Nepal Rastra Bank
Information Technology Guidelines

Release: August 2012

Bank Supervision Department
Nepal Rastra Bank

CONTENTS

ABBREVIATION

ATM	Automatic Teller Machine
BAFIA	Bank and Financial Institution Act
BCP	Business Continuity Policy
BOD	Beginning Of Day
CCTV	Close Circuit Television
CIA	Confidentiality, Integrity, Availability
COBIT	Control Objectives for Information and Related Technology
DC	Data Centre
DR	Disaster Recovery
DRP	Disaster Recovery Policy
EOD	End Of Day
IS	Information System
ISO	Information Security Officer
IT	Information Technology
NRB	Nepal Rastra Bank
POS	Point of Sale
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SMS	Short Message Service
UPS	Uninterrupted Power Supply

1. EXECUTIVE SUMMARY

The use of information technology by financial sector has changed the way they do their business. It has become a part of business rather than supporting factor of business and has created challenges of managing and governing it. Issues of tackling with changes in technology, migrating system from one to another, maintain adequate internal control system, limiting access to system and data from unauthorized access, securing electronic transactions , meeting legal requirements, managing outsourcing services, and managing other IT related risks have been emerged in banking sector.

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 banks with the objectives of strengthening banks for tackling with emerging cyber frauds, managing information technology prudently and mitigating risk aroused from implementation of information technology.

2. APPLICABILITY OF THE GUIDELINES

The objectives of this guideline are to promote sound and robust technology risk management and to strengthen system security, reliability, availability and business continuity in commercial banks of Nepal. Banks should compulsorily comply with this guidelines within two years from the date of issuance. The Action Plan (along with time frame for each action) for the implementation of the guidelines should be developed and provided to Bank Supervision Department, Nepal Ratra Bank within six month from the issuance. The extent of compliance of this guideline will be examined during the periodic onsite/offsite supervision from NRB.

GUIDELINES

1. IT GOVERNANCE

IT has been adopted by most of the commercial banks to some degree from branch automation to providing alternate delivery channels[1]. This pervasive nature of IT has increased the challenge on governing it. Since IT is very critical in supporting and enabling business goals and is strategic for business growth, due diligence on its governance is essential. IT governance is a continuous process where IT strategy drives the process using necessary resources. In this context; NRB expects commercial banks to follow following guidelines

1. Bank[1] should have a board approved IT related strategy and policy and IT policy should be reviewed at least annually. IT strategy can be long term and short term and long term strategy should be mapped to short term strategy periodically. There should be detail operational procedures and guidelines to manage all IT operations.

2. Organizational structure for IT should be commensurate with the size, scale and nature of business activities carried out by the bank and may differ from bank to bank. Broadly the organization structure consists of Development, Technology, IT Operation and Information Assurance.

3. Bank should assess the requirement of expertise to successfully complete required IT functions. A periodic IT training requirement for IT personnel according to the IT functions of the bank should be assessed.

4. Bank should have performance monitoring and measuring system of IT functions and it should be reported to appropriate level of management.

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

[1] Bank in this document refers Bank and Financial Institutions licensed by NRB.

be responsible for coordinating and communicating security related issues within the organization or with relevant external organization.

9. Bank needs to carryout detail risk analysis before adopting new technology/system since it can potentially introduce new risk exposure. The new technology/system should be assessed as a part of product approval process which incorporates security related issues and regulatory requirements. The new technology/system should have fulfilled among other things, security related aspect, regulatory and legal aspects, employed industry standard controls or compensating controls and should be tested to ensure security issues of the technology.

10. Bank should have process in place to identify and adequately address the legal risk arising from cyber law and electronic transaction related laws and acts of Nepal.

2. INFORMATION SECURITY

Robust information is crucial to achieve business goals and for managing risk prudently in banks. Accuracy, integrity, consistency, completeness, validity, timeliness, accessibility, usability and auditability are requirement of information processed and stored electronically. To achieve these qualities of data, banks should develop and maintain comprehensive information security program.

1. There should be a board approved Information Security Policy addressing all electronic delivery channels and payment system and it should be well communicated to employees, contractors/suppliers, consultant and officials.

