Information Security Policy Manual

VERSION 1.0
LAST UPDATE: MAY 2024
CONFIDENTIALITY LEVEL: CONFIDENTIAL

Document Control

Ver.	Date	Type	Description	Prepared By	Reviewed By	Approved By
1.0	1-May-2024	Final	Initial Publication Version	Amol Deshpande	Milind Panchanadikar	

Table of Contents

1. Introduction

The Information Security Procedures define the detailed requirements and processes for the Information Security Policy. These procedures aim at facilitating the implementation of the policies.
The procedures are classified into the following sections:

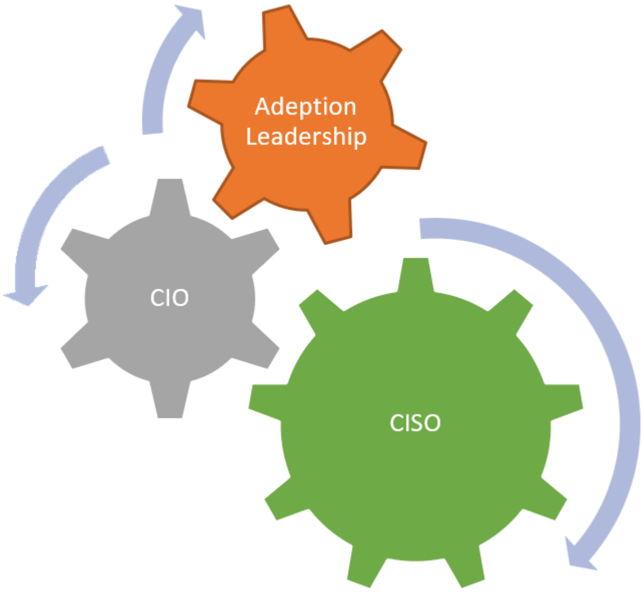
- Asset Management
- Human Resource Security
- Physical and Environmental Security
- Communications and Operations Management
- System Planning and Acceptance
- Backup and Recovery
- Vendor Management
- Access Control
- Network Security
- Information Systems Acquisition, Development and Maintenance
- Cryptographic Systems
- Incident Management
- Business Continuity Management
- Compliance
- Data Confidentiality Policy
- Extranet Policy
- Internet Security
- Laptop Security
- Network Security
- Web Security
- Wireless Security
- Punitive Actions for violation of Information Security Policies
- Visitor and Contractor premises access Policy
- Remote Access Policy
- Blackberry Policy
- Usage of personal devices
- Social media Policy
- Privacy Policy

The procedures are supported by sample forms and templates referred within the procedural activities. These forms and templates facilitate the implementation of the procedures.

The CISO is overall responsible and accountable for the maintenance and adherence to the Information Security Policies and Procedures

2. Security Organization Structure

The Chief Information Security Officer (CISO) will direct and oversee the establishment and monitoring of security controls needed to protect the Company's information assets in line with the policies specified in this document. The CISO will ensure that these policies are reviewed annually and updated as needed.



3. Asset Management

3.1. Asset Inventory Procedure

- Identify all information assets in the Organization. Information assets should include but are not limited to databases, system documentation, user manuals, continuity plans, archived information (if any), software assets, application software, system software, development tools, physical assets that support your information systems, computer equipment, processors, monitors, system log files, laptops etc. All information assets should be classified by information asset owners based on the defined Classification Guidelines (Refer: Information Classification Guidelines).
- The information asset inventory should be maintained in an Asset Register
- Physical assets should be labeled with an asset number that identifies the asset in the asset register.
- The respective Information Asset Owners shall be responsible for maintaining and updating the Information Asset Inventory of the assets they own.
- The Business Information Security Officer (BISO) must verify the information asset inventory once it is created.
- The Asset Inventory should be verified on an annual basis by the BISO.

Asset Inventory Process Diagram

3.2. Asset Classification

The Information Asset classification scheme and associated guidelines will consider:

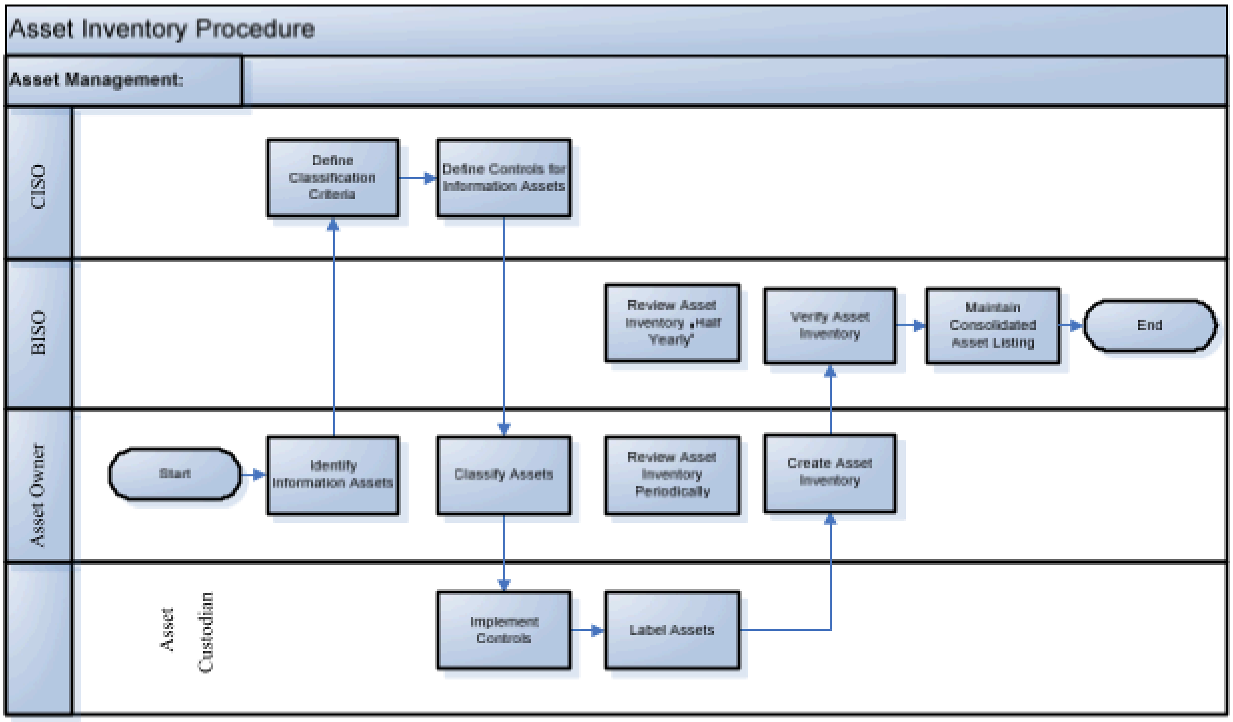
- The type of Asset
- The criticality of the Asset
- The Information Asset value
- The impact of a security breach or loss of the asset
- The basis on which access to the Information Asset will be provided and the extent of access (read, modify, delete, etc.) that will be provided to different users.

3.3. Classification Applicability

This data classification scheme is applicable to all information, whether stored or transmitted, which is in the possession or under the control of ADEPTION. For example, confidential information entrusted to ADEPTION by its customers, suppliers, business partners, and others should be protected with this Data

Classification scheme. Similarly, the employees of the company are expected to protect third party information with the same care that they protect information belonging to the company. This Data Classification scheme is also applicable to Third Parties that are in possession of ADEPTION data. For the purpose of this Data Classification scheme, no distinctions between the words data, information, and knowledge, are made.

3.4. Consistent Protection


Asset Inventory Procedure
Asset Management:
CISO
BISO
Asset Owner
Asset Custodian
Define Classification Criteria
Define Controls for Information Assets
Review Asset Inventory ,Half Yearly'
Verify Asset Inventory
Maintain Consolidated Asset Listing
End
Start
Identify Information Assets
Classify Assets
Review Asset Inventory Periodically
Create Asset Inventory
Implement Controls
Label Assets

The information of ADEPTION should be consistently protected throughout its life cycle, from its origination to its destruction. Information should be protected in a manner commensurate with its sensitivity. no matter where it resides, what form it takes, what technology was used to handle it, and what purpose it serves. Although this Data Classification scheme provides overall guidance, to achieve consistent information protection, employees of ADEPTION will have to apply and extend these concepts to fit the needs of day-to-day operations.

3.5. Information Classification & Declassification Guidelines

The following guidelines may be followed by the Information Asset Owners during classification and Declassification of data:

Classification

- Each Information Asset Owner should classify the data into the categories given according to the Asset Classification and Control Standards.
- Each Information Asset Owner should review the information, which needs to be archived and purged on a semi-annual basis. The Information Asset

Owner should ensure that the relevant data is archived or deleted appropriately.

Declassification or Downgrading

The following guidelines may be followed by the Information Asset Owners for the declassification or downgrading of the Assets:

- The designated Information Asset Owner may, at any time, declassify or downgrade information. To achieve this, the Information Asset Owner should change the classification label appearing on the original document and notify all known recipients and users.
- The date from which the confidential information will be declassified or downgraded should be indicated on the sensitive information of the company.
- The BISO may, at any time prior to scheduled declassification or downgrading, extend the period that information is to remain at a certain classification level.
- To determine whether sensitive information may be declassified or downgraded, the BISO shall review the sensitivity classifications assigned to information for which they are responsible at least once in 2 years.

3.6. Asset Management Roles and Responsibilities

Information Asset Owner

The Information Asset Owner or the Departmental Head has the responsibility of classifying the asset based on ADEPTION's Asset classification scheme and related guidelines i.e. on the basis of the Asset's Confidentiality, Integrity and Availability. The classification of the assets should be documented. This document should be reviewed and confirmed by the BISO. There should be strict version control on all documents and each change should be saved as a new version.

The Information Asset Owner should identify and approve of the controls to be implemented to provide appropriate protection to the asset. The Owner of the Information Asset is accountable for the security of the Information Asset.

Information Asset Custodian

The custodian of the Information Asset should be responsible for the protection of the Asset and for implementing the controls (as identified and approved by the Owner of the information asset) and ensuring that protection mechanisms are in place for the classified Assets.

Information Asset User

As information is important and pervasive throughout ADEPTION, all users have an important role to play as well as a responsibility to protect the information entrusted to them. All users who may come into contact with sensitive information (non-public) are expected to familiarize themselves with the asset management policy and the standards and guidelines supporting it, and to consistently use it.

3.7. Asset Classification Standards

Confidentiality Criteria

Confidentiality criteria define the level of confidentiality to be accorded to the information assets and consequently the level of accessibility to the information it contains or represents. The Risk ratings can be assigned on a scale of 1 to 5. 1 being the lowest and 5 being the highest.

Risk Rating	*Accessibility*	*Impact*
Very Low (1)	*Public*	*Public Information Sharing of such information does not have any impact on the confidentiality of the Information Asset and thus has a Very low Confidentiality rating. This form of information comes from public sources or is provided by ADEPTION to the general public.* *Examples include periodicals, public bulletins, published company financial statements, published press releases, etc.*
Medium (2)	*Internal*	*Internal Information (All departments and personnel)* *Such information is the property of ADEPTION. ADEPTION has the sole right over this information (exception: subjects of the information in most cases will also have rights to the information, such as a plan member having access rights to their contract). This form of information must be used within ADEPTION and not shared externally or with third parties.* *Examples include staff memos, company newsletters, staff awareness program documentation or bulletins, Service Contracts, Backup Tapes and CDs, etc.*

High (3)	*Restricted*	*Restricted Information* *Restricted information is a sensitive form of information. This information is distributed on a “Need to Know” basis only. Any non-public information, not confidential, that needs to be communicated to non-ADEPTION entities will fall in this category.* *Examples include employee personal information, business plans, unpublished financial statements, Minimum Baseline Security Configurations, Firewall and Router Configurations, client details and private information etc.*
Very High (4)	*Confidential*	*Confidential Information* *Confidential information is the most sensitive form of information. It is so sensitive that disclosure or usage would have a definite impact on ADEPTION’s business.* *Extremely restrictive controls need to be applied (e.g., very limited audience and those who are authorized to have such form of information).* *Examples include strategic plans, investment decisions etc.*

3.8. Information Classification Matrices

Security Control Matrix

Security	*Information Classification*			
Service	*Public*	*Internal*	*Restricted*	*Confidential*
Identification and Authentication	*None*	*User IDs and Passwords*	*Strong Authentication (encrypted username and password or token or certificate)*	*Strong Authentication*
Authorization and Access Control	*Access Control for Modification*	*Authorization by business department affiliations or function, access control at information category or directory level*	*Fine-grained access control - by user and role, by document or special purpose directories*	*Access control and authorization at the field level*
Auditing	*System-level for modification, events, alarms*	*System-level for user access, access denials, alarms*	*System-level for user, access, file changes, access denials, alarms*	*All events, alarms*
Physical Control of Media (paper, removable disks, writable CD-ROM, etc.)	*None*	*Labels and Marking, document destruction, secure storage*	*Labels and Marking, document destruction, secure storage*	*Labels and marking, document destruction, access lists, secure storage, audit program*
Security Operations	*System configuration-level audit, investigation of security events*	*System configuration-level audit, compliance audit, investigation of security events*	*Frequent system configuration-level audit, compliance audit, investigation of security events*	*Frequent system configuration-level audit, compliance audit, investigation of security events*

Transmission Control Matrix

Information Medium	Public	Internal	Restricted	Confidential
Local area network or Wide area network	*Use access controls to limit scope across the network*	*Use access controls to limit scope across the network*	*Encryption*	*Encryption*
Fax	*No special requirements*	*Attend Fax*	*Encryption* *Attend Fax* *Do not use programmed numbers.* *Verify destination number.* *Fax to and from a physically secure location*	*Encryption* *Use messenger.* *Minimize faxing*
Printer	*No special requirements*	*Print to a physically secure printer*	*Print to a physically secure printer* *Verify destination*	*Print to an attended and physically secure printer* *Verify destination printer.*
Video or voice conference call	*No special requirements*	*Owner approves roster of attendees*	*Encryption* *Owner approves roster of attendees*	*Encryption* *Owner approves roster of attendees.* *Ensure that meeting cannot be overheard.* *Ensure confidential material not in view of camera*

Information Medium	Public	Internal	Restricted	Confidential
Modem or ISDN	Password	Password Owner defines access requirements	Strong authentication	Encryption Strong authentication
Database	Use access control to limit authorization	Password protection is suggested	Data should be encrypted when not in use	Data should be encrypted when not in use
Email	No special requirements	Encryption	Encryption	Encryption Mark as “Highly restricted do not copy”
Paper	No special requirements	External mail Internal mail Mark “Open by Addressee only”	Certified external mail Internal mail Mark “Open by Addressee only”	Registered external mail. Double envelopes Use messenger service. Hand deliver internally Mark “Open by Addressee Only”

Labeling and Storage Control Matrix

Information Medium	Public	Internal	Restricted	Confidential
Servers	*No special requirements*	*Strong Password* *Locked in physically secure computer room*	*Encryption* *Strong authentication* *Restricted user access list* *Audit trail enabled.* *Locked in physically secure computer room*	*Encryption* Strong authentication Restricted user access list Audit trail enabled. Locked in physically secure computer room
Desktops	*No special requirements*	*Strong password*	*Encryption* *Strong authentication*	*Encryption* *Strong authentication* *Store on mainframe or servers or removable media*
Laptops	*No special requirements*	*Lock the laptop in the cabinet when not in use.*	*Encryption* *Strong authentication* *Minimize use.* *Lock the laptop in the cabinet when not in use.*	*Encryption* *Strong authentication* *Minimize use.* *Lock the laptop in the cabinet when not in use.*
Removable media (e.g. diskettes)	*No special requirements*	*Lock media in cabinet when not in use*	*Encryption* *Lock media in cabinet when not in use*	*Encryption* *Lock media in cabinet when not in use*
Hardcopy (Paper film or videos etc.)	*No special requirements*	*Front page labeled "Internal use only".* *Printed reports should be locked in cabinet when not in use*	*All pages labeled "Confidential".* *Confirmation of receipt required.* *Printed reports should be locked in cabinets when not in use*	*All pages labeled "Highly Restricted Copy #, Page #"* *Borrower should fill out a distribution log.* *No Copying Allowed* *Printed reports should be locked in cabinets when not in use*

Destruction Controls Matrix

Information Medium	Public	Internal	Restricted	Confidential
Hard drives, Removable media (diskettes, tapes etc.)	*No special requirements*	*Delete files.* *Lock media in cabinet when not in use*	*IT must perform an erase of files.* *Lock media in cabinet when not in use*	*IT must perform an erase of files, seven times formatting.* *Lock media in cabinet when not in use*
Electronic copies of files	*No special requirements*	*Delete old previous copies*	*Erase all copies on a timely basis*	*Erase all copies on a timely basis*
E-mail	*No special requirements*	*Periodically delete old Emails.*	*Erase Emails immediately*	*Delete Emails immediately*
Paper, film or videos, etc.	*No special requirements*	*Shred or delete all documents and files, or place in secure receptacle for future shredding*	*Shred or erase all documents and files, or place in secure receptacle for future shredding*	*Return to owner for destruction.* *Destroy printer cartridges after exhaustion*

4.Human Resources Security

4.1. Including Security in job responsibilities

- The HR function should prepare a document identifying the various roles in the organization.
- The responsibilities associated with each role must include Information Security responsibilities of the employees. The BISO should identify information security responsibilities for each role.
- The roles and responsibilities must be shared with all the employees.
- Head of HR must track the application of the roles and responsibilities for employees on a half-yearly basis.
- HR functions should provide a mechanism to address employees' concerns and issues related to his job responsibilities.
- All users should follow the Users Policies and Guidelines.

4.2. Personnel Screening Procedure

- All applicants are to fill out an application form at the time of attending the interview.
- The application forms should be screened by the interviewer. HR must ensure that:
  - Background checks should be performed on all applicants by an independent agency.
  - References should be contacted to assess the correctness of the information provided by the applicant.

4.3. Confidentiality agreements

- Confidentiality agreements should be separate from the appointment letter.
- Standard confidentiality agreements should be prepared based on the role and the department of the employee.
- Confidentiality agreements should be given to the employee, contractor or third-party user at the time of joining. the Confidentiality agreement should be signed by the employee, contractor or the third-party user and returned to the HR department at the time of joining.
- Employees must also sign-off on a Security Policy sign-off document affirming that they have read and understood the Information Security Policy. The Departmental Head of every new employee should ensure that he/she has signed the security policy sign-off document.

4.4. Terms and conditions of employment

ADEPTION's terms and conditions of employment, mentioned in the appointment letter should contain reference to:

- The legal and information security related responsibilities like copyright laws or data protection legislations of the employees, contractors, or third-party users
- The extent and duration of the responsibilities
- An indication of management action in case the terms of employment are violated.

The employees, contractors or third-party users should sign the terms and conditions of Employment at their time of joining.

The HR department should ensure that new employees have signed the terms and conditions of employment.

4.5. Training and Awareness procedures

The methods of training covered in this procedural document include classroom training, training manuals, web-based training, tuition reimbursement, certification exams, on-the-job training, and in-house training.

Determination of training requirements

The training needs of ADEPTION are to be identified based on the following:

- Strategic Information Security training based on an organization's business objectives.
- Internal Audits or Inspection External Audits or Inspection
- Role and responsibility-based training matrix. It should be maintained to list down the types of Information Security training that shall be applicable to each role within the organization.
- Information Security process improvements initiatives etc.

Operational continuity

For each key or vital Information Security function, an additional staff member needs to be trained to ensure continuity of operations of the organization. Also consider providing cross training to different personnel within the operations team in order to continue operations due to shortage of staff. These need to be identified and factored into the training requirements of the staff.

Awareness programs

- ADEPTION should hold awareness programs for its employees on a periodic basis. These programs should be designed to spread awareness among its employees regarding Information Security.

- Awareness programs should be conducted by an internal faculty on and on-going basis or in exceptional cases by an external party.

Measuring training effectiveness

For all Information Security training, a test or a quiz should be administered by the faculty to assess if the staff knowledge is adequate for performing project tasks, faculty's feedback form and training examinations should all be evaluated. The Training Coordinator should maintain the records of these evaluations.

Course evaluation

At the end of the training, all the participants must be made to fill up a Feedback Form, which is used to collect the participant's feedback on the course.

Training examination

After completion of each internal security training program, a Training Exam should be conducted immediately after, to assess the individuals understanding and readiness. On the basis of the examination results, Performance Analysis should be done to evaluate training effectiveness.

Post training evaluation

Post training evaluation should be carried out to collect the feedback from the Supervisors of the training participants after one month of training.

Analysis of training effectiveness

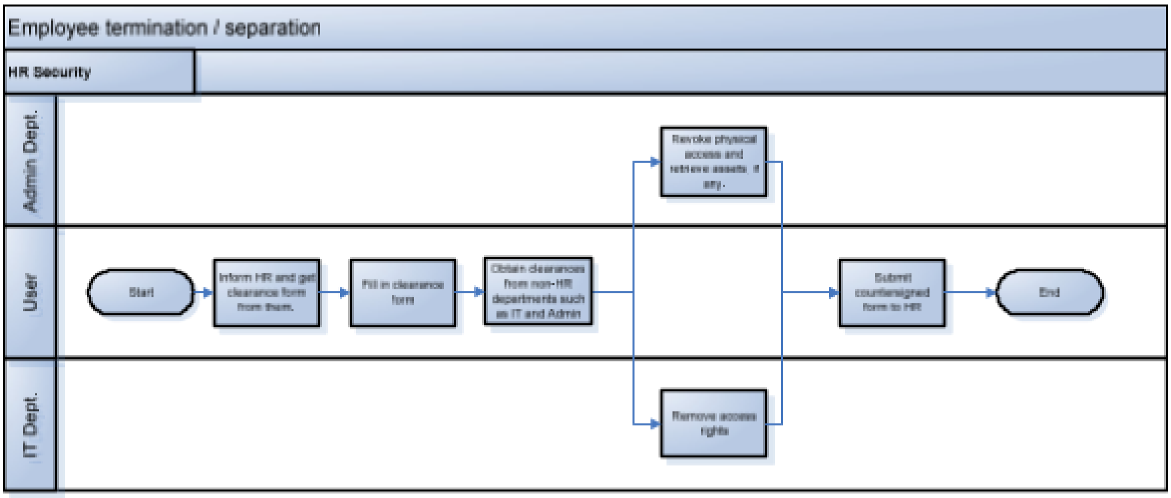
The analysis of the training effectiveness can be done with the help of the following guidelines:

- Evaluation of faculty and training by the trainees
- At the end of the training, all attendees to be given a training evaluation form. The rating should be in a scale of 1 to 5, 5 being the highest and most effective.
- The rating should be considered by the HR department when evaluating the faculty and when considering inviting the faculty again.
- The names of the employees need not be entered in the evaluation form, so that the employees can give the appropriate rating as per their understanding of the course.
- At the end of the training, the trainer should evaluate the training based on the response from the participants and the results of the test on the training to judge the understanding of the subject.

