

| **Reporting Institution Name** | | | **Reporting Quarter** | | | |
|---|---|---|---|---|---|---|
| **Cyber security root cause Areas** | **Event** | | **Incident** | | | |
| | **Number** | **Value of Loss** | **Number** | **Value of Loss** | **No. Unresolved from prior period** | **No. Resolved this Qtr.** |
| Asset Management | | | | | | |
| Access Controls | | | | | | |
| Operations Security | | | | | | |
| Communication Security | | | | | | |
| System Acquisition, Development & Maintenance | | | | | | |
| Third Party relationships | | | | | | |
| Information Sec. BCM | | | | | | |
| Human Resource | | | | | | |
| Cryptography | | | | | | |
| Physical & Environmental | | | | | | |
| **Total** | | | | | | |