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.

7. Bank should harden their system i.e. should be configured with highest level of security setting in operating system, firewall and system software. The default password should be changed immediately after installation. The updates, patches and enhancements for security should be installed as recommended by the vendors.

8. Bank should develop and implement comprehensive computer virus protection mechanism.

9. Bank should deploy strong cryptography and end-to-end encryption to protect customer PINs, user passwords and other sensitive data in networks and in storage.

10. Bank should install firewalls between internal and external networks as well as between geographically separate sites. And firewall should be configured according to network security policy of the bank.

11. It is the responsibility of the bank to operate and maintain adequate and effective authentication and related security measures and verify the customer with proper authorization and validation procedure before access to customer account is granted and before transaction is executed.

12. Bank should make sure the detail audit trail with transaction id, date, time, originator id, authorizer id, action taken etc. is available for each application handling sensitive information of the bank. Audit trail should be detail enough to complywith regulatory, legal and bank's requirement and should be secured to ensure integrity of information. Audit trail should be available even after migration of the system, if applicable.

13. Bank should ensure that all the applications used by the bank maintains integrity of data and free of malware and any hidden channels of data processing. This will be applicable even in purchased system.

14. Bank should adopt procedures to ensure the integrity and consistency of all critical data stored in electronic form, such as databases, data warehouses and data archives.

15. Bank should never practice updating database by accessing back-end directly. But if it has to be done due to genuine business need, it should be done under close supervision and after due authorization.

16. In the event of data pertaining to Nepalese operations being stored and/or processed abroad, there needs to be suitable controls like segregation of data and strict access controls based on principle of ‘need to know’ and 'least privilege' and robust change controls process. The bank should be in a position to adequately prove the same to the regulator/supervisor. Regulator/supervisor’s access to such data/records and other relevant information should not be impeded in any manner and NRB would have the right to cause an inspection to be made on the data centre and the system.

17. Bank should have a migration policy with details of migration process to ensure principle of information security[iv]. After each stage of migration and after completion of migration, explicit sign offs from application owner should be taken to ensure data integrity, completeness and consistency of data.

18. Information and inventory assets in bank should be recorded and classified according to criticality of information[v]. Security requirement and corresponding access control mechanism should be developed for each class and it should commensurate with level of criticality of information.

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.

21. Bank should evaluate security risk and apply appropriate additional controls if using wireless network.

22. The information security policy, guidelines and education program should be updated according to latest threats and changes in modus operandi of electronic attacks.

23. CCTV at each ATM location should be installed with adequate lighting inside ATM centre so as to capture clear picture of person doing ATM operation. However; CCTV should not capture the PIN entered by customer. Secure Transmission of message using appropriate encryption from ATM, controls relating to ATM key generation, loading, destruction, firewall, antivirus, secure PIN generation, adequate segregation of duty while creating PIN and card should be employed.

24. Bank should ensure that electronic card and its PIN is not under control of single person from the point of production till it is delivered to customer. PIN and card should not be together at any point of time before it reaches to customer hand.

25. For debit / credit card transactions at the POS terminals, it is recommended to replace existing signature based system with PIN based authorization system and the non-PIN based POS terminals be withdrawn within certain period.

26. Banks are recommended to replace current magnetic stripe card with chip based card.

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.

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.

3. Information Security Education

With the introduction of electronic delivery channels, customers don't require to visit the bank branches physically to conduct banking. This has intensified the challenges of authenticating customers. Moreover; fraudsters are designing and using more advanced techniques to impersonate users and make illegal access to customers account. To defend illegal users from accessing banking system, it has become essential to well educate customers to conduct banking operation securely. To create effective information security practice, it is also important to educate other stakeholders including its employees.

1. Bank should develop information security awareness program and periodically conduct to its employees, vendors, customers and other related stakeholders. The awareness program should be customized according to the target group. It is recommended to develop mechanisms to track the effectiveness of training program.