4.6. Termination / Separation procedures

- If any employee is found to be in breach of the security policies and procedures, then the following steps should be followed –
- In the first instance the employee shall be counseled by the respective Head of department.
- On second instance there would be a warning or formal notice issued by the Head of security
- On the third instance the employee should be reprimanded, and his/her service terminated.
    - In case of violations that may result in disclosure, unavailability or alteration of 'Confidential' information, the employee should be directly reprimanded, and his/her service terminated. (Refer: User Policies and Guidelines)
    - All relevant company personnel will be informed about the termination / separation of employees, contractors or third-party users, by the respective Head of Department.
    - Access rights (both physical and logical) of the terminated users shall be revoked by the IT department. (Refer: Access Control - Removal of User Accounts)
    - If the user had access to shared passwords, then that password will be changed upon termination / separation.
    - ADEPTION's assets available with the terminated / separated users must be returned and asset status must be updated by the admin department.
    - At all stages it is the responsibility of the respective Head of Department to inform HR and other departments of the termination / separation of an employee whereas it is the responsibility of the IT department to revoke all access from the systems. Any or all asset recovery from the employee is also the responsibility of the IT department provided employee's termination / separation was communicated to them.

Employee Termination / Separation (Process Chart)


Employee termination / separation
HR Security
Admin Dept.
User
IT Dept.
Start
Inform HR and get clearance form from them.
Fill in clearance form
Obtain clearances from non-HR departments such as IT and Admin
Revoke physical access and retrieve assets, if any.
Remove access rights
Submit countersigned form to HR
End

5. Physical & Environmental Security

5.1. Physical Security of Desktops and Laptops

- IT users assigned to every desktop and Laptop must be responsible for ensuring their physical security of the desktops.

5.2. Security of Equipment off-premises

- Regardless of ownership, the use of any information processing equipment outside the organization's premises must be authorized by management.
- Equipment and media taken off the premises should not be left unattended in public places.
- Manufacturers' instructions for protecting equipment should be always observed.
- Adequate insurance cover must be in place to protect equipment off-site.

5.3. Disposal of media

Media must be disposed of securely and safely when no longer required. Sensitive information may be leaked to outside persons through careless disposal of media. Formal procedures for the secure disposal of media must be established to minimize this risk.

The following guidelines must be considered:

- Media containing sensitive information and licensed software must be stored and disposed of securely and safely, e.g. by incineration or shredding, or formatted before use by another application within the organization.
- The following list identifies items that require secure disposal:
  - Paper documents.
  - Voice or other recordings
  - Output reports.
  - Magnetic tapes
  - Removable disks or cassettes
  - Optical storage media (all forms and including all manufacturer software distribution media)
  - Program listings.
- Test data.
- System documentation.

- Disposal of sensitive items must be logged in order to maintain an audit trail. and
- When accumulating media for disposal, consideration must be given to the aggregation effect, which may cause a large quantity of unclassified information to become more sensitive than a small quantity of classified information.

6. Communications and Operations Management

6.1. Operational Procedures and Responsibilities

Documented Operating procedures

- Documented procedures should be prepared for system activities associated with information processing and communication facilities, such as audit logging, backup, media and information handling and safety.
- Operating procedures should consider Segregation of duties issues.
- Operating procedures should be made available centrally to all employees.
- Operating procedures, and the documented procedures for system activities, should be treated as formal documents and changes must be authorized by the CTO or COO
- The CTO and COO are responsible to ensure that the operating procedures are maintained and up to date.

6.2. Operational Change Management Procedures

User Request and Approval

- Information resource changes (like installation of additional servers and network devices, installation of additional memory and storage, upgradation of OS etc.) are required in the IT infrastructure due to the need for additional capacity, upgradation of Applications, implementation of new applications, etc.
- In these cases, the request should be raised by a supervisor in the team through a mail and forward to Head of Department or corresponding Head of Operations for further approval. Business Process personnel

can also submit their requirement to the concerned technology asset owner through mails.

- The Head of Operations or Head of Department shall classify the change as Minor or Major based on the following guidelines:
  - Major Change: Critical upgrade to hardware in server class machines, upgrade in versions of OS, database and support applications.
  - Minor Change: Non-Critical upgrade to hardware in server class machines, hardware upgrade to desktops/laptops.
- A major or minor change may be further classified as an 'Emergency' change based on the criticality and urgency. The change may be carried out based on CTO's written or verbal approval. However, all steps required to carry out a change need to be completed within one week of the change.
- Head of Operations or Head of Department should then analyze both the impact of the change request on the existing infrastructure and the associated cost. If it is a Minor Change, he should approve the change. If it is a Major Change, he should forward it to CTO for approval.
- BISO should be involved in the analysis to identify any impact in security aspects due to the change for minor changes. For major changes the CISO should be involved
- CTO should approve the major changes if the cost involved in the change is within the budgetary limits. If it is above the budgetary approval of the CTO, the change needs to be ratified by the CTO from ADEPTION.

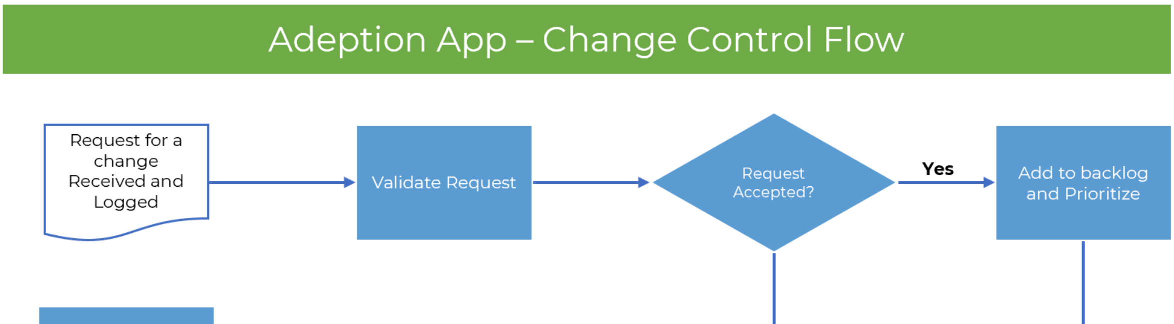
Operational Change Management Process Diagram

Testing and Implementation

- The System Administrators or Network Administrators should do the setup and testing of technology assets. System Administrators should prepare a test plan for testing the changes. Testing for Information Resource changes should be done in a test environment independent of ADEPTION Operations. Once the test is conducted satisfactorily. The changes should be implemented in the Operations network.
- During this phase, Product Owner (PO) should ensure that the user operating manual, system documentation and Minimum baseline security standards are updated before migrating to the production environment.

Rollback Plan and Documentation

- Prior to implementation of the changed programs on the production systems, backup of application code and database is taken.


Adeption App – Change Control Flow
Request for a change Received and Logged
Validate Request
Request Accepted?
Yes
Add to backlog and Prioritize

- Backup of the live servers should be taken before carrying out any major changes on the servers.
- Backup is restored in case any issues are encountered.

6.3. Segregation of Duties

- Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
- Care should be taken that no single person can access, modify, or use assets without authorization or detection.
- The IS and end-user departments should be organized to achieve an adequate segregation of duties.
- When duties are segregated, access to the computer, the production data library, the production programs, the programming documentation and the operating system and associated utilities must be limited.
- Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered.

6.4. Separation of Test and Operational Facilities

(Refer: Information Systems Acquisition, Development and Maintenance Procedures)

6.5. Third party service delivery management

(Refer: Vendor Management Procedures)

6.6. Network security management

(Refer: Network Security Procedures)

6.7. Media Handling & Security Procedures

The following procedures must be followed for the handling and security of Computer media includes tapes, disks, flash disks, removable hard drives, CDs, DVDs, and printed media.

Management of removable media

- If no longer required, the contents of any re-usable media that are to be removed from the organization should be made unrecoverable.
- Where necessary and practical, authorization should be required for media removed from the organization and a record of such removals should be kept maintaining an audit trail.
- Removable media drives must be enabled only if there is a business reason for doing so.

Disposal of media

(Refer: Physical Security Procedures)

Media and Information handling procedures

- Administration and IT team assigned for the protection of information and media are responsible for ensuring physical security of the media.
- All media must be stored in a safe, secure environment, in accordance with the manufacturers' specifications.
- All media must be handled with care and it must be ensured that it is not kept near magnetic material and not exposed to extreme heat or pollution.
- If no longer required, the previous content of any re-usable media that is to be removed from the company must be deleted by formatting.
- Head of Departments must authorize for media to be removed from the company and a record of all such removals must be kept.
  - In case of media in transit, following guidelines must be followed:
  - Reliable transport or couriers must be used. A list of authorized couriers must be agreed with the management and a procedure to check the identification of couriers must be implemented.
  - Packaging must be adequate to protect the contents from any physical damage likely to arise during transit and in accordance with manufacturers' specifications. and
  - Special controls must be adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification e.g. use of locked containers, tamper-evident packaging (which reveals any attempt to gain access), use of digital signatures and confidentiality encryption.

Security of System documentation

- System documentation of various information processing resources contains critical information about the systems and its configuration. This should be protected from unauthorized access, as disclosure of this information may compromise the security of the information stored in the information processing resources.
- The system documentation should be classified as per guidelines given in (Refer: Asset Classification Standards).
- Restricted personnel should have access to System Documentation both in hard copies and in soft copies. They should be given access to the System Administrators who administer the systems as per the distribution list.
- Hard copies of the documentation should be stored under lock and key. Key for the locker should be available only with the System Administrators who are designated for access and BISO.
- Softcopies of the system documentation should not be stored in the file server. If they are, shared access to them should be restricted as per the distribution list.
- System Administrators should not take Photocopies or printouts of the documentation without permission from BISO after providing justification for the same.

6.8. Information exchange

Information exchange policies and procedures

- The CISO must review existing relationships with external vendors to identify situations where information is exchanged with them.
- The CISO must also review information exchange between customers and ADEPTION.
- Procedures must be designed to protect exchanged information from interception, copying, modification, misrouting, and destruction.
- Cryptographic techniques in accordance with the Cryptography policy and procedures must be used to protect exchanged information. (Refer: Cryptographic Systems Policy and Procedures)
- Retention and disposal guidelines for all business correspondence, including messages, will be in accordance with relevant national and local legislation and regulations. (Refer: Compliance Policy and Procedures)
- Sensitive or critical information must not be left on copiers, printers and facsimile machines as they may be accessed by unauthorized personnel.
- Automatic forwarding of communication facilities e.g. automatic forwarding of electronic mail to external addresses must be restricted.
- ADEPTION Personnel should take appropriate precautions, not to reveal sensitive information to avoid being overheard or intercepted when making a phone call by people in their immediate vicinity, wiretapping or people at the recipient end.

Exchange agreements :

ADEPTION should establish exchange agreements for the exchange of information and software between ADEPTION and external third parties. It is the responsibility of the CISO to identify the need for such exchange agreements after reviewing relationships with third parties.

The exchange agreements could form a part of the contract with the third party. Exchange agreements should consider the following security conditions:

- Management responsibilities for controlling and notifying transmission, dispatch, and receipt of information.
- Procedures for notifying sender of transmission, dispatch, and receipt of information.
- Procedures to ensure traceability and non-repudiation of information and protection of cryptographic keys. (Refer: Cryptographic Systems Policy and Procedures)
- Minimum technical standards for packaging and transmission of information and date.
- Escrow agreements, if needed.
- Responsibilities and liabilities in the event of information security incidents, such as loss of data.
- Use of an agreed labeling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood, and that the information is appropriately protected.
- Ownership and responsibilities for data protection, copyright, software license compliance and similar considerations

Physical media in transit

The following guidelines and procedures should be considered to protect information media being transported between sites:

- Reliable transport or couriers should be used.
- A list of authorized couriers should be agreed with by the Head of Administration.
- Procedures to check the identification of couriers should be developed.
- Packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications (e.g. for software), for example protecting against any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture or electromagnetic fields.
- Controls should be adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification. examples include:
  - Use of locked containers.
  - Delivery by hand.

    - Tamper-evident packaging (which reveals any attempt to gain access).
- In exceptional cases, splitting of the consignment into more than one delivery and dispatch by different routes.

Electronic Messaging :

Information involved in electronic messaging such as e-mail and instant messaging should be appropriately protected. Security considerations for electronic messaging should include the following:

- Protecting messages from unauthorized access, modification, or denial of service.
- Ensuring correct addressing and transportation of the message.
- General reliability and availability of the service.
- Legal considerations, for example requirements for electronic signatures.
- Obtaining approval prior to using external public services such as instant messaging or file sharing.
- Stronger levels of authentication controlling access from publicly accessible networks such as 2 factor authentication.

Business Information Systems :

Consideration must be given to the security and business implications of interconnecting various business information systems and these considerations should include:

- Known vulnerabilities in the administrative and accounting systems where information is shared between different parts of the organization.
- Vulnerabilities of information in business communication systems, e.g. recording phone calls or conference calls, confidentiality of calls, storage of facsimiles, opening mail, distribution of mail.
- Policy and appropriate controls to manage information sharing.
- Privacy concerns of the client as per GDPR requirements.
- Excluding categories of sensitive business information and classified documents if the system does not provide an appropriate level of protection.
- Restricting access to diary information relating to selected individuals, e.g. personnel working on sensitive projects.
- Categories of personnel, contractors or business partners allowed to use the system and the locations from which it may be accessed.
- Identifying the status of users, e.g. employees of the organization or contractors in directories for the benefit of other users.
- Retention and back-up of information held on the system.
- Fallback requirements and arrangements.

6.9. Electronic commerce services

Electronic Commerce

Security considerations and procedures for electronic commerce should include the following:

- The level of confidence each party requires in each other's claimed identity, e.g. through authentication.
- Authorization processes associated with who may set prices, issue or sign key trading documents.
- Ensuring that trading partners are fully informed of their authorizations.
- Determining and meeting requirements for confidentiality, integrity, proof of dispatch and receipt of key documents, and the non-repudiation of contracts, e.g. associated with tendering and contract processes.
- The level of trust required in the integrity of advertised price lists.
- The confidentiality of any sensitive data or information.
- The confidentiality and integrity of any order transactions, payment information, delivery address details, and confirmation of receipts.
- The degree of verification appropriate to check payment information supplied by a customer.
- Selecting the most appropriate settlement form of payment to guard against fraud.
- The level of protection required to maintain the confidentiality and integrity of order information.
- Avoidance of loss or duplication of transaction information.
- Liability associated with any fraudulent transactions.
- Insurance requirements.

Online Transactions

Security considerations for on-line transactions should include the following:

- The use of electronic signatures by each of the parties involved in the transaction. (Refer: Cryptographic Systems Policy and Procedures)
- All aspects of the transaction, i.e. ensuring that:
    - User credentials of all parties are valid and verified.
    - The transaction remains confidential. and
    - Privacy associated with all parties involved is retained.
- Communications path between all involved parties is encrypted.

- Protocols used to communicate between all involved parties are secured.
- Ensuring that the storage of the transaction details is located outside of any public accessible environment, e.g. on a storage platform existing on the organizational Intranet, and not retained and exposed on a storage medium directly accessible from the Internet.
- Where a trusted authority is used (e.g. for the purposes of issuing and maintaining digital signatures and/or digital certificates) security is integrated and embedded throughout the entire end-to-end certificate and signature management process.

Publicly Available information

- BISO should prepare and update a register containing a list of information assets that are publicly made available regularly. The inputs for this list primarily come from the annual risk assessment exercise carried out by him.
- Based on the risk assessment, he should put in place specific controls that are required to protect the integrity and authenticity of such information. He may decide to use digital certificates, Message Authentication, etc. for protecting the integrity of the information.
- Before making any information public, that information should be first reviewed by System Administrators and then approved by the Head of Operations.
- If certain information is fed into the server for making it publicly available, the systems administrator should review the information for correctness and validity after the information is entered into the server. If the information is processed before making it publicly available, then output of such information should be verified by the System Administrators before making it publicly available.
- For critical information that is required for ADEPTION operations, a third party can also be involved in verifying that the information made available to the public is accurate and authentic.
- Before making such information publicly available Head of Operations should approve them on recommendation from systems administrator
- Once the information is made public, the BISO should check how the information is displayed as viewed by the public.
- Update and Write access to such information should be given only to authorized personnel on 'least privilege' basis and Update and Write of such information should be logged and reviewed by BISO.
- Public textual information on company's website should be reviewed and authorized by the quality function of each group company before publishing the same.

6.10. Monitoring

Systems should be monitored to detect unauthorized information processing activities. Operator logs and fault logging should be used to ensure information system problems are identified.

ADEPTION should comply with all relevant legal requirements applicable to its monitoring and logging activities.

Audit logging

Audit logs must be enabled for all critical systems. Audit Logs must include the following information when relevant.

- User IDs.
- Dates, times, and details of key events, e.g. log-on and log-off.
- Terminal identity or location if possible.
- Records of successful and rejected system access attempts.
- Records of successful and rejected data and other resource access attempts.
- Changes to system configuration.
- Use of privileges.
- Use of system utilities and applications.
- Files accessed and the kind of access.
- Network addresses and protocols.
- Alarms raised by the access control system.
- Activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems.

Monitoring System Use

The CISO must conduct a Risk Assessment and identify the level of monitoring required for individual facilities.

Protection of Log information

- Log files must be protected from alterations as well as from being edited or deleted.
- Access to the log file must be restricted.
- Storage media for the log files should be chosen to reduce the risk of failure to record events of overwriting past events.

Administrator and Operator Logs

System Administrator and System operator activities must be logged. These logs should include

- The time at which an event (success or failure) occurred.
- Information about the event (e.g. files handled) or failure (e.g. error occurred, and corrective action taken).
- Which account and which administrator or operator was involved.
- Which processes were involved.

Fault Logging

- Faults reported by users or by system programs related to problems with information processing or communications systems should be logged.
- Fault logs must be reviewed by supervisors of System Administrators to ensure that faults have been satisfactorily resolved.
- It should be ensured that error logging is enabled if this system function is available.
- Logging of errors and faults can impact the performance of a system. Such logging should be enabled by competent personnel, and the level of logging required for individual systems should be determined by a risk assessment, taking performance degradation into account.

Clock synchronization

- Where a computer or communications device has the capability to operate a real-time clock, this clock should be set to an agreed standard, e.g. Coordinated Universal Time (UTC) or local standard time.
- System Administrators should ensure that the clocks on all systems are synchronized.

6.11. IT Asset Management

Software Assets

Asset Owners shall maintain a detailed list of software wholly owned by ADEPTION in the Software Asset Register.

The list shall be updated whenever software is procured, developed, shelved out or modified. For all software ADEPTION owns the following details shall be maintained:

- Name of the software, version number and vendor's name.
- The location and identity of the hardware on which the same is installed.
- Serial Key for the installation
- Total number of installations
- Location of original software installation media and documentation
- Warranty period and warranty end date if any.

System Administrators are responsible for managing the licenses for each of the software used. They should ensure that limit on the maximum number of users for licenses is not exceeded.

They should ensure that license terms of the software were not infringed.

Hardware Assets

A detailed list of hardware assets wholly owned by ADEPTION shall be maintained in the Hardware Asset Register by System Administrators. The list shall be updated whenever hardware is procured, modified or shelved out. For all hardware ADEPTION owns the following details shall be maintained:

- Type of Hardware, Serial Number and Vendor's Name
- Location of Hardware installation.
- Configuration and Make
- Date of Acquisition
- Warranty periods and warranty end date

Warranty claims shall be documented and monitored for all claims raised with the vendors. Expiration of warranty shall be followed up with appropriate and adequate maintenance contracts with the vendors.

Software Asset Management

- The responsibility of managing all software (Operating System, third-party business applications, Databases, OS of Network equipment, etc.) lies with the IT team.
- CTO should ensure that ADEPTION software is updated for new applications, only after completion of successful testing.
- CISO and BISO should subscribe to CERT, Bugtraq, vendor sites or other vulnerability-alert sites.

- Based on the alerts from various sites, the necessity and requirement for installing vulnerability patches, software updates, etc. shall be evaluated, tested and implemented by following Operational Change Control Procedures.
- In-house applications are updated as per procedures detailed in Systems Development and Maintenance Procedures.
- Databases & Application: The Operations personnel shall manage all production databases and applications. Databases and applications shall be configured as per Minimum Baseline Security Standards (MBSS). Database integrity and stability shall be continuously maintained by Database Administrators through:
    - Management of the technical requirements of the database and application according to instructions and technical releases relating to the database and application as specified by the vendors of the software application and / or the database management system.
    - Periodic cleansing of the database according to instructions and technical releases relating to the database as specified by the vendors of the software application or the database management system.
    - Manipulation of data in the application databases otherwise than through legitimate business applications that own the data are discouraged and shall be permitted only in extreme circumstances. Such changes shall require written authorisation of the business process owner of the application. In addition, such amendments to data shall be subject to change control procedures as defined in Change control Policy and Procedure Manual, including a complete backup of the database prior to any manipulation of data.

6.12. Anti-virus and Malicious Software Procedures

Installation of Virus and Malicious Software Protection Software

BISO should ensure that Anti-Virus software is installed in all possible entry points (Network gateways, Servers, Desktops, etc.) of viruses and Malicious Software. He should also ensure that they are installed with the latest version of the Anti – Virus Software.

Update of Virus 'DAT files'

These are the files, which contain the data on virus signatures. The update of anti-virus can be automated using software or can be done manually.

- Automatic Update
    - A system connected to the Internet checks the vendor site at a scheduled time for any new virus updates.
    - If there is any update it will download, and it should push the update to a server.
    - From the server, an operating system job should be scheduled in the network server for pushing these DAT file updates onto servers/client computers/laptop computers/network nodes connected.
    - This job should be scheduled to run immediately after copying the DAT files on the central host computers.
    - Specific vendor software can also be used to push DAT files on the clients / servers.
- Manual Update
    - A system connected to the Internet checks the vendor site at a scheduled time for any new virus updates.
    - If there is any update it will download, and it should notify the System Administrator about the new update.
    - The system administrator should then update the servers / desktops / laptop computers with the latest virus DAT files.

Anti-Virus software upgrades

The upgrades are the newer versions of the anti-virus software. It is the responsibility of the BISO to procure and provide newer versions/engines of Anti-virus programs in regular and timely manner and ensure a quick rollout.

