NRB Guidlines

Banking Security

Nepal Rastra Bank

Information Technology Guidelines

Intent

New delivery channels such as ATM, internet banking, mobile banking have increased the risk of financial loss and electronic frauds along with other banking risks. Technology risk is not only concerned with operation risk of the bank, other banking risks like credit risk, reputation risk, compliance risk, market risk, strategic risk are also increased due to it. Moreover; emerging concept such as virtualization, data centre and disaster recovery site hosting, security outsourcing etc. have also increased the challenges of dealing with these issues.

Technology has also given new avenue for cyber fraud and the modus operandi of fraud from both internal staffs and external parties have been changing. Frauds related to debit and credit card, ATM, internet banking and mobile banking are emerging in present financial organization in the world.

In this scenario, NRB has felt necessary to regulate and guide IT related activities in commercial

GRC

5. IT related risk should also be considered in the risk management policy or operational risk policy of the bank and it should cover all e-banking activities and supplier activities as well. Periodic update of risk management is essential.

6. Banks are encouraged to implement international IT control framework such as COBIT[ii] as applicable to their IT environment.

7. The board should be adequately aware of the IT resources of the bank and ensure that it is sufficient to meet the business requirement.

8. Bank should designate a senior official of the bank as Information Security Officer (ISO) who will be responsible for enforcing information security policy of the bank. ISO will also

Oversight and CIA

2. Bank should conduct Risk Assessment periodically (at least annually) for each asset that has possibility of impacting the CIA[iii] of the information of the bank.

3. Bank should take necessary measures to ensure that all of its employees, consultants and contractors are aware of information security policy of the bank and comply with it and can be done by clear job description, employee agreements, policy awareness and its acknowledgements.

4. Access authorization for information of the bank should be in "need to know" basis and with least privilege and it should be for required time only. Bank should closely supervise individuals with privilege access to the system. With their system activities logged, access to system by privilege users should be done by more strong controls and security practices.

5. Banks should implement appropriate physical and environment controls taking into consideration of threats, and based on the entity's unique geographical location, building configuration, neighboring entities etc to secure critical hardware, system and information.

6. Since information security is not one time activity and cannot be gained by just purchasing and installing suitable hardware or software, bank should institutionalize processes to regularly assess the security health of the organization and detect and fix the vulnerabilities. It is recommended to conduct penetration testing of the system periodically.

Privileged access

19. Employee with privilege access such as system administrator, security officer or officer of other critical system should be scrutinized additional screening process such as background check, credit check etc before assigning in their respective job.

20. Bank should have data security policy and procedure in place to ensure security of data stored or transmitted electronically. This should cover, among other things appropriate data disposal procedure, storage of data in portable devices, security of media while in transit or in storage, physical and environmental control of storage media, encryption of customer's critical information being transmitted, transported or delivered to other locations.

New channels – mobile security

27. Online payment by using card should be authenticated using second factor and instant alert should be provided to customers using email/SMS/automated voice call.

28. Bank, inter-alia, should consider security of information that can be stored in mobile devices and encryption of transaction information and PIN/Password from mobile devices to bank's system while providing banking services using mobile devices (. Additional controls like daily transaction limit, per transaction limit etc. should also be defined if bank is providing fund transfer facility. Mobile banking should be allowed for accounts in Nepalese currency only.

Cyber

29. As the risk of cyber attack and its trend is increasing, banks should, inter-alia, implement more than one factor for authenticating critical activities like fund transfers through internet banking facility. The authentication methodology should commensurate with the risk of internet banking.

30. Bank should implement adequate security measure to secure their web applications from traditional and emerging cyber threats and attacks and critical application should employ latest SSL encryption.

Situation awareness: outsourced operations

1. Board and senior management are responsible for due diligence, oversight and management of risks associated with outsourcing and accountability of outsourcing decision rests with board and bank management.

2. Bank should evaluate the risk before entering into outsourcing agreement of technical operations that can significantly impact the business operation and reputation of the bank and it should be evaluated periodically

3. All outsourced operations should be subject to bank's information security and privacy policy and bank should ensure that outsource service provider implement adequate internal controls, logical access control and physical security controls to ensure the same.

4. Bank should ensure that outsourcing of IT operation do not interfere or obstruct regulatory activities. Moreover; the authority of regulatory bodies under the BAFIA and NRB Act to carry out any inspection, supervision or examination of the service provider's role,

virtualization

10. Emerging technologies such as virtualization, data center hosting, and disaster recovery site hosting, applications as a service and cloud computing have no clear legal jurisdiction for data and cross border regulations. Banks should clarify the jurisdiction for their data and applicable regulations at the beginning of an outsourcing or offshoring arrangement. This information should be reviewed periodically and in case of significant changes performed by the service provider.

Secure operations

2. Adequate segregation of duty should be enforced in all IT operations. There should be documented standards/procedures for administering an application system, which are approved by the application owner and kept up-to-date. Access to the application should be based on the principle of least privilege and "need to know" commensurate with the job responsibilities.

3. Critical system functions and procedure such as systems initialization, network security configuration, access control system installation, changing operating system parameters, implementing firewalls and intrusion prevention systems, modifying contingency plans, invoking emergency procedures, obtaining access to backup recovery resources, administering critical application, creating master password and cryptographic keys should be carried out in joint custody.

4. Banks need to implement a 'change management' process for handling changes in technology and processes to ensure that the changes are recorded, assessed, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled manner and environment.

Security testing

Many software fails due to inadequate system testing and bad system design. Application that handles financial information of customers' data should, inter-alia, satisfy security requirements. Deficiencies in system design should be recognized at early stage of software development and during software testing. Among other things, following points should be taken into account while developing software.

Key areas

- Fraud management
- BCP
- Awareness
- Shared Ownership