2. Bank should ensure that customers are adequately educated so that they take appropriate security measures to protect their devices and computer systems and ensure that their hardware or system integrity is not compromised when engaging in electronic banking. Bank should have appropriate procedures in place to promptly response the customers query regarding securely accessing electronic banking.

3. Banks are responsible for safety and soundness of their system. They should use appropriate customer authentication system to authenticate customers before access to system is allowed and customers should also be adequately educated and aware of securing their credentials.

4. Information Disclosure and Grievance Handling

Bank should clearly provide information about the services, cost, security features, risk and benefits of electronic banking environment. Precise information about responsibilities, obligations and rights of customers and bank regarding electronic transaction should be delivered to customers.

1. Bank should publish clear information about the dispute or problem resolution process in case of any security breaches and fraudulent access to customer's account. The condition on which loss will be attributable to the bank or their customers should be clearly explained.

2. Bank should publish customer privacy and security policy; cost of transaction etc. in their website or at the time of subscription of the corresponding electronic delivery channels and it should be relevant and helpful to make informed decision for subscribing electronic delivery channel.

3. Bank should clearly inform user on the amount transaction cost at each of their ATM location or electronically before committing the transactions from ATM. and other electronic delivery channels

4. Bank should develop dispute handling mechanism with expected timing of bank response, to handle disputed payments, transaction and other issues in electronic banking delivery channels.

5. Bank shall be responsible for grievance handling in case of customer files complaints on disputed transaction and procedure for handling grievance should be formulated by the bank.

6. Banks should provide clear information to their customers about the risks and benefits of using e-banking delivery services to enable customers to decide on choosing such services. Bank should educate customers on which protections are provided and not provided in each of their delivery channels.

5. OUTSOURCING MANAGEMENT

It has become quite common for Nepalese banks to outsource some or all of IT functions. Inter-branch communication, software, hardware and other technical and administrative functions are commonly outsourced by Nepalese banks. Emerging technologies such as virtualization, Data Centre and Disaster Recovery Site Outsourcing are also becoming popular. Whatever the reasons of outsourcing, bank has responsibility to ensure that their service providers are capable of delivering the level of performance, service reliability, capability and security needs that are at least as stringent as it would expect for its own 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,

responsibilities, obligations, functions, systems and facilities must be recognized in the agreements.

5. Banks should establish a process for monitoring and control of outsourcing activities and it should commensurate with the nature, scope, complexity and inherent risk of the outsourced activity. The accountability of performance of outsourced activities should be specified in the agreed service level and it should be evaluated periodically. A periodic review of operational and financial condition of the outsource service provider should be carried out.

6. It is the responsibility of the bank to ensure availability, integrity and confidentiality requirements even if outsourced service provider is outsourcing some or all of its functions.

7. Bank should ensure that availability and quality of the banking services are not be adversely affected by outsourcing arrangements of the bank. The contingency planning of the bank should address the availability of alternate services providers or possibility of canceling outsourcing activities and bringing the outsourced activities back in house in urgent situation.

8. While outsourcing IT operations outside the country, country risk factors such as economic, social and political reasons should also be considered while accessing the risk of outsourcing activities. Bank should proactively evaluate such risks and develop effective and appropriate mitigating controls and if required exit strategy. The same should also be considered if the outsource service providers are operating across multiple countries or outsourced some or all of its functions abroad.

9. To ensure continuity of critical applications, bank should have suitable strategy in place. Bank can either receive source code and its updates from the vendor or can arrange a software escrow agreement to ensure source code and its updates availability in case the vendor goes out of business.

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.

6. IT OPERATIONS

IT infrastructure have been developed and grown in banks over few years and has been used to support processing and storage of information in banks. IT should be operated to ensure timely, reliable, secure information. To ensure effective and efficient delivery of information, following guidelines should be followed.

1. Board and higher management should oversee functioning of IT operation and should ensure safe IT operation environment.

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.

5. Bank should have a documented migration policy with migration methodology to ensure completeness, integrity, confidentiality and consistency of data. Bank should ensure that audit trail of the older system is available even after migration to new system. Audit trail of pre migration, migration and post migration should be available for review.