Review of Logs

BISO should check the logs of the desktops / laptop computers / servers that were infected with viruses. He should report to the CISO about virus incidents detected and removed.

BISO should check the anti-virus software activity/logs, especially to check whether the users are running the AV system regularly on their desktop computers (in case the user has the option to stop the scan).

BISO's should also check all the servers / desktops to ensure that they are updated with the latest version.

7. System Planning and Acceptance

7.1. Systems Planning Procedures

Technology Infrastructure requirements are identified during the Technology Infrastructure planning process. Technology planning is a process that helps ADEPTION in maximizing technology investments by following a systematic approach to identify and implement the required technologies to accomplish ADEPTION's objectives. Technology Infrastructure planning typically consists of the following phases:

Formation of Technology Planning Team

The CTO should form a Technology Planning team consisting of Heads of Departments, BISO and relevant Business Process Owners of ADEPTION.

The Business Process Owners should primarily play a role in identifying and clarifying ADEPTION's business needs. Responsibilities for all persons should be distributed appropriately and expectations must be set clearly so that each person is involved in the process.

It is also imperative that management should support the Technology Planning process actively. As management buy-in is required for obtaining the required funding for the plan, the management should be convinced on the need for the technology infrastructure identified in the plan.

Identification of Requirements

In this step, the information system needs of ADEPTION should be identified. The needs will primarily flow from the business plans and IT Plans of ADEPTION.

The Business Process Owners should play an important role in this phase in identifying and advocating the need. During this phase, the team should also analyze regulatory requirements.

The CTO, Head of Operations, BISO and Head of Networking should convert the Business needs into technology needs. Having identified the needs of ADEPTION, it is also important to prioritize the needs. This will facilitate the implementation of the infrastructure in a systematic way.

Analysis of available resources & solution

Once the needs are identified, the next step is to make a concrete plan on how to meet these needs. This phase of planning requires high-level technical knowledge. Having identified the needs in the previous step, the most suitable technology options that can satisfy the needs of ADEPTION should be identified.

Certain technology requirements may be satisfied by the existing information processing resources. In these cases, it is important to analyze the existing capacity and based on those future capacity requirements needs to be identified. Following steps should be followed in using the capacity of existing infrastructure.

- Determine required workload: The workload that each resource of the information system should cater to should be characterized in terms of its individual components. System requirements for each element of the information system should be ascertained to allow for acceptable processing of the workload.
- Analyze Current Capacity: There are several steps that should be performed during the analysis of capacity measurement data.
- Check the usage of the various resources of the system (CPU, memory, I/O devices, and Network Bandwidth). This analysis identifies highly used resources that may prove problematic now or in the future.
- Look at the resource utilization for each workload. Ascertain which workloads are the major users of each resource. This helps narrow down the attention to only the workloads that are making the greatest demands on system resources.
- Determine where each workload is spending its time by analyzing the components of response time, allowing to determine which system resources are responsible for the greatest portion of the response time for each workload.

Measure Overall Resource Usage

It is also important to look at each resource within the systems to see if any of them are saturated. If it is found that a resource is running at 100% utilization, then any workloads using that resource are likely to have poor response time. If the goal is throughput rather than response time, utilization is still very important.

e.g. If there are two disk controllers, for example, and one is 50% utilized and the other is swamped, then there is an opportunity to improve throughput by spreading the work more evenly between the controllers.

Measure Resource Usage by Workload

Alternatively, the resource utilization for each workload can be analyzed, which would clearly throw up the possible bottlenecks that each workload faces in terms of resources.

Identify Components of Response Time

The resources that are responsible for the greatest share of the response time are indicators for where one should concentrate the efforts to optimize performance. Hence it is possible to determine the components of response time on a workload-by-workload basis, and it can be predicted what the components will be after a ramp-up in business or a change in system configuration.

Determine capacity requirements

After the existing capacity requirement is identified, future requirements should be identified. The future requirements flow from requirements identified in the previous phase (Identification of Requirements). After system capacity requirements for the future are identified, a capacity plan should be developed. The plan should contain the following:

  - How to use the existing capacity to meet the future requirements.

- How to augment the existing capacity to meet the future requirements.
- Timelines and implementation for meeting the requirements.
- In selecting the most suitable new information processing resources, the following considerations should be addressed:
    - Ability to support the current and future needs.
    - Nature of the Technology (Commercial off the shelf package, customized product or in house development)
    - Compatibility with existing and other systems
    - Price
    - Performance & Security requirements
    - Regulatory requirements
    - Cost – benefit analysis
    - Alternatives for the technology
    - Existing customers of the technology
    - Maintenance, Support and ease of usage

Preparation of Technology Plan

The analysis done in the previous step should be documented as action plans and projects. The documentation should include the following aspects:

- Business requirements translated into IT needs.
- Technology that best satisfies the need.
- Probable cost, and Cost-Benefit Analysis
- Action plan for acquiring or development of the solution.
- Possible Implementation plan with high level deadlines for the projects

The documentation should be comprehensive so that it can serve as a supporting case for each of the technologies identified.

The plan should be approved by the CTO for implementation.

Updating of the Plan

The Technology Plan should be a living, breathing document. As new needs and priorities come up, the Plan should be suitably modified. The technology team should meet every quarter to review the plan so that new needs, priorities, trends and technologies are analyzed and updated in the plan, which then can be converted into action plans for implementation.

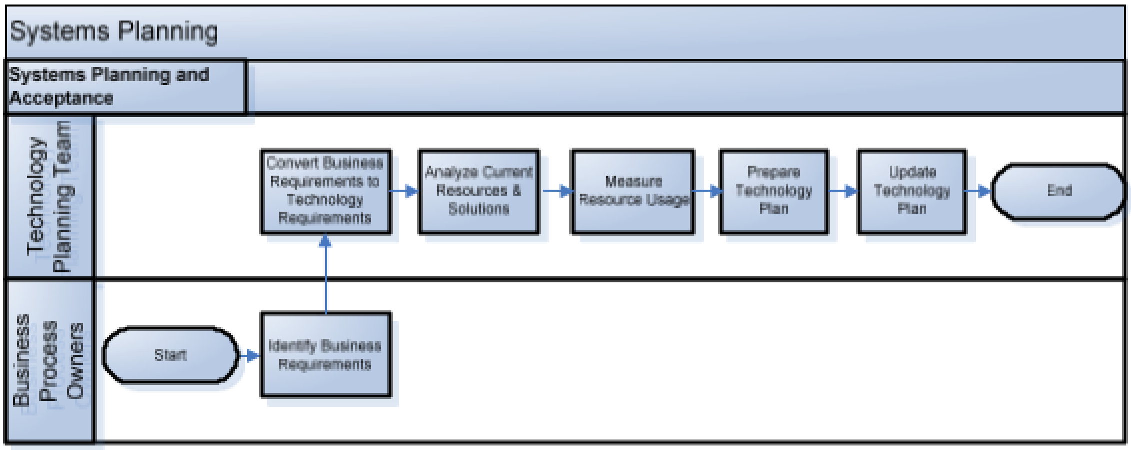
Systems Planning (Process Chart)

7.2. Capacity Monitoring Procedures

Monitoring System Performance

Important aspects such as disk usage, memory, CPU utilization of critical application systems should be monitored by System Administrators on a daily basis to ensure that any anomaly or potential disruptions are detected early and corrective action can be taken. Network equipment should be monitored by Network Administrators at multiple points of time every day for memory and CPU utilization.

If the disk space is over utilized by system or application data, System Administrators should request CTO for increasing the storage space or alternatively, reduce the data managed by deleting some of the historical data after approvals from CTO and BISO.


Systems Planning
Systems Planning and Acceptance
Technology Planning Team
Business Process Owners
Start
Identify Business Requirements
Convert Business Requirements to Technology Requirements
Analyze Current Resources & Solutions
Measure Resource Usage
Prepare Technology Plan
Update Technology Plan
End

Monitoring Bandwidth Utilization

The Network Administrator should regularly supervise the bandwidth utilization using tools or custom scripts and peak levels should be defined in the bandwidth-monitoring tools / scripts such that alerts are generated and automatically communicated to the Network team so that the team is made aware of the choking or disruption of any particular link.

Monitoring Parameter Thresholds

Component	Parameter	Point-in-Time Threshold Levels	Period of Time Threshold Levels
Servers	RAM	85%	75%
	Hard disk	80%	70%

	CPU	85%	70%
Network Devices	RAM	85%	75%
	CPU	85%	70%
Links	Link Utilization	80%	75%
	Verification of Service Levels against SLA	Based on parameters defined agreed in SLA	Based on parameters defined agreed in SLA

Reporting

System Administrators monitoring various information systems should update capacity monitoring. This should be reviewed by supervisors of Systems Administrators on a weekly basis.

Quarterly reports based on the above forms should be generated to clearly depict patterns of utilization of System performance and Bandwidth over a period of time. These should be submitted to the Head of Operations and BISO.

7.3. Systems Acceptance Procedures

Any new information processing system internally developed or purchased should be evaluated well before accepting for implementation in the production environment. Systems acceptance process consists of the following phases:

Setting up Acceptance Criteria

Acceptance criteria for new information systems, upgrades and new versions should be established by the Technology Planning Team and suitable tests of the system should be carried out prior to acceptance. The following controls should be considered:

- Business functionality requirements from the new system.
- Information Security Requirements
- System performance and capacity requirements as per the business need.
- Availability of routine operating procedures for all activities related to the system.
- In the case of critical systems, the training of certain personnel in the manual operational processes and the functional user processes.
- Agreed minimal set of security controls in place.
- GDPR privacy concerns are met.
- Business continuity arrangements within the critical systems and their alignment with the other systems in the environment
- Service level definitions and vendor commitments in the case of critical systems.

- Test reports that hold evidence that installation of the new system will not adversely affect existing systems, particularly at peak processing times. In the case of critical systems, ADEPTION may even test this in a simulated laboratory environment of the vendor based on peak load inputs (as expected by ADEPTION team).
- A preliminary risk assessment of the effect the new system has on the overall security of the company.

For major new developments, the business users should be consulted at all stages in the development process to ensure the operational efficiency of the proposed system design.

Prepare for System Acceptance

In this phase the system, the test environment is finalized and established, and a detailed test plan is prepared. The testing team will identify and deploy the necessary tools and information systems required for the testing. Preparation of the environment in which acceptance testing will be performed should be primarily focused on confirming that it is as close to the production environment as possible. This will ensure that the test environment is ready and operational before the acceptance testing begins.

Validate the Acceptance Criteria & Claims

In this phase, the acceptance criteria defined by ADEPTION personnel, and the claims made by the information system developer or vendor are matched and validated. Based on these criteria and claims the Test plan is updated to create specific test scenarios. Any test data required for testing should be uploaded into the system during this phase. Configuration of the information system should be set like the production system. At the end of this phase the system should be ready for testing.

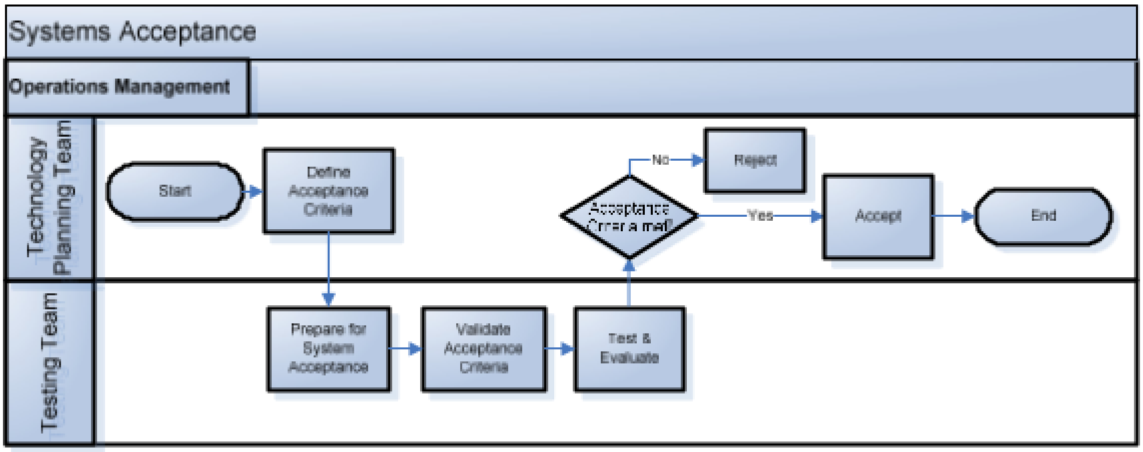
Testing & Evaluation

In this phase, the acceptance criteria is tested and evaluated as detailed in the test plan. A complete suite of tests is performed against the system under evaluation and the results are observed and documented. Any observations identified contradictory to the criteria and claims should be documented & reported to the Head of Operations and CTO. CTO should analyze the test results and evaluate the seriousness of the deviations.

Acceptance

Based on the test results CTO may decide to accept the information system for implementation in ADEPTION facility. The system should be accepted only if they are acceptable. Otherwise, the CTO may allow the vendor or the developer to modify the system to resolve the deviation. In those cases, only the test corresponding to the deviant observation should be tested again before accepting the solution.

System Acceptance (Process Chart)



8. Backup & Recovery

8.1. Identification of Data to be backed up

- The Technology Planning Team (consisting of Heads of Departments, Business Process Owners and BISO. refer: System Acceptance Procedures) should decide on application and operating systems software, data (including databases), application and operating systems configuration information, hardware configuration information (where applicable) and Log files / Logs from various systems that need to be backed.
- They should also decide and document the frequency of data to be backed up, medium of backup, location of storage of the backup media, retention period for the backup and overall backup plan for that data.
- The users are responsible for taking and maintaining the backup of all critical data residing on their individual workstations. They should fill in the backup instruction form if they need to back up from their workstations. The request should be approved by respective Departmental Heads.
- Based on the data identified for the backup a daily, weekly, monthly backup schedule should be prepared by system administrators.

8.2. Data Backup Procedure

- Backup Administrators should set up an automated process or use backup software to backup all identified data.
- Backup Administrators should monitor the backup software logs. He should also store them securely for possible future reference.

8.3. Storage of backup

Cloud storage

Data back-up should be maintained in a geo-redundant cloud storage environment that is accessible to the Backup Administrator from any location.

8.4. Backup Restoration

- If a backup restoration is required due to data loss or for testing purposes, the user should make a request for restoration and get the approval from the Manager of Operations for the request. The Manager should ensure that the user has the right to access the data required for restoration. Once the approval and authorization is obtained, the data should be restored by the System Administrators.
- A log should be maintained by the Backup Administrator, containing the date and time along with the name and signature of the person who requested for the restoration of the data. In case of emergency restorations, a telephonic approval from Manager-Operations is

sufficient but all necessary procedures and documentation should be completed after the restoration has been successfully carried out.

8.5. Restoration testing

- To verify the readability of backup media, readability, mock restoration tests should be carried out by System Administrators, at least once in a month on the test servers.

~~o~~The entire process should be documented detailing the test plan, the activities carried out and the test results. ‘Cloud backup’ should be used for such restoration. It should be ensured that the restored data is deleted from the test servers after successful completion of testing.

(Refer: Asset Classification & Control Policy for deletion procedures)

9. Vendor Management

9.1. Outsourcing Procedures

Goals and Objectives

Project Team (Refer: System Acceptance Procedures) should articulate the goals and objectives of the outsourcing initiative and communicate how the process will benefit the organization. The outsourcing initiative should serve the objective of ADEPTION to concentrate on core competencies, obtain financial benefits and gain competitive advantage.

Team constitution

The coordination for constituting the project team and evaluation of the outsourcing should be performed by the CTO.

Business rationale & Risk Assessment

The Project Team should identify and document the rationale behind outsourcing an activity and perform a cost – benefit analysis of outsourcing the activity. The project team should prepare a document on the business rationale & risk assessment and present it to the CTO for analysis and discussion. The document should cover, among other things:

- Definition of the type of outsourcing (e.g. applications processing, software maintenance, contingency/disaster recovery planning)
- The type of information or data processing functions or services to be outsourced.
- Reasons for opting to outsource an activity. and
- High-level Cost-Benefit analysis.
- The reasons for outsourcing the function or service.
- Background information about the third party

9.2. Vendor Selection Procedure

Invitation of Bids

Upon obtaining the necessary approval from CTO, the process for Vendor selection should be initiated for the activity to be outsourced. The team should invite at least three parties for the bid. Exceptions should be noted and appropriately approved by CTO. A Request for Proposal ('RFP') should be issued to the bidding parties with adequate time for response. The team leader in consultation with the key team members should prepare an analysis of chosen vendors with their comments.

Vendor Analysis & Evaluation

Prospective vendors, who would provide documentation of the product or service, demonstrate the functionality or details of services and offer formal proposals, should be identified. The supplier data along with credentials performance should also be reviewed. Contract requirements detailing expected quality, acceptable performance and criteria, contract provisions, payments options and their direct linkage to deliverables should be prepared. The contracts should be finalized after obtaining the concurrence from the legal department. Once the proposals are received, they should be evaluated against the desired and critical functionality, quality specifications, payment terms, future maintenance service and support from vendors.

The Vendor analysis should cover at the minimum parameters mentioned in the Vendor Selection Criteria.

ADEPTION should consider interviewing and analyzing the skills of personnel proposed to be deployed by the Outsourced Party on ADEPTION's sites.

Vendor Selection

Based on the analysis and the evaluation criteria, the team should select the best vendor satisfying all the requirements of ADEPTION. The team should document the reasons for selecting the vendor and the possible risk factors associated with the vendor. This analysis is presented to the CTO for approval. The strategic sourcing team will have the final authority to select the vendor based on the merits.

9.3. Contracts, SLA and NDA procedures

Once the vendor is selected, a formal contract should be signed with the service provider. Contract should include all legalities followed by ADEPTION. The contract should be bound by a strong Service Level Agreement (SLA) to ensure that the service provider provides a defined level of service continuously and efficiently without disrupting the operations in ADEPTION. It should be ensured that the SLA is fair and equitable to both parties, clear, complete and documents the 'exit' clauses precisely. ADEPTION should ensure the following:

- Usage of SLAs with measurable parameters as the prime reference against which to manage and measure the Vendor's performance.
- Adequate time scales before renewing the contract to allow time for review of past performance.
- System Availability: Overall system availability is the most stated service level that is associated with non-performance clauses.
- SLA should also include mutually acceptable punitive clauses to handle breach of SLA.

ADEPTION will subject outsourced parties such as vendors, auditors, consultants, etc., to the same access restrictions to which an internal user would be subject. Since Confidential/Internal information cannot be controlled once it is distributed outside ADEPTION. third-party access to the same should be restricted to the information they require in completing the contracted work. Non-Disclosure agreement (NDA) / Confidentiality agreement should be signed by vendors, third parties, contractors and also by subcontractors of the vendors in order to protect ADEPTION's information assets.

Every employee of the vendor who is involved in the outsourcing activities of ADEPTION should sign the Non-Disclosure / Confidentiality agreement.

9.4. Risk Assessment & Security Measures

Prior to outsourcing the actual process after deciding the vendor, BISO should conduct a Risk Assessment specific to the vendor that is being outsourced. BISO should obtain and study the Business Continuity Plans (BCP) / Disaster Recovery Plans (DRP) of the vendor to understand the state of readiness/preparedness of the vendor to meet eventualities and the corresponding risk to ADEPTION's operations. Security measures that need to be implemented by ADEPTION and the vendor will be identified as a result of this Risk Assessment and Risk assessment carried out when ADEPTION was evaluating the benefits of outsourcing. Implementation of these measures should be added as part of the contract / SLA.

9.5. Subcontracting by the Vendor

The SLA/Contracts with key vendors should include ADEPTION's policy on subcontracting issues, and to clearly specify the minimum acceptable performance levels with an emphasis on enforcing with immediate effect. The system of outsourcing should address the subcontracting issues by the vendor. There should be a minimum acceptable performance level enforced by SLA, expected from the vendor in the event of sub-contracting.

ADEPTION should reserve the right to accept or reject a sub-contractor if there are strong reasons to do so.

9.6. Vendor Relationship Management

The strategic sourcing Team should establish relationship management teams, made up of people from both organizations, required at two levels — operational, and overall relationship management. These teams should have clearly defined responsibilities, relationships to the other teams and procedures for their operations.

The team should meet regularly in accordance with the team's responsibilities. Operational teams should meet continually.

One person from ADEPTION and one person from the vendor should be established as a single point of contact to manage operational issues. Appropriate escalation hierarchy should be established for each of the vendors to resolve outstanding issues related to outsourcing. The strategic sourcing team and the relation management teams should be updated regularly about the operational issues faced by ADEPTION.

9.7. Vendor Management Standard

Considerations for Contract

Other than the regular legal issues, ADEPTION should consider including the following information security related aspects in the contract with the vendor.

- General policy on Information Security
- Procedures regarding protection of assets
- Description of each service to be made available.
- Provision for the transfer of staff where appropriate.
- The respective liabilities of the parties to the agreement.
- Specific Access Control procedures
- The establishment of an escalation process for problem resolution. Contingency arrangements should also be considered where appropriate.
- Responsibilities regarding hardware and software installation and maintenance.
- A clear and specified process of change management.
- Involvement of the third party with subcontractors.
- How information security related legal requirements are to be met.
- What arrangements will be in place to ensure that all parties involved in the outsourcing, including subcontractors, are aware of their security responsibilities?
- How the integrity and confidentiality of the organization’s business assets are to be maintained and tested.
- What physical and logical controls will be used to restrict and limit the access to the organization’s sensitive business information to authorized users?
- How the availability of services is to be maintained in the event of a disaster.
- What levels of physical security are to be provided for outsourced equipment?
- The right to review and audit the processes and security controls.