6. Vendors, suppliers or consultant who are authorized to access critical system of the bank should be subject to close supervision, monitoring and access control similar to those applying to internal staffs.

7. High degree of availability of the service is critical for online environment. Bank should be able to ensure that they have adequate resources in terms of hardware, software and other operating capability to deliver consistently reliable service. Bank should identify and maintain standby software, hardware and network components critical for availability.

8. Bank should conduct periodic risk assessment of their IT environment including human resource, technology and processes. The probable events or activities that can adversely affect the bank's operation or reputation should be identified during risk assessment and suitable mitigating strategy should be in place.

7. INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND IMPLEMENTATION

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.

1. User functional requirements, security requirements, performance requirements and technical specification should be documented and approved by appropriate level of management before software is developed.

2. Information security requirement should be incorporated at each stage of software development lifecyclevi. Security requirements relating to access control, authentication, transaction authorization, system activity logging, audit trail, data integrity, security event tracking etc. should be incorporated along with business requirement.

3. All system should have audit trail detailed enough to use it as forensic evidence and audit trail should meet, inter-alia, regulatory and legal requirements.

4. Banks are encouraged to conduct source code review of the application with the objective of finding loopholes and defects residing in the software due to poor programming practice, coding errors, malicious attempts etc. All the vulnerabilities, loopholes and defects found should be fixed before system is implemented.

8. Business Continuity And Disaster Recovery Planning

The role of banking sector in economic growth and stability is vital and requires continuous service and reliable service. The introduction of electronic delivery channels and 24/7 services availability has increased the demand of Business Continuity Planning (BCP) framework comprising of all critical aspects of people, process and technology. Business Continuity should be formed to minimize financial, operational, legal, reputational and other risks and it includes policies, standards and procedures to ensure continuity, resumption and recovery of business processes and minimizes the impact of disaster. A business continuity plan generally incorporates business Impact analysis, recovery strategies, business continuity plan as well as testing, training, awareness, communication and crisis management program.

Disaster Recovery Planning (DRP) deals with technical aspects of BCP and is a part of it. Most of the applications in banking are mission critical in nature and requires high availability. While designing the banks IT system and Datacenter (DC), fault tolerance of such mission critical system should be taken into account.

1. Bank should have board approved BCP Policy. There should be detail procedures and guidelines for prioritizing critical business functions, incident handling and how the institutions will manage and control identified risk. The BCP should also include allocation of sufficient resources, allocating knowledgeable person etc and should be reviewed periodically.

2. A senior officer of the bank should be appointed as Head of Business Continuity Planning function and he/she will be responsible for developing BCP, it regular updates, prioritization of critical business activities, recovery, testing, training and other aspects of BCP.

3. A BCP should consider all probable natural and man-made disasters, security threats, regulatory requirements, dependencies on outsourcing activities and issues of operating in multiple countries. BCP should also consider people aspect along with technical aspects.

4. A BCP team should be formed and it should comprise of senior offers from various departments as required and it should be formed in head office as well as in branch offices.

5. BCP should be periodically, at least annually, tested to ensure its effectiveness. The testing should include all aspects and constituents of the bank i.e. people, processes and resources including technology. BCP testing should be both planned and unplanned and should be audited by internal audit of the bank. The testing and its outcome should be documented and amendments in BCP be made as suggested by the outcome of the test.

6. BCP should specify RPO and RTO [vii] of the business processes and suitable data recovery strategies should be chosen in DRP to meet required RPO and RTO. Bank can choose Hot Site, Warm Site or Cold Siteviii for backup site but it should meet the RPO and RTO requirement as specified in the BCP.

7. Bank can use their own standby site and system or outsource it from some disaster recovery providers. Depending on RPO and RTO requirements, bank may opt for high availability system to keep both system and data replicated on remote site or live replication of data to offsite location or back up made to offsite location or backups made to electronic media and sent offsite periodically or combination of above strategies.

8. Whatever the arrangements has done for standby site, bank should also adopt disaster mitigating strategies such as locally mirroring data and system, arranging UPS and generator for long term power failure, using surge protector to minimize the effect of power fluctuations and providing adequate physical and environmental controls in the DC.

9. The datacenter, disaster recovery solution, enterprise network and security and branch or delivery channels should be designed and configured for high availability and no single point of failure.

10. The location of building containing datacenter and critical equipment rooms must be chosen so as to minimize the risk of natural and man-made disaster, flood, fire, explosion, riots, environmental hazards etc. Physical access to datacenter and critical equipment rooms must be restricted to authorized individuals only.

11. Bank should check transaction and data integrity between DC and DR site periodically. It is recommended to make this check as a part of End of Day (EOD) or Beginning of Day (BOD) process.

12. Bank should develop appropriate incidence response plans, including communication strategies and outsourced services, to ensure business continuity, control reputational risk and limit liability of service disruption. The incidence response plan should, inter-alia, cover mechanism to identify incidence as soon as it occurs, recovery of e-banking system and services, communication strategy to address external party and media, procedure to alert related regulatory body etc.

9. IS AUDIT

Since the increasing complexity of IT environment in banks has created significant risk, comprehensive risk management comprising of various standard internal control framework, bank's own requirement and NRB requirement. To ensure the effectiveness of implemented controls framework and adequacy of the adopted security plan and procedures, banks should conduct IS audit annually.

1. Board or the audit committee should provide sufficient resources to conduct audit to ensure the audit team is capable of evaluating IT controls in sufficient IT coverage.

2. If the bank does not have enough staff to conduct IS Audit or bank lacks expertise and experience in its staffs, IS audit can be outsourced to external professional provider. However; the responsibility of audit planning, risk assessment and follow up rests on the bank. The audit committee should ensure that the outsourced service provider has expertise and experience in IS Audit.

10. FRAUD MANAGEMENT

Nepalese banks are using electronic delivery channels to provide banking services. Increased use of Internet banking, mobile banking, payment card (debit and credit card), ATM is also creating risk of electronic fraud in banking system. In this context, bank should among other things follow following guidelines.

1. Banks should identify and document all electronic attacks and suspected electronic attacks in their system and report to Nepal Rastra Bank monthly.

2. Customers should be made aware of frauds along with fraud identification, avoidance and protection measures.

GLOSSARY

Access Control:	Enable authorized use of a resource while preventing unauthorized use or use in an unauthorized manner.
Assurance:	Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation.
Encryption	Encryption is the process of converting data into a form, called cipher text, which is not easily understood by unauthorized people or application. The cipher text is converted back into original form by a process called decryption.
Information Security Policy:	The statement of required protection of the information objects.
Subject:	An active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state.
Object:	A passive entity that contains or receives information. Note that access to an object potentially implies access to the information it contains.
Risk Management:	The ongoing process of assessing the risk to mission/business as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate, cost effective controls to achieve and maintain an acceptable level or risk.
Security:	Security is a system property. Security is much more than a set of functions and mechanisms. IT security is a system characteristic as well as a set of mechanisms that span the system both logically and physically.
Threat:	Any circumstance or event with the potential to harm an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. Threats arise from human actions and natural events.
Vulnerability:	A weakness in system security requirements, design, implementation, or operation, that could be accidentally triggered or intentionally exploited and result in a violation of the system's security policy.

ENDNOTES

[i] Electronic delivery channels : Electronic medium from which customers can do banking operation such as mobile banking, Automated Teller Machines, Internet Banking etc.

ii COBIT (Control Objectives for Information and Related Technology) is an IT governance framework and supporting toolset and provides guidance for organization to govern IT. It is an international open standard designed by IT Governance institute and it defines control and security of sensitive information. For further information visit: www.itgi.org.

[iii] CIA: Confidentiality, Integrity and Availability

Confidentiality:

Confidentiality is the assurance that the information remains private to the bank and is not viewed or used by unauthorized users. Since data storage and transmission happens in electronic form, transmission of data via public network, practice of outsourcing some functions have increased the challenge in maintaining confidentiality of information.