Considerations for SLA

The Parties	
ADEPTION	*Description of ADEPTION, including location, contact telephone and telefax numbers, email addresses, and contact names.*
The Vendor	*Description of the Vendor, including names, titles, locations, contact numbers and addresses.*
Agreement	
Services	*Agreement on the "Services specification", below.*
Staff Competence	*Agreement by the vendor that staff will be competent.*
STAFF AVAILABILITY	*Agreement that selected vendor staff will be available for a minimum time period specified before being rotated.*
Changes	*Agreement on the "Service change procedures", below.*
Contingency Planning	*Agreement on the "Contingency planning procedures", below.*
Termination	*Agreement on conditions under which the agreement may be terminated.*
Services Specification	
Business Need	*General statement of the business need and the reasons for outsourcing.*
Statement of the Service to be provided	*the Description of each Service to be provided, including its end users, its Services to be provided performance criteria (Service Levels) and its performance measures*
Resources	*Description of the resources that the outsourcer will apply to the Services.*
Security	*Description of the security methods to be used to protect ADEPTION's applications and data.*
Support	*Description of the support normally available to ADEPTION, including Service Levels and performance criteria.*
Limitations	*Description of limitations upon the provision of the Services, such as hours of operation, including, where appropriate, Service Levels.*

Reporting	Description of the standard reporting process, including details of the statistics on Service Levels and performance measures to be provided and the frequency of reporting. Description of the processes by which ADEPTION will make information available, at the request of the vendor. Description of the processes by which ADEPTION will monitor reporting on statistics and performance measures to determine the Service Levels.
Training	Description of the training available to ADEPTION, including training in the Services and training which is otherwise available.
Performance Measurement	Description of the methods by which customer satisfaction will be measured, including, where appropriate, Service Levels and performance measures.
Service Change Procedures	
Changes requested by Description of the process by which ADEPTION will request changes. ADEPTION	
Expected expansion	Description of the processes and methods to be used by ADEPTION to allow for expected expansion of the Services, including, where necessary, any changes to the Service Levels.
Contingency Planning Procedures	
Outages	Description of the process to be used and it’s the Service Levels specified for informing ADEPTION of planned outages.
Failure correction	Description of the process to be used for service faults and failures, including the methods for keeping ADEPTION informed for the situation and progress towards a resolution.
Escalation	Description of the escalation procedures to be used by The Vendor to correct faults and failures, including contact points, methods of reporting faults, information required about faults, their priorities and their potential impacts.
Security Requirements	
POLICY	The general policy on Information Security

ASSET PROTECTION	*Procedures to protect organizational assets, including information and software.* *Procedures to determine whether any compromise of the assets, e.g. loss or modification of data, has occurred.* *Controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during, the contract.* *Integrity and availability* *Restrictions on copying and disclosing information*
LIABILITIES	*The respective liabilities of the parties to the agreement*
Indemnity	*Arrangements to cover the losses incurred to ADEPTION due to inadequate service provided by the vendor*
NOTIFICATION	*Arrangements for reporting, notification and investigation of security incidents and security breaches*

10. Access Control

10.1. User Account Management

Requisition for New User Accounts

- Every user requiring access should complete the requisition form for Creation of New User Account and forward it to system administrator for operating system and email access or network administrator for access to network devices and services or application administration for application and database access after approval & authorization.
- The reporting manager should approve new user accounts.
- For third party users (consultants, auditors, vendors, etc.), a person coordinating with the third party shall approve the approval and authorization shall be given after analyzing whether the access rights requested by the user are the minimum required to perform his/ her duties. Privilege – Job Function matrix should be referred for this purpose.
- Administrators should verify the completeness of the form, authorization, and approval before creating the user accounts.
- Administrators should verify that the requested user does not already have a user account.
- System Administrators and Application Administrators should maintain a list of user credentials (Operating Systems, Applications, Databases, etc.) along with full name, designation and contact information of the user. Network administrators should maintain user credentials for network equipment and other network services. They should update the list when a user account is created, modified and deleted.
- Common user IDs must not be issued to multiple users when it is technically feasible to provide individual IDs. In situations where a common ID is required, specific permission and authorization must be taken from the CTO and BISO, detailing the reason and users who have been granted the right to use this ID and password.
- For contract employees and consultants, a user account having expiration date, which coincides with the conclusion of the contracted project, shall be created. else care shall be taken by the system administrator to disable the account on the expiry date. In case the id is still required, the account shall be kept active after seeking an approval.

Removal of User Accounts on Transfer / Termination

- The administrators must ensure that the user-ID is revoked upon termination or resignation of employees and revoked, or access modified upon change of responsibilities. BISO shall review to ensure that the user credentials are removed, or access rights are revoked on the last working day of the terminated employee.
- In cases where a common user account is used or the resigned employee's user account needs to be maintained for auditing purposes or if the application does not permit to remove the user account, then

passwords of these accounts should be changed on the last working day of the employee.

- The departmental head shall ensure that all the responsibilities are transferred to another individual.
- The departmental head shall also monitor the activities of the resigned / terminated employee from the moment he resigns.
- The HR function should ensure that all ADEPTION assets with the employees such as PCs, keys, ID cards, proximity cards, software, data, documentation, manuals etc. of terminated employees must be returned to the employee's departmental head or the Human Resource Department.
- Above procedures shall be followed also for involuntary termination of the employees.

10.2. Privilege Management

Privilege – Job function Matrix

- System administrators, Network Administrators, Application administrators along with the help of BISO and Departmental heads should identify all the privileges associated with all Operating System, Business applications, Databases and Network elements used within individual businesses.
- These privileges should then be mapped with the job functions of the personnel involved in ADEPTION's operations to develop and document Privilege – Job Function Matrix. In most applications, operating systems and database privileges required for performing a job function are put together to create an application role for effective and secure management of access privileges. Wherever applicable, application roles should be created for each of the corresponding job functions in the business.
- This exercise should be carried out whenever an Application or Operating System or a Database or network equipment is to be used for the first time.
- Privilege – Job function Matrix should be modified by system administrators/ application administrators/ network administrators in the following scenarios.
    - When an Application, Operating System, Database or network equipment undergoes a major change or new module, or functionality is added.
    - A new job function or role is created • Job Function or Role is changed.
- Privilege – Job Function Matrix should be approved by the business team and CTO before implementation.
- Granting Privileges

- Privileges are granted to users on two occasions. One is during the creation of a user account and when a user requests for additional privileges due to changes in job function or changes in responsibilities. Users assigned high privileges for special purposes should be required to use a different user identity for normal business use (e.g. "System Administrator" login is not to be used for running the application).
- When a new user is created, the privileges should be granted as per the request after verifying the approval and authorization. Once the access privileges are granted then it should be updated by the person who creates the user.
- If a user requires additional access rights, then he should fill the Additional Access Request Form and forward it to departmental head and BISO for approval and authorization.
- Once the access privileges are granted then it should be updated by the person who granted additional privileges.

Review of Privileges

While the Departmental head shall review the access granted to his/her department personnel quarterly, the BISO shall review the List of Users in various information systems along with their access privileges on a quarterly basis. He/she should verify in the information systems whether the privileges granted to the user are as per what is approved and documented.

- BISO should verify whether the granted privileges are removed when the expiry date of them is over.
- BISO should also check whether any additional privileges are obtained in an unauthorized manner.

10.3. Password Management

Password Parameters in Operating System, Applications, Databases and network equipment shall be configured as per password management policies detailed in Information Security Policy – Access Control Policies. Wherever password policies cannot be configured due to certain limitations, the same shall be documented.

Storage and Management of Critical Passwords

Below listed table explains what type of passwords are called critical passwords. These passwords should be carefully managed to ensure that these passwords are not forgotten or are not lost.

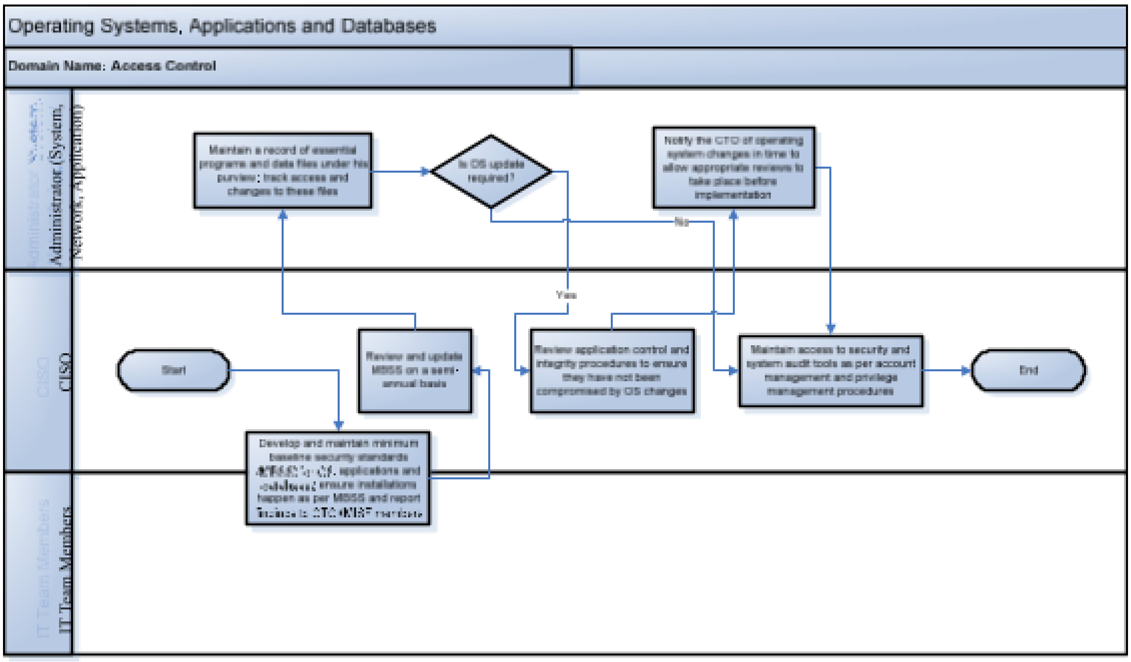
System	*Types of Passwords*
Operating Systems	*Administrator Password(s)*
Information System / Business Application	*Super User Password (where available) Business Applications* *Administrator Password*

	System Password (for database connectivity) where available
Databases	*Database Super User Password* *Database Administrator Password* *Database Security Officer Password*

Critical passwords can be stored and managed using software password vaults. In these cases, software specific handling procedures should be documented and followed.

10.4. Operating System, Applications & Databases

- CISO along with other members of the IT team should develop and maintain Minimum Baseline Security standards (MBSS) for Operating Systems, Applications and Databases. CISO shall consider the following during the development of MBSS:


Operating Systems, Applications and Databases
Domain Name: Access Control
Administrator (System, Network, Application)
CISO
IT Team Members
Maintain a record of essential programs and data files under his purview; track access and changes to these files
Is OS update required?
Notify the CTO of operating system changes in time to allow appropriate reviews to take place before implementation
No
Yes
Start
Review and update MBSS on a semi-annual basis
Review application control and integrity procedures to ensure they have not been compromised by OS changes
Maintain access to security and system audit tools as per account management and privilege management procedures
End
Develop and maintain minimum baseline security standards (MBSS) for OS, applications and databases; ensure installations happen as per MBSS and report findings to CTO/ISSC members

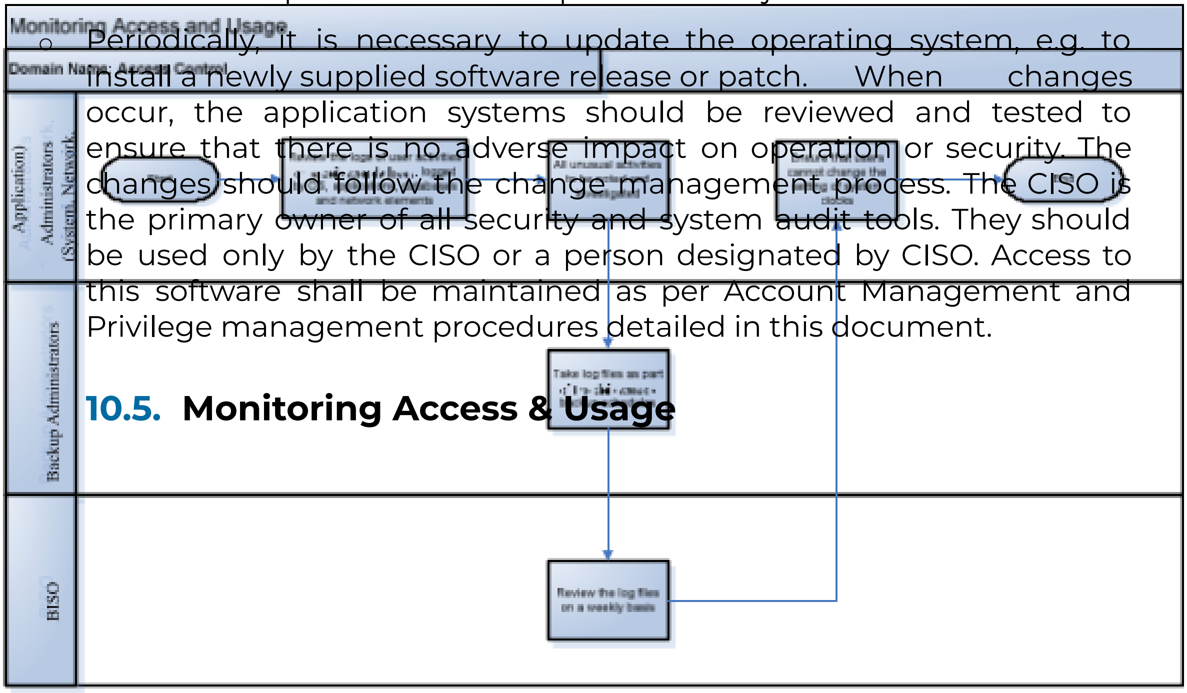
  - All the policy requirements for Operating Systems, Applications and Databases as detailed in Access Control Policy
  - Restriction on use of various type of user accounts
  - Restriction on access advanced programs and utilities
  - Restriction on access to OS commands

- He shall also ensure that all the installations of OS, Applications and Databases are configured as per MBSS.
- Prior to implementation, the CISO should ensure that the system administrator is adequately trained to understand security. Access to systems must not be allowed until security administration functions are in place.
- CISO along with the BISOs should review all installations of Operating System, applications and Databases on an annual basis to ensure that all of them are configured as per MBSS. He should report the findings of the review to the CTO and other members of the Infosec Steering Committee.
- Adequate licenses must be obtained for the operating system installed on the systems, workstations as well as production systems. After the

installation of the operating system and before its usage, a full backup of the operating system must be taken on production servers. Any subsequent changes must have a proper version backup.

- The direct access to OS Commands and through sensitive utilities accessing operating system commands must be restricted to those users who require this access to perform their job functions.
- Periodically, it is necessary to update the operating system, e.g. to install a newly supplied software release or patch. When changes occur, the application systems should be reviewed and tested to ensure that there is no adverse impact on operation or security. The changes should follow the change management process. The CISO is the primary owner of all security and system audit tools. They should be used only by the CISO or a person designated by CISO. Access to this software shall be maintained as per Account Management and Privilege management procedures detailed in this document.

10.5. Monitoring Access & Usage


Monitoring Access and Usage
Domain Name: Access Control
Administrators (System, Network, Application)
All unusual activities to be noted and investigated
Take log files as part of
Backup Administrators
Review the log files on a weekly basis
BISO

All user activities must be logged by the operating systems, applications, Databases and network elements. If logging degrades the performance of the systems, only critical commands or actions should be logged and monitored. Respective system and network administrators must review the logs on a daily basis wherever feasible. else review should be on a weekly basis. All unusual activities must be noted and investigated by them.

Logging of Application/OS Activities

All Applications, Operating Systems and Network Equipment must have audit logs enabled. Log files must record the following:

- Login failures / success
- Account lockouts.
- All system or application administrator actions
- System or application start, stop, re-initialization (with user identity and time of action)

Other actions that need to be monitored shall be identified based on the specific risks identified in the application, operating system and network elements. Events that are monitored are also dependent on the amount of log that each event generates and the load on the application due to logging.

The audit logs should include the following:

- User IDs.
- Dates and times for log-on and log-off.
- Terminal identity or location if possible.
- Records of successful and rejected system access attempts.
- Records of successful and rejected data and other resource access attempts.

Operating Systems, Applications and Network equipment should be configured in such a way that log files are not overwritten or deleted. Log files should be taken as part of the daily/weekly backup schedules by backup administrators.

Log files should be accessed only by the System administrators, CTO and BISO. Applications, Operating System and Network elements should be configured in such a way that normal users cannot read, write and delete the logs.

Review of Logs

- Log files should be monitored daily or weekly by the respective administrators. Monitoring should be performed by personnel who are not involved in performing any administrative duties.

Synchronization of System Clocks

The correct setting of system clocks is important to ensure the accuracy of audit logs, which is required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs hinder such investigations and damage the credibility of such evidence. A system shall be put in place to ensure that all the servers, network equipments and desktops are synchronized to have the same time.

The network administrators must ensure that users cannot change this setting.

Automatic Connection Time-out of On-line Terminals

Where technically feasible, the OS must be configured to time-out on-line terminals/desktops/laptops after 10 minutes of inactivity. Screen saver password should be enabled for all the OS.

11. Network Security

ADEPTION's network must be used for valid business purposes only. The protection of information contained on the company networks is therefore the responsibility of the management and the activity and content of user information on the company computer networks is within the scope of review by management.

ADEPTION shall develop and implement network security systems and procedures, and provide network security resources (Firewall, IDS, etc.) to protect all business data, related application systems and operating systems software from unauthorized or illegal access at a level that is appropriate for the information /computing resources.

11.1. Network Access Management

- Network Services – Job Function Matrix
- Network administrators along with the help of BISO should identify all network services (E-mail, Internet, Telnet, Network File Server, FTP, etc.) used in ADEPTION. Network administrators should also identify various types of privileges available within the network services.
- These services along with the types of privileges should then be mapped with the job functions of the personnel involved in ADEPTION's operations to develop and document Network Service – Job Function Matrix.
- At the end of this exercise all network services including privileges required for access should have been identified and documented. This should be reviewed and approved by Head – Infrastructure.
- This exercise should be carried out when network services are to be used for the first time.
- Network Service – Job function Matrix should be modified by Network administrators if a new job-function is created or when network services are changed significantly.
- The changes to Network Service – Job Function Matrix should be reviewed and approved by Head – Infrastructure before implementation.

Granting Network Access

Refer: 'Requisition for New User Accounts' in Access Control Procedures

Review of Network Privileges

Refer: 'Review of Privileges' in Access Control Procedures

Access to Third Parties, External Agencies

ADEPTION may need to provide access to external parties like customers, vendors, service providers, etc. ADEPTION may have to provide normal or privileged access to its information systems for other agencies to conduct business transactions with other parties or share information.

The following procedures should be followed for managing interactions with other parties:

- Business process owners should initiate access requirements for external parties as well as requirements of access to external parties.
- For long period (more than 2 weeks) access requirements, ADEPTION should first sign a Mutually Acceptable Agreement / Contract with the third-party for providing access to them. This should include the following aspects.
- Information that is to be shared.
- Details on security policies applicable on the third party.
- Legal implications of misuse of ADEPTION's resources
- The Third-party shall fill in a form or attain permission via an email. The form or email should contain what type of access is required, which application is going to be used, what data is going to be transmitted, encryption methodology required/used, etc. This shall be then approved by the Business Process Owner interacting with the third-party. Access is provided by the network administrator after review by the BISO. If a third party needs to gain access to ADEPTION's resources for a short period of time, following must be the procedures to be followed while granting the access rights to the third party:

    - An access right form or email approval must be completed by the third party and approved by BISO stating all the levels of access required (read or write).

    - In case the third party wants to modify any data they must obtain approval from the respective business process. On receiving intimation, the network administrator must create separate IDs for the third party.

    - Network administrators must do a fortnightly review of the activity logs generated at the Operating System level to monitor the activities performed by the third party. The business or technology employee coordinating with the third party shall view the actions being taken by the connecting vendor when the connection is provided for debugging or support on production systems.

    - If ADEPTION requires access to systems of other agencies, ADEPTION shall follow procedures and guidelines imposed by the external agencies. Internally, the access should be approved by the Business Process Owners and BISO.

Internet Service Access Request

- All employees will be granted internet access after the creation of domain user-ids.
- Access to the internet should be automatically revoked for employees on revocation of their domain id. Any overriding of Internet access policies shall be approved by the CTO and BISO after giving justification of the policy overriding requirement. The overriding could be access to restricted sites, downloading of any software programs, etc.

11.2. Network Management

Routers, Firewalls & Modems are integral components of Network Security Architecture. Other than these three, there are other network elements that exist in a corporate network which include switches, bridges, hubs, etc. Given its key role in protecting the network from intruders, adequate time and resources should be assigned for maintenance of Routers, Firewalls and Modems.

Network Change Management

Any changes to the network components such as firewall rule changes, router access control list changes, configuration changes, upgradation of network infrastructure should follow the Operational Change Management Procedures. (Refer: Communications and Operations Management – Operational Change Management Procedures)

Network Diagram

The CTO and Infrastructure Head should be responsible for maintaining an updated network diagram. Periodic reviews must be conducted by the CISO to ensure that the diagram is updated to reflect the existing network architecture. Network Diagrams should be updated as and when there are changes made to the network architecture.

11.3. Data Transmission

Use of Encryption Technology

Refer: Cryptographic Systems Policy and Procedures

11.4. Network Assessment

- Vulnerability assessment of information resources in the ADEPTION network should be performed on an ongoing basis to test for known software flaws and weaknesses. This activity should be coordinated by the CISO. New exploits are continuously discovered and must be tested for on a consistent basis. It is important to verify that all known software flaws are addressed adequately. Appropriate action should be taken as and when vulnerabilities are identified during the assessment.
- The BISO along with other members of the IT Team shall prepare list of assets on which the assessment should be carried out. They should prepare an ongoing assessment plan for all the assets and carry out the assessment on all identified assets as planned.

- The BISO should also verify whether all the network resources are configured as per Minimum Baseline for Secure Configuration Standards. The BISO should ensure use of proven Vulnerability Assessment & Management tools for performing the assessment.
- A detailed assessment report should be submitted to the CTO and individual business CTOs every month and an Executive Summary report to the Infosec Steering Committee.
- A third-party independent network assessment shall be carried out annually to provide assurance to the management, customers, shareholders and other parties involved in ADEPTION. The same can be done in order to meet any regulatory requirements.

12. Information Systems Acquisition, Development and Maintenance

12.1. Non-application related Information Systems' Maintenance

Refer: Communications and Operations Management

12.2. Application Development Procedures

The main objective of defining a standard process for application development is to design, develop and maintain high quality and secure software most efficiently and effectively. Every phase in the methodology will form the primary input to the next phase of Development. It is very important to ensure that each phase is complete and correct before moving on the next phase. The development methodology consists of the following phases:

Planning & Feasibility Study

- First and foremost a small team comprising a project manager and one or two team leaders should be formed to kick-start the project once the project is finalized.
- This team should perform the initial planning and feasibility study for the project.
- The team will seek a high-level understanding of the system that needs to be developed. Based on the information collected a comprehensive project plan is prepared which contains the following aspects.
- Key phases of the project and goals to be achieved.
- Target dates for completion and reaching the goals.
- Resources required for completing various phases of the project.
- Documentation required during the course of the project.
- Formation of the entire project team.

System Analysis & Requirements Definition

- The goal for this phase of software development is to analyze the existing system and understand the needs of the Business Process Owner.
- The designated team for requirements gathering should discuss with the Business Process owners and develop a complete, unambiguous, and understandable requirements document. The requirements document should be prepared in such a way that the requirements should be traceable through each following phase of the software development.

- Most critical aspect in this phase is that the team should sit with the Business Process Owner and identify key security requirements. These requirements should be mutually agreed with the Business Process Owners.
- The requirement specification document should contain the following:
    - Functional requirements
    - Security Requirements
    - User Interface Requirements
    - Contractual / Legal / Statutory requirements
    - Performance Requirements
    - Other attributes – Reusability, Maintainability, Portability, extensibility, etc.

Message Authentication / Encryption

- Message authentication should be considered for applications where there is a security requirement to protect the integrity of the message content, e.g. electronic funds transfer, specifications, contracts, proposals etc with high importance or other similar electronic data exchanges.
- Encryption should be considered for transferring confidential information across the network. Type of encryption technology used and strength of the encryption should be identified based on the criticality of the information handled.

Output data validation

- Plausibility checks to test whether the output data is reasonable.
- Reconciliation control counts to ensure processing of all data.
- Providing sufficient information for a reader or subsequent processing system to determine the accuracy, completeness, precision and classification of the information.
- Procedures for responding to output validation tests.

System Design

- A software design is a meaningful engineering representation of some software product that is to be built. A design should be traced to the requirements specification and should be assessed for quality against predefined criteria.
- In the design phase four major areas should be analyzed and designed: data, architecture, interfaces and components. The following four design models are prepared during this phase:
- Data Design – Details about the data structures that will be implemented in the software.

- Architecture & Component Design – Details major structural and procedural elements that are required to meet the requirements of the software.
- Interface Design–Details how the software elements communicate with each other, with other systems.
- Comprehensive design documents containing the above four models should be developed during the phase that will form the basis for development or coding. This document should be reviewed by BISO to ensure that all security requirements are converted into design elements, and nothing is left out.

Development - Coding

- Design documents will form the basis for development of the software for the programmers to code.
- Each procedure / module is developed according to the specifications received by the technical team. This involves designing and coding programs and subprograms and creating tables and data elements.
- Secure coding guidelines specific to the Language / Platform should be given to programmers to help them develop secure codes.
- Following conditions should be avoided while programming.
  - Hard-coding passwords
- The following generic guidelines should be followed in developing programs.
  - All temporary files created by a program should be deleted when the temporary files are no longer needed.

Testing

- Unit Testing
  - The objective of the Unit Test is to ensure that the developed program meets functional and technical design requirements and that all transactions, database updates, and functionality flow accurately. This testing is carried out by the programmer for various scenarios. The testing should ensure that all identified functions and logical paths in the code are covered and considers all normal, unexpected and error Input / output handling conditions.
- Integration Testing
  - Integration test is carried out when the individual modules / components of the entire application are merged and tested together. This is carried out once the unit testing of all components is completed. In this case, the test plans should focus on the testing of interdependency of modules.
  - In this phase, BISO should test whether all the security requirements are built into the programs.

- Acceptance Testing
    - Once the Integration testing is completed, the business process owners or Operations team should test the application to ensure that it meets all their requirements. The following requirements should be tested at this phase:
    - Functional requirements User Interface Requirements
    - Contractual / Legal / Statutory requirements
    - Business process owners or Operations team should sign-off the acceptance if all the requirements are met. If there are any defects, changes should be made to the program to rectify the defects in the program.

Protection of system test data

Test data used should be very much similar to the production data. Access to the test environment should be given only to the personnel involved in testing.

Implementation in the Production Environment

- Once the application is successfully tested it should be ported to the production environment.
- The implementation in the production environment should be performed by a systems administrator or a person authorized by the supervisor.

Development, Test, and Production Environment

- Development, Test environment and Production environment must be physically and logically separated from one another as far as possible.
- Access control environment deployed in the production environment should be deployed in the test environment as well.
- Different log-on procedures should be used for operational and test systems, to reduce the risk of error. Users should be encouraged to use different passwords for these systems, and menus should display appropriate identification messages.

Access control to program source code

The following procedures should be implemented by the Head of applications for protecting the source code from unauthorized access.

- Where possible, program source libraries should not be held in operational systems.
- Operational staff should not have unrestricted access to program source libraries. Only personnel involved in testing and personnel who are involved in migrating to production should have full access which enables them to compile the program.
- Programs still under development or maintenance should not be held in operational program source libraries.

- Program listings should be held in a secure environment.

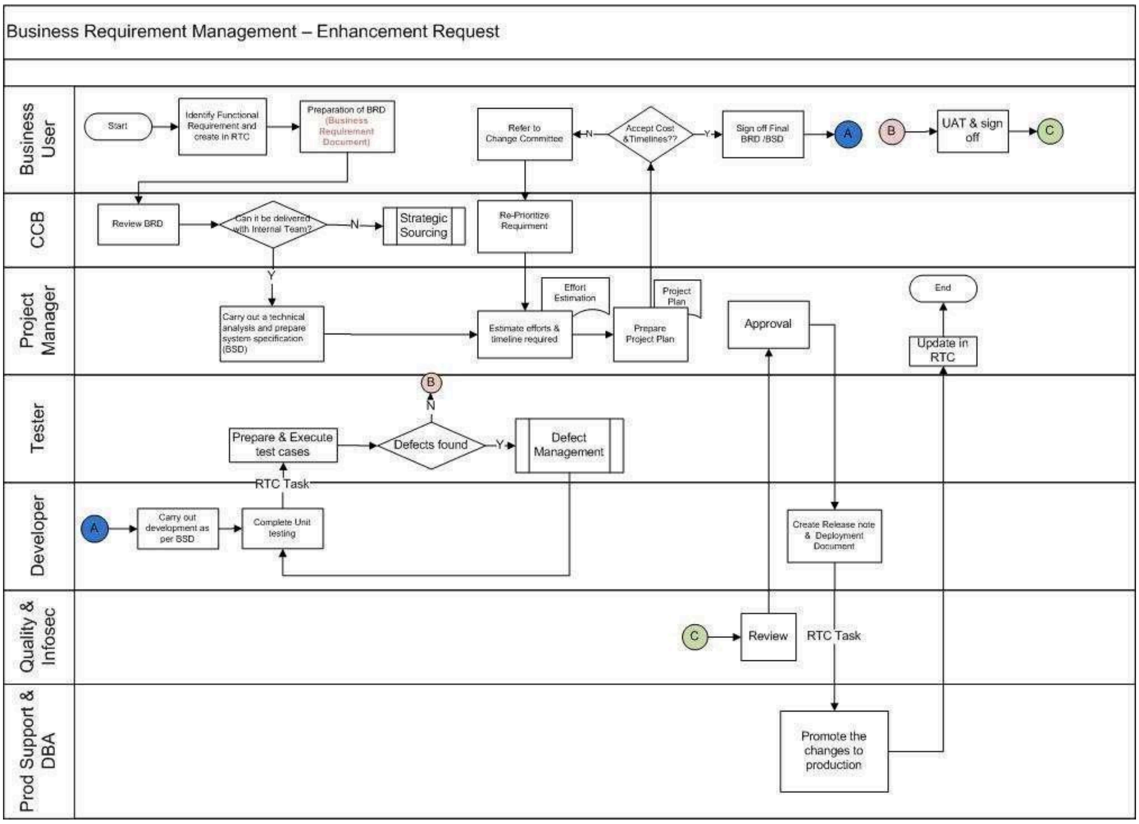
12.3. Configuration Management Procedures

Change control Process consists of well-defined and documented activities that help in managing the changes in software and software projects. It identifies the functional and physical attributes of a software at various points in time and performs systematic control of changes to the identified attributes for the purpose of maintaining software integrity and traceability throughout the software development life cycle and maintenance of operational software. It also defines the need to trace the changes and the ability to verify that the final delivered software has all the planned enhancements that are supposed to be part of the release.

Specific Configuration Management processes must be defined for each application development project and maintenance of each operational software. The project team formed at the start of the project should define and implement the configuration management procedures for each of the projects. Program Change Control Procedures

Emergency Program change control procedures

For all program changes requiring emergency actions and response process, which bypass the suggested policies and procedures above, the following procedures must be adopted:


Business Requirement Management – Enhancement Request
Business User
CCB
Project Manager
Tester
Developer
Quality & Infosec
Prod Support & DBA
Start
Identify Functional Requirement and create in RTC
Preparation of BRD (Business Requirement Document)
Refer to Change Committee
N
Accept Cost &Timelines??
Y
Sign off Final BRD /BSD
A
B
UAT & sign off
C
Review BRD
Can it be delivered with Internal Team?
N
Strategic Sourcing
Re-Prioritize Requirment
Y
Carry out a technical analysis and prepare system specification (BSD)
Effort Estimation
Estimate efforts & timeline required
Project Plan
Prepare Project Plan
Approval
End
Update in RTC
B
N
Prepare & Execute test cases
Defects found
Y
Defect Management
RTC Task
A
Carry out development as per BSD
Complete Unit testing
Create Release note & Deployment Document
C
Review
RTC Task
Promote the changes to production

- Verbal approvals should be obtained by the Operations team from the respective Business Process Owners. This must be immediately followed by an email confirming the same. A verbal approval for the same should be confirmed over the telephone to the Head of Operations.

- Operations personnel, in conjunction with the subject matter experts (In-house/External vendors) must coordinate the process of the emergency program changes with adequate supervision.
- Once the emergency change request has been resolved, the Head-Applications must ensure that all activities performed for the emergency program changes are documented. This documentation would include the names of program files changed, reasons for change, effect on other functionality of the application, tests conducted to verify accuracy of the changes, along with the user sign-off.
- Any sub-normal procedures followed during the emergency program change (e.g. giving super-user or root password to the support personnel performing troubleshooting etc.) should be identified and restored to the original settings and configurations.
- Even in the situation of an emergency, the 'need-to-do' principle shall be followed, with appropriate restrictions on the support personnel executing program changes.
- The testing should be carried out in such a manner so as to ensure the accuracy and integrity of live data and systems.
- The documentation recommended in 'Documenting the Changes' above for normal program change procedures must also be completed after implementing emergency program changes.

Updating of OS Patches

- Operating systems should be updated with latest patches and updates in order to ensure that they are free from vulnerabilities, which can be exploited by un-authorized users to gain access to the system. But OS patches may affect the normal applications running on them.
- BISO with the help of Operations personnel should review the application security controls to verify that they are not compromised.

Restrictions on changes to software packages

Vendor-supplied software packages should be used without modification as far as possible. Where a software package needs to be modified the following points should be considered:

- The risk of built-in controls and integrity processes being compromised.
- Whether the consent of the vendor should be obtained.
- The possibility of obtaining the required changes from the vendor as standard program updates.
- The impact if ADEPTION becomes responsible for the future maintenance of the software because of changes.

In case of changes being necessary the following steps are to be followed:

- Only the latest patches should be applied to packaged software applications.

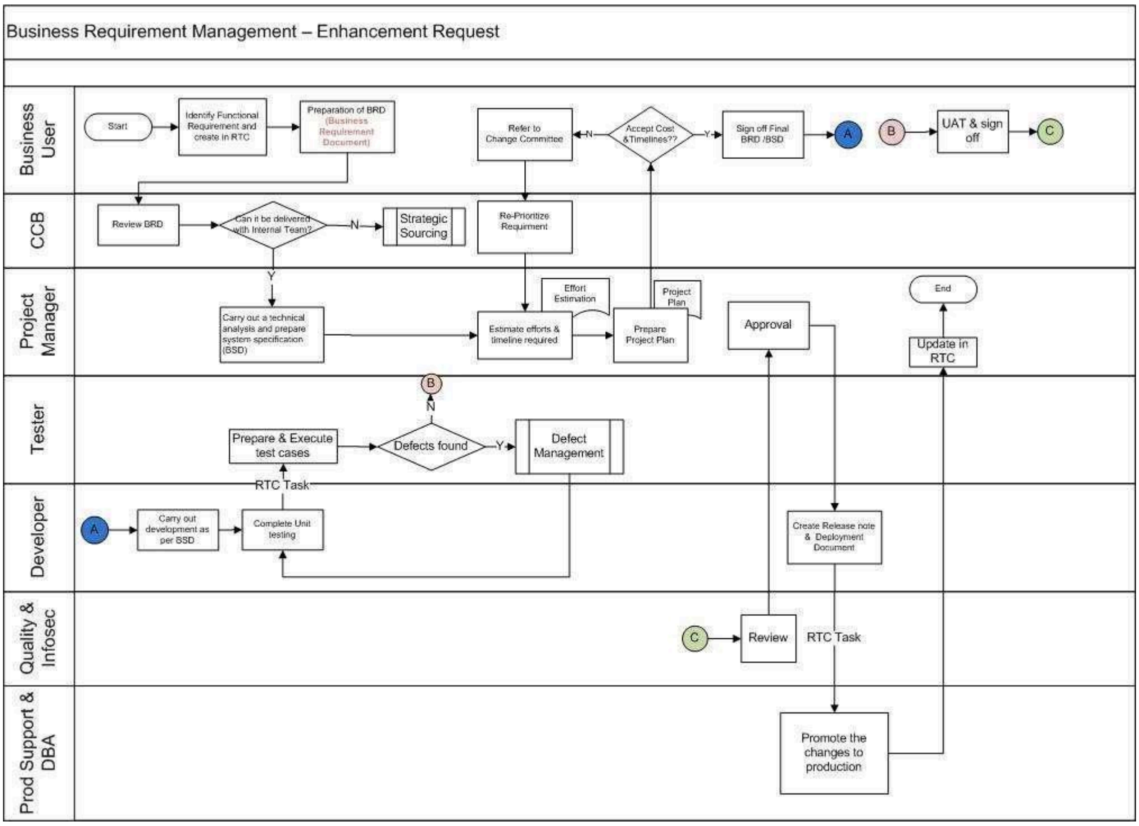
- The patches must first be tested in an isolated test environment before deployment.
- The test results of the same must be reviewed by the application owner and signed off prior to implementation in the production environment.
- A roll back plan should be in place prior to rolling out the production patch / update.
- If possible, the test results should be reviewed and validated by an independent evaluation body.

Outsourced Software Development

Following procedures should be implemented if the application to be used is developed by third-party (External vendor)

- The agreement (Refer: Vendor Management Procedures) signed between ADEPTION and the third party should include the following:
- Application Development Methodology & Program Change Control Procedures in compliance to ADEPTION methodology
- Sharing of Application Code, Design Documents, Test Plans, etc.
- Provision for modification of code by ADEPTION personnel in-case of extreme emergency.
- Agreements on quality and accuracy of the code
- Assurance from a third party that the application development and maintenance procedure are in accordance with agreement between the vendor and ADEPTION.
- Testing of the Applications
    - The application should be thoroughly tested as per Testing Procedures detailed in Application Development Methodology in this document.
    - If the source code is available, the system should be tested for the existence of Trojan code / Covert channel.
    - System should be accepted and implemented in the production environment only after detailed testing (Refer: Systems Planning and Acceptance Procedures).
    - If any changes are required in the application developed by the third-party procedures detailed in Program change Control in this document should be followed.

Application development (Process Chart)


Business Requirement Management – Enhancement Request
Business User
CCB
Project Manager
Tester
Developer
Quality & Infosec
Prod Support & DBA
Start
Identify Functional Requirement and create in RTC
Preparation of BRD (Business Requirement Document)
Refer to Change Committee
N
Accept Cost &Timelines??
Y
Sign off Final BRD /BSD
A
B
UAT & sign off
C
Review BRD
Can it be delivered with Internal Team?
N
Strategic Sourcing
Re-Prioritize Requirment
Y
Carry out a technical analysis and prepare system specification (BSD)
Effort Estimation
Estimate efforts & timeline required
Project Plan
Prepare Project Plan
Approval
End
Update in RTC
B
N
Prepare & Execute test cases
Defects found
Y
Defect Management
RTC Task
A
Carry out development as per BSD
Complete Unit testing
Create Release note & Deployment Document
C
Review
RTC Task
Promote the changes to production

13. Cryptographic Systems

13.1. Cryptographic Procedures

Business Policy

Business policies, as applied to cryptographic services, define the requirements for when and in some cases, where cryptography must be applied within the corporate infrastructure. ADEPTION business policies for cryptographic services are as follows:

- Unless each occurrence is specifically authorized by the departmental head or CTO, readable secret information must not be sent by electronic mail. If encrypted with a ADEPTION approved method, and if encrypted at the source and decrypted only at the destination, then secret information shall be sent over an electronic mail system.
- The IT department must ensure that all portables, laptops, notebooks, and other transportable computers containing sensitive ADEPTION information must consistently employ both hard disk encryption, for all files, and boot protection.
- ADEPTION personnel in the possession of portable, laptop, notebook, palmtop, and other transportable computers containing sensitive ADEPTION information must not leave these computers unattended at any time unless the sensitive information has been encrypted.
- IT administration must ensure that passwords must always be encrypted when held in storage for any significant period of time or when transmitted over networks. This will prevent them from being disclosed to unauthorized parties.
- If passwords or Personal Identification Numbers (PINs) are generated by a computer system, all software and files containing formulas, algorithms, and other specifics of the process must be controlled with the most stringent security measures supported by the involved computer system.
- Encryption software is necessary to transfer ‘confidential’ information over the third party network or public networks.
- CISO should identify the right encryption software after careful evaluation. CTO shall authorize the procurement of encryption software after evaluation is done by the CISO. Owner of the Encryption Software is CISO.
- Access to Encryption software is linked to the person who handles confidential information. The software should be given access to all personnel who handle confidential information. The user should fill ‘Request for use of Encryption Software form’. The request should be approved by CTO/ CTO and authorized by BISO.
- BISO shall maintain list of users who have Encryption software.

Technical Policy

Technical policies, as applied to cryptographic services, define the requirements for baseline implementation, technical criteria, or in some instances, corporate procedures for how cryptography must be applied. ADEPTION technical policies for cryptographic services are as follows:

- Flow Control Systems: To prevent intruders from interfering with Internet commerce activities, all Internet commerce servers (web servers, database servers, payment servers, security servers, etc.) must employ unique digital certificates and must use encryption to transfer information in and out of these servers. An exception is made for web servers, FTP servers, and any other ADEPTION servers supporting communications with customers, prospects, or other members of the public.
- Design of Password: Whenever user-chosen passwords or encryption keys are first specified, they must be entered twice and masked so that onlookers cannot see what was typed. Both of these entries must match in order to be accepted by the system. This requirement will prevent typing mistakes from locking users out of the system or preventing access to important information.
- Symmetric and Asymmetric Encryption: ADEPTION will support the symmetric key encryption algorithms. In addition, ADEPTION will support the asymmetric key encryption algorithms. In the case of asymmetric keys, digital certificates must be used to bind an entity to a public key. Moreover, such digital certificates must use the X.509v3 standard format.

Key Management

Key management deals with ADEPTION policies surrounding the lifecycle of cryptographic keys. The following requirements apply:

- Key Generation: All symmetric cryptographic keys must be randomly generated according to industry standards.
- Symmetric Key Lifetime: When symmetric encryption is used, policies will be applied depending on the where and how the data is being processed. The primary difference is data-in-transit versus data-at-rest. Also, while data is at rest (i.e., contained within a storage media) it is considered to be either active or in-active.
- Data-in-Transit:
  - 128 bit encryption must be used as a minimum standard
  - In case of dynamic keys, Master keys must be changed at least once a year.
  - Key-encrypting keys must be changed at a minimum of once a month and
  - Data encrypting keys must be changed per session or once every twenty-four hours.
- Data-at-Rest:

    - Active Data – data that is readily available from a local storage media device such as a hard drive, static RAM card, or other computer accessible media device.
    - Master keys must be changed at least a year.
    - Key-encrypting keys must be changed at least once every six months unless the key-encrypting key is also a master key (e.g., Kerberos KDC Master Key) and
    - Data encrypting keys must be changed at least once a year.
- In-Active Data – Data that is archived for extended periods of time and is not readily available for immediate processing by computing devices.
    - In case of dynamic keys, master keys must be changed at least once every two years.
    - Key-encrypting keys must be changed at least once a year unless the key-encrypting key is also a master key (e.g., Kerberos KDC Master Key) and
    - Data encrypting keys must be changed at least once a year.

Asymmetric Key Lifetime

In cases where asymmetric encryption is used, the lifetime of asymmetric keys associated with a public key certificate are dictated by the Certificate Policy document of the issuing authority.

- Key Storage: Cryptographic keys must be stored within an encrypted key store or in some type of encrypted form using approved algorithms otherwise the keys must be stored on a security token such as a smart card. If the key is stored on a smart card or other token device, the cryptographic keys must never leave the token.
- Key Archival and Retention: The key associated with data that is archived, must itself be archived. Archives of encryption keys must not be archived with the data that is being protected by those keys.
- Key Destruction: Cryptographic keys must be deleted or destroyed if the keys are:
    - No longer in use or
    - Have been compromised and
    - Not a part of a key retention program.

13.2. Key Ownership and Distribution

Encryption keys are confidential information, and access must be strictly limited to those who have a need-to-know. The owner(s) of data protected by cryptographic services must explicitly sign responsibility for the encryption key management to be used to protect this data. If cryptographic keys are transmitted over communications lines, they must be sent in encrypted form. The encryption of keys must be performed with a stronger algorithm than used to encrypt other confidential data protected by the keys being transmitted.

- Key Compromise: Cryptographic keys that are compromised must be reported immediately to BISO or CISO and the information owner of the data being protected. Furthermore, the key must be changed and/or destroyed, according to the Key Destruction procedure outlined under 'Asymmetric Key Lifetime' in the earlier section, and a new key must be generated. The data protected by the comprised key must be re-encrypted with the new key as soon as the new key is available.

14. Incident Management

The purpose of this incident-handling procedure is to provide guidance to restore normal IT operations quickly and efficiently following an incident at ADEPTION.

14.1. Definitions

Security/Operational incident

A "Security/Operational incident" is an adverse event where:

- The IT resource is attacked or threatened with an attack.
- Accessed/monitored/modified without authorization and
- Used in a manner inconsistent with the established organization's/regulatory policy resulting in a real or possible loss of confidentiality, integrity or availability of the IT resource or information.