Integrity:

Data integrity is different from referential integrity of database management system. Integrity implies that data should not be modified without authorization by individual or application. Individual can be internal or external to bank. Data integrity is violated in different ways such as, a staff of the bank can intentionally or accidently can type wrong data, or computer application which are not written or tested in correct way can violates integrity of data during bulk operation of data and so on.

Availability:

Availability implies that information should be available to respective customers whenever required. Information for critical system such as banking system must have high degree of availability. The disruption of service or information from hardware failure, software failure, power outage, DOS (Denial of Service), DDOS (Distributed Denial of Service) and other disruptive events should be minimized to minimum time.

[iv] Information Security Principle:

CIA (Confidentiality, Integrity and Availability) has been treated as basic principle of information security traditionally. But for critical organization such as government, banking etc, other principle are also considered as important principle.

Authenticity:

This ensures that data, transaction, communication and documents are genuine. This is important for information security since it ensures that parties involved in the process are genuine.

Non repudiation:

Non repudiation is the process that ensures that one party of transaction cannot deny that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. Electronic commerce uses technology such as digital signatures and encryption to establish authenticity and non-repudiation.

Identification:

To get access to the system, a subject needs to be identified first. Process of authentication, authorization and authentication cannot b e start without identifying the subject. Subject can be identified by different factors such as username, smart card, biometric information such as facial, finger print, eye retina etc.

Authorization:

After authentication of subject, access is authorized and granted. Authorization ensures that the claimed activity or access to the object is valid. Often, an access control matrix is used to compare the validity of claimed access.

Accountability and Auditability:

Accountability is established by linking a human to the activities of an online identity through the security services and mechanisms of auditing, authorization, authentication, and identification. Accountability implies that every action on some entity has to be traced uniquely and it supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after action recovery and legal action.

[v] Information Classification

The need of protecting business and customer information asset is obvious for any organization. This classifies the information according to the value of information and level of protection required for it and is an important step for prudent risk management. Even though number of information classification level can be increased to any number, a manageable number classification is essential. ISO17799 standard has classified information into following five levels.

Top Secret: Highly confidential internal information and document. Security at this level is the highest possible.

Highly confidential: information which is considered critical to the organization's ongoing operations and could seriously impede or disrupt them if made shared internally or made public.

Proprietary: Procedures, project plans, operational work routines, designs and specifications that define the way in which the organization operates.

Internal Use: information not approved for general circulation outside the organization, where its disclosure would inconvenience the organization or management, but is unlikely to result in financial loss or serious damage to credibility/reputation.

Public: information in the public domain: press statements, annual reports, etc. which have been approved for public use or distribution.

[vi] Software Development Lifecycle

Software Development Lifecycle (SDLC) is conceptual model used in software development or alteration process that describes the stages involved in an information system development project, from an initial feasibility study through maintenance of the completed application. Various methodology have been developed in SDLC such spiral model, Rapid Application Development, Waterfall Model, Joint Application Development, fountain model etc.

[vii] RPO and RTO

Recovery Point Objective (RPO) – The acceptable latency of data that will be recovered i.e. amount of data, measured in time, that that can be lost from disaster.

Recovery Time Objective (RTO)–The acceptable amount of time to restore the function i.e. amount of time it takes to recover from a disaster event.

[viii] Hot, Warm and Cold Back up Site

1. Cold Sites: This type of backup site does not include hardware and software. Even backup copy of data is not kept in this type of backup site. This makes a cold site is the most inexpensive type of backup site for an organization to operate, but requires additional time following the disaster to have the operation running at a capacity close to that prior to the disaster.

2. Hot Sites: This site is nearly a duplicate of the original site of the organization and consists of full computer systems as well as near-complete backups of user data. Real-time synchronization between the two sites may be used to mirror the data environment of the original site, using wide area network links and specialized software. Organization can relocate its data centre after a disruption to the original site with minimal losses to normal operations within a matter of hours or less than it. This type of backup site is most expensive to implement but are widely used by financial institutions, government agencies and ecommerce providers.

3. Warm Sites: This type of site is somewhat between hot site and cold site and it will have hardware and connectivity already established, (may be on a smaller scale than the original production site). The backup of data will be kept in warm site but this can be few days old.