Examples of Security incidents are:

- internal or external attempts (either failed or successful) to gain unauthorized access to the IT system or its data.
- denial of service (DoS) or unauthorized disruption to IT system and infrastructure
- actual or suspected loss of proprietary, confidential or entrusted information of the organization
- changes to system hardware, firmware or software characteristics without the department head knowledge, instruction or consent
- malicious code (virus, trojan horse) attacks
- social engineering (tricking someone to disclose confidential/proprietary information like passwords that could compromise system security)
- signature update failure and
- hoaxes (deliberate trickery intended to gain an advantage e.g. false virus warnings may lead some users to ignore all virus warning messages, leaving them vulnerable to a genuine, destructive virus).

Examples of Operational incidents are:

- Firewall hardware failure.
- anti-virus appliance hardware failure and
- IDS hardware failure.

Problem/event:

An event is an observed or observable occurrence in a system, a network or daily operations.

An event will be termed as an incident if it is considered to have "adverse" impact on the IT system/infrastructure or through pre-positioned criteria that describes the circumstances under which events will automatically be deemed adverse.

An event will be an incident when it is analyzed and classified to be adverse by the incident response team.

Until events are classified as adverse, they are considered as "suspected incidents".

Incident Response Team (IRT / IR Team)

The Incident Response Team (IRT) is formed to address any incidents and initiate immediate action to resolve the same. The Incident Response Team issues guidelines proactively to address potential threats/ risks arising out of incidents. While incidents should be handled at various levels based on the severity and impact of the incidents however most incidents are to be handled at the Incident Team leader level.

The team shall consist of the following members:

Incident Management Leader (IML):

The CEO is the IML and should be responsible for overall management of the incidents. The IML is responsible for taking critical decisions regarding business operations/process changes during/after an incident.

The IML or a person designated by him only can deal with the media in case of any incidents.

Incident Management Coordinator (IMC):

The CISO and CTO together play the role of IMC at ADEPTION. IMC is responsible for coordinating with the BISO and CTOs of individual business and other departmental heads to manage and resolve the incident. The IMC should work with the Incident Response Team Leader to contain the damage caused by the incident and should be the focal point for recovery efforts.

Incident Response Team Leader (IRTL):

CTO & BISO shall be the Team Leaders for all IT related incidents. They shall be part of any IR team. Head of Admin shall be the Team Leader for Non-IT related incidents. The BISO should be the 'one point contact' for all the users for all incidents. He must try and obtain as much information as possible from the person reporting the incident. BISO is responsible for evaluating the incident and appropriately initiating the escalation process. BISO and CTO shall delegate action on incidents to Information Security Coordination Team.

Incident Response Team Members:

The members of the Information Security Coordination Team (ISCT) are the team members for Incident Response. They should get a detailed briefing from BISO before acting on any incident. They should also meet the person reporting the incident for obtaining further information.

CISO and IR Team members must have the list of all emergency contact details of the entire Incident Response Team, Vendors, Suppliers, Service providers, etc. An emergency pocket sized card can be prepared containing contact numbers of the Incident Response Team members and distributed to all the employees.

Help Desk Team:

It is the responsibility of helpdesk team to:

- Answer, evaluate, and prioritize the incoming telephone, e-mail, and in-person requests for assistance from users experiencing problems with hardware, software, networking, security and other computer-related technologies.
- Escalate problems to help desk support engineers.
- Escalate any security incident/problem to the IT and system security departments promptly.
- Call software and hardware vendors to request service regarding defective products and
- Log and track calls using remedy problem management database and maintain the history of records / problem related documentation.

14.2. Problem/Incident handling process

In order to differentiate between incidents (security/operational) / problems that can occur in ADEPTION, the following process has been developed. The process provides details on how incidents/problems can be handled during the normal course of the organization's operation. The IT department should develop detailed procedures to handle day-to-day problems.

14.3. Incident Handling Procedure

Refer: Computer Security Incident Response Team framework document

Problem/event reporting

- Problems occurring in the organization should be reported by the users directly to the help desk personnel as per the ADEPTION problem management process.
- The CISO should ensure that one or more of the following measures are implemented to identify events that could result in an incident:
  - Logging and monitoring enabled on all critical infrastructure information systems
  - Detective controls such as File Integrity Monitors, MD5 hash implemented on critical files and systems

- Problem/event identified by IT/security department should be reported to the respective IR member based on the type of the problem. The table – number provides a template for personnel responsible to IT and security management. In any case, the IRT member who first knows about this event should inform and involve other IRT members based on the event/incident type as appropriate.
- The security assessments can highlight potential weaknesses in the system proactively and should be reported to IRT Head.
- All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in system or services to IRT Head.
- The IRT members, who are involved in resolving the event/incident can be minimum, based on the incident type. The following are the examples of incidents, and to resolve these incidents, the following IRT member(s) (at a minimum) should be available.
    - Antivirus and Firewall security incidents – antivirus administrator and BISO
    - Web server security incidents – Application administrator, Database administrator, Firewall administrator and BISO
    - Operational problems – Product administrator and
    - Network operational problems – Network engineer.
    - Security weaknesses – IRT Head.

14.4. Problem/event review and analysis

The problem should be reviewed by the helpdesk to distinguish it as an operational day-to-day problem or a security event.

Example problems are:

- desktop hardware issues
- printer hardware issues
- e-mail client configuration issues and
- internet browsing issues.

If it is an incident, then it should be escalated to the IRT team for further review.

14.5. Incident Classification and Escalation

The BISO should classify the incident based on the matrix given below. BISO should assign the classification based on the information collected from the person reporting the incident. Based on the Severity and Impact BISO shall form the Incident Response Team. The escalation chart with contact details should be pasted on the notice board or the desks of each employee.

Incidents are classified based on:

- Possible Business Impact
- Maximum tolerable downtime

Incident Classification				
Impact severity level	Impact zone	Preferred resolution target	Escalation	Examples
Devastating Impact (Level 3)	Entire Facility affected	4 hours	CEO	Immediate & long-term threat to Data Centre, Server room, Site and/or multiple processes for prolonged time Downtime of entire bureau application or database resulting in delay in delivery of reports Unauthorized disclosure of highly confidential information. Severe Power outage, Fire.
High Impact (Level 2)	One or few Operations affected	6 hours	CTO/ CISO	Virus threat, Partial disruption of activities (affecting up to 30% of operations), Unauthorized disclosure of confidential information.
Immediate & Moderate Impact (Level 1)	Operations partially affected	8 hours	BISO/ CTO	Some part of the application not working, issues with Batch processing, Internal applications not functioning, office communication failure, etc
Low or No Impact (Level 0)	Local– Does not affect business operations	24 Hours	BISO/ CTO	Tailgating, Unclaimed Access cards, Scheduled maintenance tasks, etc.

Expected Reporting/ Response Time – Immediate

Escalation: The escalation hierarchy is as follows:

- Level 1 – IR BISO/ CTO
- Level 2 – IM CISO/CTO
- Level 3 – IM CEO
- Members at appropriate levels shall escalate incidents.

14.6. Incident investigation

- The security event should be reviewed by BISO and CISO in order to decide whether it is an incident or event.
- The incident should be analyzed and impact over the business should be identified, if possible.
- The cause of the incident should be identified to further distinguish it as a **security incident or operational incident**, if possible.
- The incident should be escalated to senior management such as CTO, CISO and IT support & networking manager.
- The CTO, IT support and networking manager and CISO should classify the incident type as “Operational” or “Security” and incident severity as “HIGH”, “MEDIUM” or “LOW”. The incident can be classified to its severity based on its business impact to the organization’s services.
- At a minimum, following criterias may be used to identify the incident **as an operational incident**:
    - hardware problem over security and network devices
    - inappropriate configuration by the IT and security team
- The operational incident should be prioritized as **high/medium/low**. The following are the examples of operational incidents:
- Operational incident – High
    - firewall failure due to hardware problem
    - server hardware failure and
    - production database failure.
- Operational incident – Medium
    - IDS/IPS/ Content filtering appliance hardware failure
    - e-mail relay agent hardware failure
    - internet link failure
    - production application server failure
    - production application database failure

    - external zone and DMZ switch hardware failure and
    - internal e-mail server hardware failure.
- Operational incident – Low
    - One clustered server failure
    - application zone switch/router hardware failure.
- The security incident should be prioritized as **high/medium/low**.
- The following are the examples of security incidents:
- Security incident – High
    - external internet router failure due to successful hacking attempt from the internet
    - both external firewall failure due to successful hacking attempt from the internet
    - web server deface
    - application server compromise due to successful hacking attempt
    - e-mail relay agent failure due to successful hacking attempt
    - virus or worm detection(unconfined)
    - unauthorized changes to the configuration of network and security devices
    - unauthorized account in the security and network devices and
    - confirmed security violations by user or external contractor.
- Security incident – Medium
    - repeated active probes or port mapping from internet
    - attempted web page attacks or defacements launched from internet
    - unauthorized modification of the webpage's on the web server
    - application server hacking attempt
    - virus or e-mail spam issues with multiple users
    - unauthorized installation of instant messengers for chatting over the internet
    - attempt to gain unauthorized access to the resources, either from within or outside the organization's network

    - unauthorized modification of production application system without prior approval and
    - unauthorized installation of software.
- Security incident – Low
    - non-repeated scans or pings from internet over web server and e-mail relay agent
    - virus or e-mail spam issues for less than 10 users
    - account lockout due to incorrect password trials
    - unprotected system console and
    - missing anti-virus software

14.7. Incident response and resolution

- The appropriate solution should be implemented based on the type and impact of the security incidents.
- The cost of information security incidents should be quantified and monitored before implementation.
- Denial of service attacks:
    - identify the source IP address of the attack on the external firewall and implement the access control rule to block that source IP address at external firewall, external perimeter router
    - escalate the incident to the ISP to block the source IP address and
    - configure the external IDS to perform "TCP reset" and "firewall reconfiguration" over the source IP address of the attack.
- The BISO should maintain a database of all incidents encountered within the business. (Refer: Incident Register)

Viruses and worm

- disconnect the system from the network which is infected with the virus.
- update the anti-virus signature on the system and scan the machine at both operating system level and boot level (if possible)
- verify the vendor site for any tool which will scan the system for the presence of viruses or worms on the system.
- in the event of "worm" which may spread through specific "port", identify the port from the vendor site and block it at all the firewalls ensure the anti-virus has up-to-date anti-virus signature file and

- alert all the users in the organization by sending an e-mail stating not to open any e-mails from unknown sources or particular type of e-mail with specific “subject”, “attachment” or “content”.

Server/System deface

- disconnect system from the network.
- collect log files on the web server to trace the source of this attempt and also verify log files on the external IDS/IPS and external firewall.
- perform host-based vulnerability assessment over the web server to identify any latest vulnerabilities on the system.
- verify the file permissions on the production application server and perform host-based vulnerability assessment over the system.
- verify all the file permissions and user permission on the system.
- perform penetration testing over the system by restricting it to specific source on the internet and
- reconnect the system back to the production network for internet users.

Additional Resolution Measures

- In the event of an incident that cannot be resolved an appropriate alternative solution should be implemented where possible and follow a review process to obtain approval from the Infosec Steering Committee.
- Should incident response require changes to security and network devices configurations, changes should be made in accordance with the change management and configuration management process recommended separately.
- The vendors should be called for any support over the incidents, which cannot be resolved by the ADEPTION’s team.
- The incident should be resolved, and the IT infrastructure should be brought to normal working operations.

14.8. Incident documentation

- The incident should be documented to clearly identify whether it is a security incident or operational incident. The incident handling form provided in the appendix should be used for the documentation.
- For operational incidents, the incident handling form will be maintained by the IT team.
- For security incidents, the incident handling form will be maintained by the BISOs
- The incident severity should be documented.
- The person who reported the incident and the personnel involved in resolving the incident should be documented.

- The incident description and the solution implemented should be clearly documented. This will facilitate the IR team in applying the same solution if the incident occurs again in the future.
- The time required to identify and to resolve an incident should be documented.
- The incidents as per the incident management policy should be reported to the senior management through Infosec Steering Committee meetings.
- The incident database can be used as a guide to resolve similar and specific incident occurrences.
- The incident documentation should be supported with evidence in a method which can be presented to conform to the rules for evidence laid down in the relevant jurisdictions.

15. Compliance

15.1. Compliance with Legal requirements

Identification of applicable legislation

- Advice and approval on the statutory, regulatory and contractual requirements of ADEPTION Corporate Office should be sought from the legal department. The BISO should document the requirements in a register with the corresponding controls associated with each regulatory and legal requirement.
- The legal department should instruct the employees on the legal requirements and the compliance to such legal requirements.
- The legal department should also ensure that the controls are implemented immediately to ensure compliance.
- Regular review to the compliance should be carried out by the legal department in conjunction with the Central Security Team.

15.2. Safeguarding of Organizational Records

Refer: Physical Security and Asset Management Policy and Procedures

Prevention of misuse of Information Processing facilities

Refer: Human Resources Security

15.3. Independent Reviews of security policy and technical compliance

Compliance with Security policies and standards

Compliance to the following policies and procedures should be regularly checked:

- Asset Management
- Human Resources Security
- Communications and Operations Management
- Systems Planning and Acceptance
- Backup and Recovery
- Vendor Management
- Access Control
- Network Security
- Information Systems Acquisition, Development and Maintenance
- Cryptographic Systems
- Incident Management
- Business Continuity Management

- Compliance

Technical Compliance Checking

The systems used should be regularly monitored by the operations personnel in order to check compliance with the defined standards. A check should be performed bi-annually to ensure that users are only performing processes that have been explicitly authorized.

One annual technical review should be carried out by a competent third party.

Areas that should be checked for compliance are:

- Access restrictions
- Review of logon patterns for indications of abnormal use or revived user Ids
- Allocation and use of accounts with a privileged access capability
- Tracking of selected transactions
- The use of sensitive resources
- Firewall activity

The findings of the compliance check should then be reported to the BISO.

15.4. Information systems Audit

Preparing Audit plan and conducting Audits

- In the event of any change in the Audit Plan, the Audit team shall prepare a revised audit plan and communicate the same to the Infosec Steering Committee.
- For technical testing of Information systems, prior approval of the Asset Owner and the BISO should be obtained. Adequate precautions shall be taken before the execution of technical testing. The testing tools shall be under the custody of the BISO and shall be physically and logically protected.
- The execution of audits may be outsourced to capable independent third parties or by an Internal Audit function of ADEPTION.
- The CISO and the BISO shall provide the Auditors with information regarding the areas of focus and the Audit Report Formats.

Audit Reports, Findings and Non-conformance closures

- The Auditors shall carry out the audit and record the non-conformances and their observations/ suggestions on the Audit Report.
- The BISO should collect the Audit Reports and review them.
- He/she should also prepare a non-conformance summary report.

- The non-conformance report prepared by the BISO should be reviewed by the CISO.
- The respective departments or functions such as operations, IT shall initiate corrective and preventive action on the non-conformances and close them within the committed closure time.
- At the end of the committed time frame, the BISO shall appoint an Auditor to verify the closure of the non-conformance or do it himself/ herself.
- The assessor shall report back the findings to the Audit Team, who then updates the non-conformance summary report.

Changes in Audit plans and Infosec Steering Committee review

- In the event of non-conformance not being closed within the committed time frame, the time taken to close it should be highlighted to the management during the Infosec Steering Committee meetings.
- The audit process and the results shall be discussed in the Infosec Steering Committee Meeting.
- The CISO and BISO shall carry out necessary changes to the audit plan based on the change in the organization and also may initiate Corrective and/or Preventive actions as may be finalized in the Infosec Steering Committee meetings.

15.5. Technical Vulnerability Assessment

- A list of assets detailing the critical assets of ADEPTION should be maintained. This list would be subjected to various vulnerability assessments.
- Internal technical vulnerability assessment of all the critical assets of ADEPTION must be carried out on yearly basis.
- An external agency / organization must be employed to conduct external vulnerability tests for ADEPTION and the critical asset list annually.
- On identification of vulnerabilities they should be reported to the CTO and prioritized on the basis of impact on business.
- BISO should overlook the closing of gaps starting with top priority. A timeline should be defined for closure of each of the vulnerabilities identified.
- In case of the remediation being infeasible the risks should be minimized and the residual risk should be documented and presented to the infosec steering committee.

16. Data Confidentiality

16.1. Data Confidentiality Policy

- Any data which contains customer-related data is considered confidential. Access and distribution is restricted.
- Name, telephone number, address, permanent address of the customer, details of nominees.
- Credit Card, Bank or Payment details.
- Date of birth details
- Usage behavior - Telephone usage behavior, Electricity usage, Investment or Credit Card usage behavior
- Data pertaining to network architecture and design is also considered sensitive.
- Internal strategy documents and
- Business product specific information
- Employee related data- payroll, provident fund, professional fund etc.
- Legal documents
- Information security risk reports, pen test reports etc.
- Audit logs/reports.

16.2. Data - Business applications

Data which is accessed or stored on a business-related application should be owned by the business user/department. Cases where data is shared with multiple departments & ambiguity exists on ownership should be highlighted to CEO of the company to decide. The business head should decide on classification of data as per the Classification procedure detailed in Asset Management policy.

16.3. Data – IT applications

If the IT applications are created or developed for business requirements, the ownership still remains with Business. If the data relates to IT infrastructure or networks the owner is the CTO of the company who needs to classify the data as per the Classification procedure detailed in Asset Management policy.

16.4. Access to data through Applications / Physical records

Data from Applications

- Users having access to application related data (especially ones having customer details) should NOT cut, copy or download them to their PC's/Laptops/Other devices unless a written authorization is taken from the 'Information Asset Owner'

MIS reports

- Some users have access to confidential data (as defined in scope above) from applications/databases by virtue of their job profiles to generate MIS. These users should ensure that once the MIS is created & sent to relevant departments, they should DELETE the data immediately from their machines. This data should be secured with "rights to use" ensuring only authorized users can access the documents.

Recipients of MIS reports

- Once a user (Information asset user) receives the reports and appropriate action is taken on them, the user should delete the report from his desktop/laptop immediately. Reports to be preserved for less than 7 days fall under the scope. Reports to be preserved for more than 7 days can be stored on central file servers and secured with 'Document rights management'. After deleting, if a report is required, a request may be sent to the MIS team again.
- Sharing of MIS or any kind of reports containing confidential (customer / company related) data on emails, USB or CD's is strictly prohibited. Any exceptions must be highlighted to the BISO's and signed off.

Data sent to Third parties for processing

- Sensitive customer related information sent to third party vendors for processing should always be sent in encrypted format and NEVER in clear text.
- Data should NOT be shared on CD's, USB memory sticks OR Emails with third party vendors unless the Information Security team has reviewed and signed off. Data should also be secured with "usage rights" using Document Rights Management solutions.

Physical Records

- Physical records which contain sensitive information should be securely stored & an owner identified for the same.
- If these records are used by vendors, the information asset owner should ensure the same level of security is implemented at the vendor site. Some measures include using numbered copies so leakage can be traced.
- User Identification data like Application user ID's and Passwords should never be sent together.
- Information (Application IDs/Passwords, statements, MIS reports etc.) 'returned' through couriers should be shredded or stored securely if they have to be re-used.
- Duplication of the documents by photocopying, printing, etc. should be restricted. Unless approved by the Asset owner, they should not be duplicated.

The information owner should periodically review the list of users (at least monthly) who have access & rights on his data to ensure only authorized personnel are provided access.

No data should be stored on public mailing sites as backup OR for sharing between employees/outside entities.

16.5. IT teams / Administrators access to data

As custodians of data, you play an even more important role in ensuring data security. No customer or network related data should reside on your desktops/laptops without appropriate encryption & document rights assigned on them for use.

- Please keep a single BUT very strong password (review the password policy for guidance) for all your critical /sensitive documents – this will ease the handover process when you need to relinquish your devices back to the company.
- When data is being shared with others (within or outside the company) appropriate security (encryption & document rights to use) has to be implemented on the files. Remove all traces of customer information from these files.
- Do NOT keep any customer related data on Development/Test/UAT servers for testing. If required, completely sanitize the data.
- Developers and test personnel should NEVER be provided access to production servers. Only production support teams should have access to these servers.
- When data needs to be shared with third party vendors for troubleshooting, sanitize the data (remove all customer references or mask them), encrypt & assign document use rights.
- Restrict the access of the third party vendors and unauthorized personnel (Branch) to the file server where shared data is stored.
- Unauthorized software like IP messenger / Yahoo messengers for data transfer should be avoided.
- Encrypt databases if feasible, take exception sign offs from the Information security team where not possible.
- Network designs and infrastructure related documents should be stored securely on desktops/laptops to prevent unauthorized access either directly from the machine or over the network.
- User ID and Password should not be shared. Specific user IDs and passwords should be created for each individual.
- If database admin's generate ad-hoc reports they should ensure the documents are secured with Document Rights Management before sending to recipients and deleted from their desktop/laptop immediately.
- All exceptions should be reviewed by the BISO's and signed off.

16.6. Recommended corporate solutions

Internal transfers – Use the 'shared folder' solution to provide restricted access & share data with internal ADEPTION colleagues.

External transfers (vendors, consultants, any third parties)

- Secure file transfer (SFT) portal – Use the SFT portal to share data with third parties.
- Data copied on USB/CD’s – Use Content Encryption software to encrypt data being moved on these devices.
- Data on Laptops / critical desktops – User ‘Disk Encryption’ software to encrypt data on these devices.

Documents (Word, Excel, PowerPoint etc.) containing customer data –use Document Rights Management (DRM)OR Password protect the same (ONLY if DRM is not feasible)

16.7. Monitoring and Auditing

The Information Security team should conduct periodic audits and highlight violations to management.

Management should take action as per “Violation of Infosec policy.”

16.8. Risk Assessment

All applications having data as defined in scope should be assessed for risk by the Business Information Security officers.

All risks identified should be brought to the notice of Working committee for resolution Risks which are to be signed off should be highlighted to the Steering Committee

The BISO’s should review these signed-off risks at least once a year and identify if appropriate solutions are available.

17. Extranet Policy

17.1. ADEPTION Extranet connectivity

This is applicable when other business entities require to connect to our network or vendors with whom we have maintenance agreements.

- A change request form requesting for connectivity should be submitted by the requesting department to the Information Security team with proper departmental approvals.
- There should be a written, signed & sealed contract / MOU / NDA with the connecting organization, unless exempted and approved by Head ISG.
- The vendor connecting for maintenance should disclose all their findings within a reasonable time. This must be included as a clause in the MOU if applicable.
- Before entering into any such agreement, the Head – ADEPTION Network, Business head (requiring connectivity) & ADEPTION Head-Information Security must be informed and a written approval be taken. This will ensure that the highest authority is well informed about the remote login being allowed for an outside entity. The agreement should lie with the business team requesting for the connectivity.
- For connectivity, a security risk assessment has to be conducted & all risks closed or signed off before the agreement is entered into.

17.2. Point Of Contact

- The requesting department must designate a person to be the Point of Contact (POC) for the Extranet connection. The POC acts on behalf of the requesting department and is responsible for those portions of this policy and the Third-Party Agreement that pertain to it. In the event that the POC changes, the relevant extranet organization must be informed promptly.

17.3. List of third party network connections

- The Network Administrator must maintain a list of third-party network connections having access to ADEPTION's network. Privileges and activities of these connection users must be monitored closely.

17.4. Use of firewall

- Any third-party connection to ADEPTION's LAN or WAN for Intranet / Extranet connections (e.g., Customers and Suppliers) must be through a firewall.

17.5. Modifying or Terminating connectivity and access

All changes in access must be accompanied by a valid business justification and are subject to security review. They should go through the change management process. The requesting department is responsible for notifying the Network management group when there is a material change in their originally provided information so that security and connectivity evolve accordingly.

17.6. Terminating Access

- When access is no longer required, the requesting department within ADEPTION must notify the network team responsible for that connectivity, which will then terminate the access. This may mean a modification of existing permissions up to terminating the circuit, as appropriate.

17.7. Adherence

- The Information Security group would conduct audits of these connections as per ADEPTION audit policy.

The third party should be provided a ADEPTION security policy handbook for their review of our expectations.

17.8. Extranet connectivity (Temporary requirement)

The requirement should be raised to the Network team with proper departmental approvals. Network team will review the requirement and after getting the relevant department head approval forward the same to Head-ISG for security assessment & approval.

Minimum rights to be granted

- Temporary User ID and password must be granted with minimum rights that are required to perform the job.
- Disabling of User ID
- On completion of the maintenance activity or at the end of the day whichever is earlier, the temporary User ID must be disabled by the application owner.

17.9. Access to Production systems

Vendor access to production systems should be limited only for troubleshooting and bug fixes over VPN. The access should be monitored at all times.

Extranet Connectivity (When we need to connect for accessing resources)

The requirement should be raised to the Network team with proper departmental approvals. Network team will review the requirement and after getting the relevant department head approvals forward the same to Head-ISG for security assessment & approval.

17.10. Administrative Settings

The connecting organization user id must be a general user id without any root privileges.

"ftp" facility MUST be Disabled for that connecting organization User ID. The login process MUST ensure that ftp is disabled (that login ID must be entered in ftp users). If otherwise, then the login should fail.

If possible, unmount other partitions, which the connecting organization does not require for checking.

17.11. Closing The Connection

Passwords must be changed before disabling the UID after the connection is over.

Delete the rule based on Firewall/VPN after the connecting organization has completed the activity.

18. Internet Service Management

18.1. Purpose of Internet use

The Internet is to be used only when necessary for the execution of a user's job responsibilities.

Information transferred through the Internet from ADEPTION IP address must be treated with the same standards and due care as information on ADEPTION company's letterhead.

18.2. Internet Security Administration

Virus Scanning of Downloaded Internet Information

- All information downloaded e.g., Email retrieval, data / FTP downloads, Active x controls, Java, Java Applets, images etc., to ADEPTION computing resources via the Internet must be screened with updated virus detection software prior to use.

Internet servers

- All necessary vendor security patches or upgrades must be installed on Internet servers.
- Potentially dangerous system software like compilers or debuggers must not reside on the Internet servers.
- Only necessary accounts must remain active on Internet servers, e.g., system and administrator accounts.
- Root and superuser accounts must not be used to connect to servers. Use a less privileged account then su or change to the administrative user once connected, to enable an audit trail to indicate better who did what as super user.
- If the servers are given complete Internet access, any kind of browsing/messenger use should be prohibited. Administrators should keep close monitoring for the same.
- The servers should be completely hardened as per ADEPTION hardening guidelines and pen tested before exposure to the Internet.

Telnet Services

- Both Inbound / Outbound Telnet services with Internet must not be allowed, unless approved by Head-ISG & CTO. When approved, SSH should be used to login remotely to a host in Intranet. SSH should not be allowed to be used over the Internet, rather only approved connections via VPN are to be given post approval from BISO.

Trivial File Transfer Protocol (TFTP)

- The use of TFTP is prohibited.

Internet Mail

- All Internet mail must be provided through an approved ADEPTION mail server.
- All mail services must be provided through the firewall and secure SMTP gateway.
- SMTP traffic must be handled by a dedicated SMTP server (e.g., SMAP / SMAPD), and not allowed to pass through the firewall to an internal mail server. Malicious SMTP traffic (e.g., pipe symbols) should be rejected and logged.
- Internal host name and addresses should be hidden from mail headers. For outgoing mail messages outbound email headers must be selectively rewritten so that all email appears as if it originated from the firewall or external SMTP relay.
- SMTP message size must be appropriately restricted to the capabilities of the mail servers.

Internet Relay Chat Services

- Internet Relay Chat Services are prohibited.

18.3. Firewall Monitoring

Monitoring tools must be in place to alert system administrators about security or other related events generated from the firewall.

The system logs generated from the firewall must be reviewed periodically to detect any unauthorized entry attempts or unusual behavior.

18.4. Firewall Maintenance

The firewall must fail in a "closed" state, to secure against the risk of an unauthorized user gaining access to the internal network during a system outage.

All services and traffic to be authorized across the firewall implementation must be well documented. Documented will be the business need, protocol used, inbound and/or outbound, port assignments, known vulnerabilities, and risk mitigation statements.

18.5. Firewall with Intrusion Detection OR External IDS/IPS:

All the traffic passing through the Internet should be subjected to inspection and all the known attacks, patterns relating to attacks will be detected and blocked by IPS.

All the applications requiring Internet access need to be tuned and complied to the signatures pattern for IPS. This can be done by Firewall having IDS/IPS functionality or external IPS which can be put in Inline mode.

The IDS/IPS should be regularly updated with the latest signatures as released by the vendor.

18.6. Network Information Dissemination

Information regarding access to, or configuration of, ADEPTION computer and communication systems, such as network diagrams, is considered confidential. This information must not be posted on electronic bulletin boards, listed in telephone directories, placed on business cards, or made available to third parties without the written permission of ADEPTION Information security team.

18.7. Service Specific Policies

The table below contains examples of some of the most common services that need to be approved by the Information security group before implementation. It is not an all-inclusive list and is subject to change.

1. Status (Y/N) = whether users can use the service

2. Auth (Y/N) = whether any form of authentication (strong or otherwise) is performed before the service can be used

Service	Policy				Policy Details
	Inside to Outside		Outside to Inside		
	Status1	Auth2	Status1	Auth2	
FTP (SFTP protocol should be encouraged)	Yes	No	No	No	FTP access will be allowed from the internal network to the external. For transmission of sensitive information, VPN’s should be implemented. No FTP access will be allowed externally through the Firewall to FTP servers within ADEPTION’s trusted network. FTP servers in the DMZ will be allowed. FTP clients on the inside will be configured to use FTP Passive Mode and will not use FTP Normal Mode.
Telnet (SSH protocol should be encouraged)	No	No	No	No	Telnet access will be allowed from the inside network to the outside network. For telnet from the outside to the inside network VPN will be required.
HTTP	Yes	No	No	No	All WWW servers intended for access by external users will be hosted outside the ADEPTION firewall. No inbound HTTP will be allowed through the ADEPTION firewall unless it uses reverse proxy and strong encryption/authentication (e.g. SSL).
SSL	Yes	No	Yes	Yes	Secure Sockets Layer sessions using client side certificates is required when SSL sessions are to be passed through the ADEPTION firewall.
SQL	No	No	No	No	Direct connections from external hosts to internal databases are not allowed. The use of reverse proxy will be considered by the ADEPTION on a case by case basis.

19. Laptop Security

19.1. ADEPTION Theft / Loss

In case of laptop theft /loss, the user needs to file FIR with the police and submit FIR copy to IT team for the insurance claim.

The Information Security group & IT helpdesk would need to be informed about the theft or any damage caused to the laptop by the user.

Laptops which were suspected to be stolen and subsequently found should not be plugged in on the network directly. This should be brought to the notice of the Information Security group for ensuring that it's not compromised.

19.2. Circulation laptop

Circulation laptops will be issued on approval to the authorized employee subject to availability. Users would need to check the proper functioning of the laptop and accessories and take custody after sign off. IT Teams will check the laptop and accessories once they are returned. The IT team needs to sign off confirming the laptop was returned. If required, users can also ask for mail confirmation from IT Teams.

The responsibility of users issued with a circulating laptop is the same as that of a user to whom the laptop is allocated on a permanent basis.

When a used laptop is being reissued, the data would be deleted before issuance.

19.3. Transfer

Users should not transfer laptops without confirmation from the IT Teams.

Users should keep IT teams informed about such transfers. Final transfer will happen on receiving mail confirmation or sign off from the employee who has received it.

Reallocation of assets should be logged by IT Teams with new user's details. The new user should confirm the receipt of the laptop to IT Teams.

If a used laptop is being reissued, the data would be deleted before issuance.

19.4. Resignation

Employees, when resigning, should surrender their laptop to IT Teams for getting necessary clearance. IT Teams will keep the asset in the name of the department and allocate on instruction of the department head.

If the department wants to keep the asset within the department, the department head or person authorized by him/her will take custody of this laptop and intimate IT Teams by mail.

IT Teams will transfer the asset on the name of the employee who has requested to keep it. On reallocation of this asset, the owner should inform the IT team on new user details (name, employee number, department, telephone Extn, location in premises etc.).

If a used laptop is being reissued, the data would be deleted before issuance.

IT Teams will maintain an inventory of all laptops issued and will ensure the recovery of these laptops before clearing a resigned employee.

19.5. Servicing / Disposal

If a laptop is damaged employees shall inform Helpdesk. Under no circumstances the employee will try to repair or rectify the damage.

The IT Team will assess the damage and will send it to the service provider (if under warranty) OR to the company approved vendor for repairs. A record will be maintained of the same (this could be on call logging system).

On return of the repaired laptop, the IT team will update the record and send the laptop back to the user.

If the laptop has to be disposed (scenarios - end of life, badly damaged etc.), IT teams will contact the Information Security group & handover the same to dispose off.

In case of IT assets damaged by a user, ADEPTION may recover the cost for repair or replacement from User, even if the laptop is under warranty as damages are not covered.

19.6. Guidelines for users

Users should not change any settings on the laptop.

Users shall ensure that they have latest Anti virus software /security patches updated and enabled on to their laptops. Users must ensure the corporate approved encryption software is installed on their laptops.

Pirated, freeware and shareware software shall not be downloaded or installed onto user laptops. Users shall use only the authorized and legal software. Copies of software installation files shall not be kept on the laptop.

Users must not share any data folders /drives on their laptops without necessary approvals. Appropriate permissions would be put in place on the folders/drives before access is provided.

Users should not install any add on card (wireless access card, modems etc.) on their own.

Backup all their data regularly.

Ensure the laptop is physically secured at all times, especially when leaving it unattended for extended periods of time e.g. lunch /tea breaks or overnight, leaving it in hotel rooms. Hardware locks should be considered for this.

If the laptop is used for Internet access at residences, the user should take special precautions not to visit malicious sites which could download potential spyware, adware, viruses, or trojans to the laptops. On suspicion (pop ups, machine slowing down, ad's being displayed etc.) the user should inform Information Security team immediately to get his laptop cleaned before connecting to the corporate network.

On theft or loss of a laptop, users have to inform the Information security team immediately. If a 'lost' laptop is found after some time, they should inform the Information security team so necessary checks can be done to ensure the laptop was not compromised.

For laptop users, who often work on sensitive information displayed on their screens, use of privacy screens should be considered.

20. Web Security

20.1. Web Security

- ADEPTION Intranet covers various services, viz. E-mail, discussion forums, File transfer (FTP), Enterprise Wide Web (EWW), Remote login (Telnet), Video conferencing, Directory services, Chat tools (IRC).
- However security for the services for Email, FTP, Telnet and Remote login is covered in other sections of the Information Security Policies and Guidelines like Network security and Email security. Hence, the policies and guidelines laid down in this document have to be read in conjunction with those specific policies and guidelines.
- Further, the ADEPTION companies are currently referring to the internal web site as their Intranet, which offers viewing to all employees, for general information, departmental data or special applications requiring approval and authentication.

20.2. ADEPTION Information dissemination

- Intranet information is for dissemination only to authorized persons. Users must not forward this information to others without seeking approval of the 'information owner' and appropriate departments, as applicable viz., Human Resources, Media Communications.

20.3. Material source permission

- If the material posted originates outside ADEPTION, written permission from the source must first be obtained and the source must be given adequate credit.

20.4. Intranet Access

Third party access

- Third party access to the Intranet must be approved by information owner's department head.

20.5. Application security

Users must be authenticated before granting access to the special applications, using user ID and password and/or certificates. As far as possible all intranet applications should authenticate users using active directory database, especially in cases where it's transactional based and involves customer information.

Secure communication at application level

- Secure communication at application level must be provided for restricted/confidential information sites, like using Secure HTTP (Https) application level encryption/authentication protocol.
- Caching of confidential information.

- Caching of confidential information must be forbidden on web server and clients.
- IP address, password should not be hard coded and view source should be disabled.
- All web applications shall be developed using secure programming guidelines as defined

20.6. Logging and auditing

Logging of web server

Critical applications or areas should be logged as required by the application owner.

Central contact point of report

Users must report to a central contact point, the Head-ISG, whenever, confronted with

- anomalies that could point to an intrusion, and
- all violation incidents

20.7. Application Induction process

Mandatory hardening, auditing & third party penetration testing of web servers to be carried out before going live for Internet facing applications. Intranet applications which are transactional in nature and involve customer information should also undergo this process.

All new web applications being inducted should undergo Application Security Life Cycle (ASLC) process & risks signed off before going live, especially for Internet facing applications.

20.8. Web servers security

Network Services

- Unused and unnecessary network services must be turned off on the host machine.

Client access

- SSL should used for web sites providing sensitive contents (transactional nature and involves customer information)
- All programs, scripts, web documents and arbitrary files present on the web server must be made available and accessible on a strict 'need to know' basis.
- If the FTP server and the web server share the same space for web content, upload / download rights should be strictly authenticated.

WWW Log Checks

- In addition to the regular system logs, Web and systems administrators must perform Web log checks for suspicious activity on the host servers, using approved tools.

Prohibiting Protocols

- Routing Information protocol (RIP) must not be allowed on systems directly connected to Internet. Static routes must be used on such systems.

Server Root Directory

- The server root directory must be configured so that only the server owner can write to the configuration and log directories and to their contents.

Permissions for Directories Containing Executables

- All directories that store executable files must be assigned the minimal file permissions required. For example, the contents in a UNIX server's cgi-bin directory must be assigned 755 permissions, or world executable and readable, but not Writeable.

Control of Document Root

- Automatic directory listings must be disabled and unwanted files removed entirely from document root.

Log Files

- The company shall maintain logs for intranet systems for a period of 60 days. It is the responsibility of the web server admin to maintain these logs.
- Web server administrator must backup the Web log files after at least 2 months, before deleting them.

Embedded Links

- Additional authentication of embedded links on the Website must be ensured, in order to prevent cascading of loss to such sites or confidential network locations due to the security compromises of the website.
- Third party URLs (redirection) on the Websites should provide a warning message which will indicate that user is getting redirected to a non-ADEPTION web-site.

21. Wireless Security

21.1. Administration

- Access provision – the administrator will not provide the connectivity unless the access provision requirement listed in point 4 is met.

21.2. Client based security

- All laptops with wireless should be equipped with antivirus software which should be updated regularly.
- Use of peer-to-peer communications bypassing access points is prohibited.

22. Disciplinary Action

22.1. Disciplinary Action

A staggered approach shall be followed in taking disciplinary action against the employee on compliance. Employees may initially be let off with a lighter penalty (e.g., a reprimand) till the security culture is established in ADEPTION. Implementation may thus be done in the following three steps:

Step 1 (1st 6 months): Counseling

Step 2 (Next 3 months): Verbal Reprimand & Written Memo

Step 3 (Subsequently): Any of the punitive actions mentioned below.

Punitive actions will be laid down for each category of the violation. Punitive action may be decided on a case-to-case basis depending on the impact of the violation on the information systems resources of ADEPTION. A few possible punitive actions for each level of violation are listed below:

Severity Category	Possible Punitive Action
High	Suspension of Service / Termination of Employment / Cancellation of Contract
Medium	Severe Reprimand / Suspension of Service
Low	Reprimand

The high and medium severity violations may directly result in the execution of Step 3 bypassing Steps 1 and 2.

Suggested categorization of various violations

Type of violation		Severity		
		High	Medium	Low
E-Mail Security				
9	Unauthorized use of another person’s e-mail		X	
10	Intentionally sending viruses through e-mail attachments	X		
11	Transmitting confidential or sensitive company information without sufficient security	X		
12	Inappropriate auto forwarding of e-mail			X
13	Using e-mail in a manner that		X	
	interferes with normal business activities	X		
	or hampers employee productivity			X
	or embarrasses ADEPTION	X		
	or consumes more resources involves solicitation is associated with any for-profit outside business activity		X	
14	Blanket forwarding of e-mail			X
15	Sending profane, obscene or derogatory e-mails	X		
16	Using hand-rendered signatures in e-mails	X		
Password Policy				
17	Violating password naming conventions			X
18	Re-use of same passwords or using the same password across different systems			X
19	Password /User ID sharing / disclosure	X		
20	Insecure conveyance / storage of passwords by normal users		X	
21	Insecure conveyance / storage of critical passwords	X		
22	Making unauthorised password resets of other users in their absence	X		
23	Making password resets of other users in their absence for emergency business purposes without approvals		X	
24	Non-use of screen saver by normal users			X
25	Non-use of screen saver on servers	X		
26	Not disabling default passwords		X	
27	Not hardening servers as per approved hardening documents	X		

28	Laptops not secured with encryption software (with no exception sign off)	X		
29	Non-adherence to coding / development security guidelines	X		
30	Downloading & Installing freeware / shareware without authorization/ approvals. Storing unauthorised software (MP3, unofficial files etc.) on local desktop / laptops		X	
31	Having network sniffer's, scanning agents without BISO approval	X		
32	Disabling anti-virus agent on machines without BISO /CISO exception /approval	X		
33	Installing modems on desktops without BISO approval	X		
34	Not adhering to clear desk policy-customer information lying on desks or in open	X		
35	IT /Server rooms being used as store rooms		X	
36	Not backing up company data on backup folders		X	
37	Copying company information /data on personal removable media	X		
38	Permitting vendors/ third parties devices to connect to internal networks	X		
39	Saving /Storing corporate data on public mailing sites	X		
40	Sending corporate data in clear text to third party vendors (consultants/auditors/suppliers)	X		
41	Storing critical/confidential data on laptops/desktop without authorization		X	

23. Visitor and Contractor Premise Access Policy

23.1. Information Disclosure

Visitors should not request information that does not pertain to their visit, or the work being performed.

Confidential or otherwise inappropriate nature, requests for corporate documents, customer information, financial projections, comments on any matter currently under litigation, future products or future corporate direction, or requests for information or statements in the name of the company (as might be requested by a reporter or a lawyer) will be reported to the Office of the CISO, and will be dealt with under the "Punitive action for violation of policy" policy this into their estimates for exit times.

23.2. Emergency Evacuation

In the event of an emergency, it is the sponsoring employee's responsibility to ensure that the Visitor is escorted and remains in the Evacuation marshalling area.

23.3. Network or System Access

Consultants or other Visitors that require internet network access should either access the same using their data card OR request the employee to provide a ADEPTION owned machine to access the same. Under NO circumstances will consultants or other Visitors personal / official devices be connected to ADEPTION network.

Visitors who require access to production IT networks will need permission from their employee sponsor, who will arrange temporary credentials with the Helpdesk.

After credentials are arranged, activities on the network will be subject to the Acceptable Use Policy & monitored by the employee. Visitor use of employee credentials is not permitted under any circumstances.

Visitors who require access to the production network will require prior permission from the CTO and BISO / CISO. Visitor use of employee credentials is not permitted under any circumstances.

Contractors making changes to production systems on ADEPTION networks are subject to the IT and Production Systems Change Control Policy. In these cases, employee sponsors are required to review this policy with affected Visitors and ensure that the lead time and exceptions sections especially are clearly identified.

Remote access to ADEPTION networks is governed by ADEPTION 'Remote Access Policy'.

23.4. On Courtesy

All employees of ADEPTION are to bear in mind at all times that all Visitors are either customers or potential customers. Even in the case of clear violations of this policy, all actions, dealings and conversations are to be courteous in nature and dealt with by HR.

23.5. Responsibility

This document is maintained jointly by the Administration Department and the Office of the CISO (Chief Information Security Officer).

Enforcement of this policy falls to these offices, as indicated in this document.

23.6. Penalties

Violation of any of the requirements in this policy by any employee will result in suitable disciplinary action, as given in Punitive Action for violation of policy.

Violation of any of the requirements in this policy by any Visitor can result in similar disciplinary action against the sponsoring employee and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.

24. Remote Access

24.1. Remote Access

The security component of any Remote access tool shall include the following technologies in order to guarantee the security of network connections, authenticity of users and the privacy and integrity of data:

- Authentication:
  - Authentication methods: Authentication database source must be Active Directory or LDAP, and the Authentication protocol must involve a challenge- response protocol that is not susceptible to replay attacks. The remote access tool must mutually authenticate both ends of the session.
  - Application support and scalability: Users of any IP-based service shall be authenticated in order to establish a secure VPN session.
  - Access Control: The remote access management systems shall be used to control destination addresses, subnets and domains, and the ports and services available to all client or vendor access.
- Remote access tools must support strong, end-to-end encryption as mentioned in ADEPTION policy for Cryptographic Security.
- All approved remote access systems shall be placed directly behind the firewall at each location that has information which needs to be accessed from other locations.
- End users who need access to information from another non-ADEPTION site shall do so through a VPN client or SSL session.
- ADEPTION antivirus, data loss prevention and other security systems must not be disabled, interfered with, or circumvented in any way.
- File Share mechanism via VPN or SSL based remote access systems is prohibited.

24.2. Remote access for ADEPTION Employees

All employees issued a ADEPTION laptop /desktop and having adequate approvals from the functional head and ADEPTION information security team are authorized to connect remotely to ADEPTION computer systems.

Remote access via client based VPN or SSL connectivity should only occur from computers issued from ADEPTION unless the ADEPTION Information Security team reviews the configuration on non-ADEPTION computers to ensure adequate installations of anti-virus software Data leakage prevention software, security patches and USB/ CD is blocked.

Remote access should be limited to specific systems required by the employee to perform their job function.

24.3. Third party Remote access

Third parties comprises of vendors consultants, auditors etc. either based out of ADEPTION premises or off-premises & supporting ADEPTION systems.

Remote access via client based VPN or SSL connectivity should only occur from computers issued from ADEPTION unless the ADEPTION Information Security team reviews the configuration on non-ADEPTION computers to ensure adequate installations of anti-virus software Data leakage prevention software , security patches and USB/ CD is blocked.

If access is provided from non-ADEPTION endpoints an exception shall be taken in this regards Head-IT and Group CISO.

Third parties shall be assigned remote access after obtaining approval from the sponsoring functional manager, Head – IT and Group CISO.

If third parties require privileged ID, monitoring of their activities shall be performed and the access shall be revoked immediately on their termination of association with ADEPTION. Sponsoring Functional Manager shall be responsible to inform the IT and Information Security group of such termination.

In addition, an expiration of not more than 15 days or lesser shall be placed on all third party user-IDs unless appropriate approval is given. Expiration of IDs will occur in the authenticating database. After the expiration, third parties who wish to continue working for ADEPTION should obtain approval in order to regain the User-ID.

Remote access should be limited to specific systems required by the third party to perform their job function.

24.4. Compliance & Audit

- Periodic audits shall be carried out to ensure compliance with this policy.
- Remote Access System Owners shall maintain evidence of
  - All requests for granting remote access.
  - All notifications for initiating the revoking of remote access.
  - All evidence for granting, revoking, or changing remote access privileges shall be maintained in a repository such as Change Management System (Refer Annexure I).
  - SOP’s and System Design documents for remote access systems.
  - All changes to the remote access system configuration.
  - Patch upgrades performed on remote access systems.
- On a monthly basis, the system owners shall ensure that the accounts active within the Remote access solutions are accurate. All discrepancies shall be resolved quickly.

24.5. Definitions

Challenge-Response:

- A protocol where one party presents a “challenge” and the other must present a “response” to be authenticated.

Data loss prevention:

- System to identify, monitor, and protect data in use, at rest, and in motion from accidental or intentional transmission.

LDAP:

- Lightweight Directory Access Protocol -- a protocol for querying and modifying directory services (often user authentication information).

Replay Attack:

- The use of a previously recorded authentication session in order to obtain unauthorized access.

Remote access tool:

- Any of a number of tools that provide remote access to a computer system “as if” the remote user were actually sitting in front of the computer.

25. Information Security Risk Management Framework

25.1. Introduction

Every organization, small or large, is susceptible to risks in different areas e.g., operational, market, legal, environmental, reputational, brand, liability, financial, property loss etc. Any of these can impact the organization (positively or negatively).Most organizations are,concerned primarily with the type of risk that may affect them in a negative way. However, there are positive risks which are referred to as opportunities.

Risk management helps the organization to identify, evaluate, analyze, monitor and mitigate risks that threaten the achievement of the organization’s objectives in a disciplined and systematic way.

This framework is defined on generally accepted industry best practices and standards. Though the framework can be applied to general risk management, this is mainly focused on Information and IT Risk Management.

25.2. Objective

The objective of this framework is to ensure that Information Security risks are identified, evaluated, analyzed, mitigated and monitored on a continuous basis and maintained at the optimum level.

25.3. Terms and Definitions

Sr. No.	Term	Definition
1	Organization	Organization refers to Adeption, all Locations. It also applies to the assets owned by Adeption and maintained at third party locations.
2	Information Asset	An information asset is any data, device or other component of an organization's information system that has value to the organization e.g. hardware, software, documents, people, third party services etc.
3	Access control	Access control includes both access authorization and access restriction. It refers to all the steps that are taken to selectively authorize and restrict entry, contact, or use of assets. Access authorizations and restrictions are often established in accordance with organization and security requirements.
4	Accountability	To make an entity accountable means to assign actions and decisions to that entity and to expect that entity to be answerable for those actions and decisions. Therefore, accountability is the state of being answerable for the actions and decisions that have been assigned.
5	Asset	An asset is any tangible or intangible thing or characteristic that has value to an organization which include obvious things like machines, facilities, patents, software, services, information, people, and characteristics like reputation, image, skills and knowledge.
6	Attack	An attack is any unauthorized attempt to access, use, alter, expose, steal, disable or destroy an asset.
7	Authentication	Authentication is a process that is used to confirm that a claimed characteristic of an entity is actually correct.

8	Availability	Something is available if it is accessible and usable when an authorized entity demands access.
9	Organization continuity	Organization’s ability of delivering its products and services at acceptable predefined levels after disruptive incidents occur.
10	Confidentiality	Confidentiality is a characteristic that applies to information so that it is accessible or disclosed to only authorized entities.
11	Conformity	Conformity is the "fulfillment of a requirement" or to comply with requirements which can be customer, contractual, regulatory, and statutory and so on.
12	Consequence	Outcome of an event
13	Context	An organization’s context includes all internal and external issues that are relevant to its purpose. Internal context includes its approach to governance, contractual relationships, capabilities, culture, and standards. It also includes the organization’s structure, policies, objectives, roles, accountabilities, its human, technological, capital, and systemic resources. External context includes stakeholders, social, cultural, political, legal, regulatory, technological, economic, natural, and competitive environment. Continual improvement is a set of recurring activities that are carried out in order to enhance the performance of processes, products, services, systems and organization. Any administrative, managerial, technical, operational or legal method that is used to manage the risk. It includes processes, policies, procedures, programs, tools, techniques, technologies, devices, and organizational structures.
14	Control Objective	A statement that describes what controls are expected to achieve.
15	Correction	Any action that is taken to eliminate a nonconformity. Corrections do not address causes (corrective actions address causes).
16	Corrective action	Steps taken to eliminate the causes of nonconformities in order to prevent recurrence.
17	Documented information	Information that is controlled and maintained.
18	Event	Occurrence or even a non-occurrence (when something doesn’t happen that was supposed to happen). Events

		sometimes referred to as incidents.
19	Executive/ Senior management	People who are responsible for implementing the strategies and policies needed to achieve an organization's purpose.
20	Information security	Protect and preserve the confidentiality, integrity and availability of information. It may also involve protecting and preserving the authenticity and reliability of information and ensuring that entities can be held accountable
21	Information security continuity	It is the predefined level of security continues during a disaster or crisis.
22	Information security event	A system, service, network state, condition or occurrence that indicates that information security may have been breached or compromised or that a security policy may have been violated or a control may have failed.
23	Information security incident	One or more unwanted or unexpected information security events that could possibly compromise the security of information and weaken or impair organization operations.
24	Information security incident management	A set of processes that organizations use to deal with information incident management. It includes detection, reporting, assessment, response, remediation and learning process.
25	Information Security Management System (ISMS)	Set of policies, procedures, documents, records, plans, guidelines, agreements, contracts, processes, practices, methods, activities, roles, responsibilities, relationships, tools, techniques, technologies, resources, and structures that organizations use to protect and preserve information to achieve organization objectives.
26	Information System	Applications, services, or any other assets that handle information.
27	Integrity	Protection of accuracy and completeness of information.
28	Likelihood	Probability of something to happen.
29	Management System	Set of policies, procedures, documents, records, plans, guidelines, agreements, contracts, processes, practices, methods, activities, roles, responsibilities, relationships, tools, techniques, technologies, resources, and structures that organizations use to achieve organization objectives.
30	Monitoring	To determine the status of an activity, process, or system.
31	Nonconformity	Non-fulfillment or failure to meet a requirement

32	Nonrepudiation	Nonrepudiation techniques and services are used to provide undeniable proof that an alleged event actually happened or an alleged action was actually carried out by a person or entity.
33	Outsource	When an organization makes an arrangement with an outside Organization to perform part of a function or process.
34	Policy	A policy statement defines a general commitment, direction, or intention.
35	Procedure	A procedure is a way of carrying out a process or activity.
36	Process	A process is a set of activities that are interrelated or that interact with one another.
37	Requirement	A requirement is a need, expectation or obligation.
38	Residual risk	The risk left over after implementation of controls.
39	Risk	Risk is the “effect of uncertainty on objectives”. Risk is often expressed as a combination of two factors: probability (Likelihood) and consequence (Impact).
40	Risk acceptance	Risk acceptance is deliberate decision to live with or tolerate a risk or prepared to take a particular risk.
41	Risk analysis	Risk analysis is a process that is used to understand the nature, sources and causes of the risks that have been identified and estimate the level of risk.
42	Risk assessment	A process of risk identification, analysis and evaluation.
43	Risk evaluation	A process that is used to compare risk analysis results with risk criteria in order to determine whether or not a risk or a specified level of risk is acceptable or tolerable.
44	Risk identification	A process that involves finding, recognizing and describing the risks that could affect the achievement of an organization’s objectives.
45	Risk management	A coordinated set of activities, methods and techniques that organizations use to deal with the risk.
46	Risk owner	A person or an entity that has been given the authority to manage a particular risk and is accountable for doing so.
47	Risk treatment	Selecting and implementing one or more treatment options (Mitigate, Accept, and Avoid, transfer) to keep the risk at acceptable level.
48	Stakeholder	A person or an organization that can affect or be affected by a decision or an activity.
49	Third party	A person or anorganizationthatis independent of the people directly involved with activity.

50	Threat	A threat is a potential event which could exploit a weakness in the system.
51	Vulnerability	A vulnerability is a weakness of an asset or control that could potentially be exploited by one or more threats.

25.4. Scope:

This framework applies to all organization’s processes looking to identify, mitigate and monitor Information Security risks on a regular basis. The scope of this framework includes definition of risk management in line with the requirements of ISO 31000 and can be applied to all risks including but not limited to Information Security, Business Continuity, Privacy and Service Management.

25.5. Overview of Information Security Risk Management

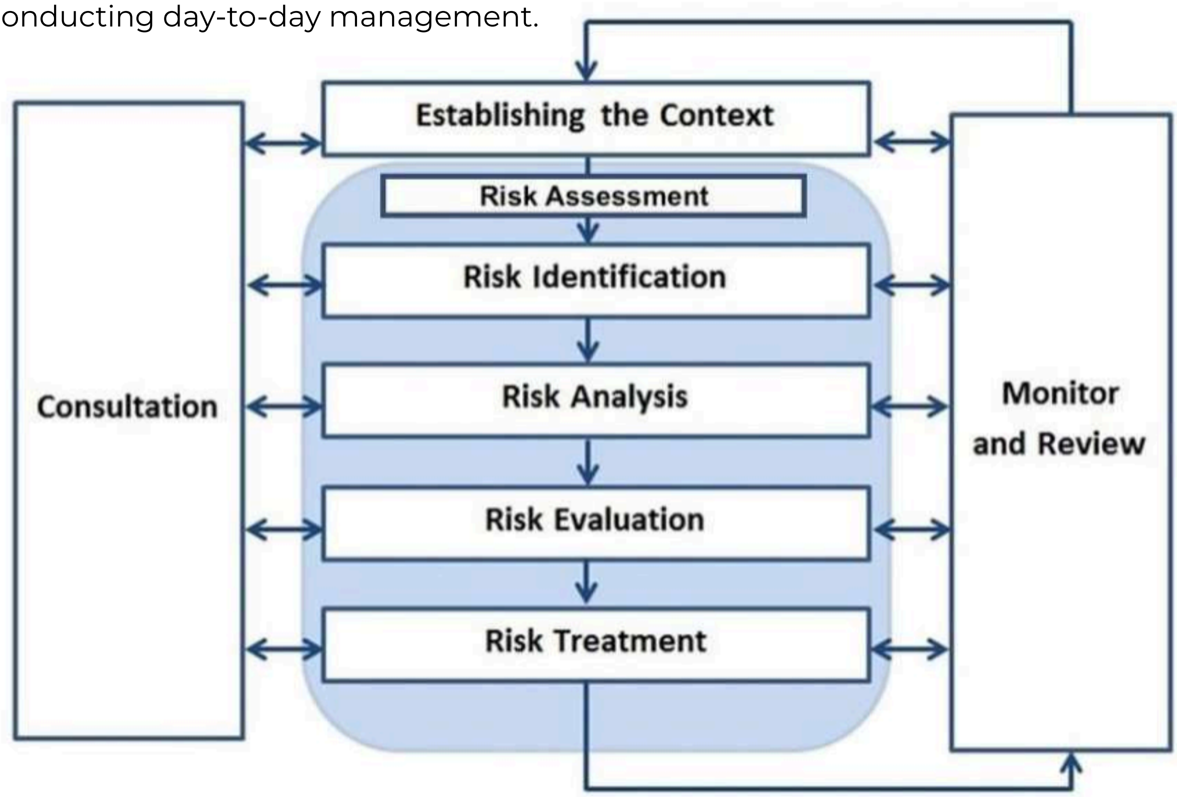
Information Security Risk Management (ISRM) is a continual process that involves the following key steps:

1. Communicate and consult
2. Establish the context
3. Identify the risks
4. Analyze risks
5. Evaluate risks
6. Treat risks
7. Monitor and review

It is important to follow this process when conducting ISRM as this ensures that the approach to ISRM is both comprehensive and consistent.

This process shall be formally conducted across the Organization on an annual basis. This framework illustrates both top-down and bottom-up approach to risk management.

Although this process is conducted on annual basis, ISRM is not solely an annual process. ISRM shall be kept as a continuous process with a close linking to organization's opportunities and risks. Therefore, everyone has a responsibility to continually apply this process when making security related decisions and when conducting day-to-day management.



25.6. Steps in Information Security Risk Management

1. COMMUNICATE AND CONSULT

1. Communication and consultation with internal and external stakeholders shall be considered as an important step throughout the ISRM process to ensure that the organization has a comprehensive picture of the risks we

face.

2. Communication shall be targeted to external stakeholders of the organization on:
   a. The organization's risk management approach.
   b. Requesting feedback where appropriate
3. Internal communication and consultation within the Organization shall be aimed at informing internal stakeholders of:
   a. The risk management process
   b. Seeking feedback in relation to the process c.Key risks and their respective owners

2. ESTABLISH THE CONTEXT

Organization shall aim to define the risk context which will include building:

The external context

This shall include:

1. Understanding the expectations of external stakeholders in terms of ISRM
2. Extenttowhichthisexternal environment will impact the ability of the Organization to achieve its objectives. This will include:
   a. Organization, Social, Regulatory, Cultural, Competitive, Financial and Political Environments in which the Organization operates.
   b. Considering existing Organization strengths, weaknesses, opportunities and threats in terms of information security.

This shall include understanding organizational elements and the way they interact, such as:

a. Culture, internal stakeholders, structure, capabilities (in terms of resources such as people, systems, processes and capital), goals and objectives and the strategies in place to achieve these

b. The goals, objectives, strategies, scope and parameters for the risk management process itself

Note: The “Establish the Context” part of the risk management process will only need to be repeated when there are significant changes to either the external environment or operations of the Organization.

3. IDENTIFY RISKS

1. Risk identification shall be carried out in the risk management process to ensure a complete list of risks are identified
2. Risks shall be mapped to the control objectives to ensure that no risk

scenario or control weakness is overlooked

3. Asset groups shall be defined in detail so that the risk applicability or control requirement can be mapped to the specific asset group only. This shall ensure relevant controls are applied to identified sub groups and excessive/inadequate controls can be avoided
4. Risks can be identified using various tools and techniques including

   but not limited to: a. Structured Interviews

   b. Audit
   Report c.
   Checklists

   d. Surveys and
   Questionnaires e.
   Focus Groups

   f. Root Cause Analysis
   g. Incident Management
   h. Strategic and Organization Plans etc.

4. ANALYZE RISKS

1. The risk shall be adequately described once it is identified
2. Components of a comprehensive risk description shall include

   (Risk Statement): a. Event e.g. Virus attacks;

   b. Cause e.g. Improperly managed antivirus; and

   c. Impact i.e. Inability to continue work due to possible information corruption.
3. Assess the impact of the risk eventuating with no controls in place (Inherent Risk). This will inform the gross risk rating with impact and likelihood.
4. Risk analysis shall involve (Residual Risk):
   a. Identifying controls currently in place to manage the risk by either reducing the consequence or likelihood of the risk;
   b. Assessing the effectiveness of current controls;
   c. Identifying the likelihood of the risk occurring; and
   d. Identifying the potential consequence or impact that would result if the risk was to occur.
5. Controls are aimed at bringing the risk within an acceptable level. Evaluation of current controls shall be carried out through processes including but not limited to:
   a. Controlled self-assessment;

   b. Internal Audit reviewing the effectiveness of
   controls; and c. External Audit reviewing the

effectiveness of controls.

6. The consequence and likelihood ratings, as identified after consideration of current controls, shall be combined to determine the overall risk level (residual risk).

5. EVALUATE RISKS

1. Risk evaluation shall take into consideration overall level of the risk.
2. Inputs from risk evaluation shall be considered to determine whether further risk treatment actions are required to bring the risk within a level acceptable.
3. The output of the risk evaluation phase shall be a prioritized list of risks.
4. There may be times when the action required will differ from that identified above. In such cases, the CIO must approve deviation from the above action.

6. TREAT RISKS

1. Risk treatment shall involve examining possible treatment options to determine the most appropriate actionfor managing a risk. Treatment actions shall be required where the current controls are not managing the risk within defined tolerance levels.
2. Treatment options may involve improving existing controls and implementing additional controls.
3. Possible risk treatment options shall include:
   a. Avoid/Terminate the risk – Change organization process or objective so as to avoid the risk;
   b. Mitigate/Treat the risk – Undertake actions aimed at reducing the risk c. Transfer the risk – Transfer ownership and liability to a third party; and d. Accept/Tolerate the risk – Accept the impact of the risk

4. Decision on the preferred treatment option shall be based on a cost benefit analysis. 5. The preferred treatment option shall trigger the following:

   a. The cost of any actions shall be incorporated into the relevant budget planning process;
   b. A responsiblepersonshallbe identified fordeliveryofthe action, with this expectation being communicated to them;
   c. A realistic target date of completion shall be set;
   d. Projected risk rating (after implementation of Risk Treatment Plan) shall be evaluated

7. Risk Acceptance Criteria

The risks identified as part of risk assessment exercise will be taken as acceptable level of risk only if either of the following criteria is met:

▪ If the Risk Level is Low i.e. Green zone (Risk Rating <=9)

▪ The Information Security Committee perceives that the cost of control for effectively mitigating the risk is greater than the risk.

▪ The risk is going to be nullified / mitigated in the near future due to change in control environment or operating environment.

▪ Risks is beyond the control of organization and are primarily of

National/global nature ▪ Implementation of control might create concerns regarding safety of employees and/or

humans in the neighborhood.

▪ The control impedes the operations

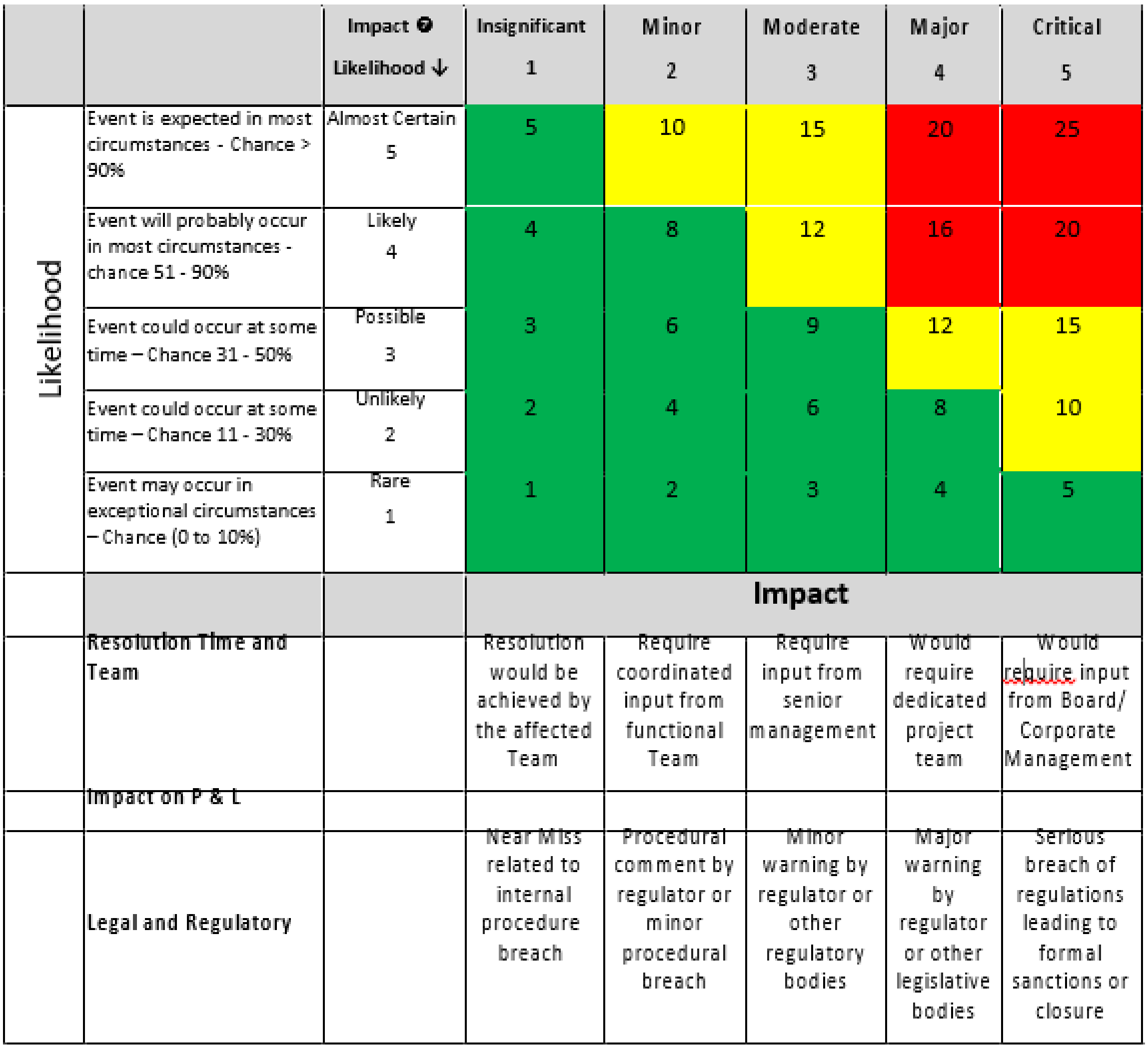
8. MONITOR AND REVIEW RISKS

1. The risk assessment shall be done periodically or after implementation of further mitigating controls and residual risks shall be reviewed.
2. Risk information shall require regular monitoring and review to ensure currency
3. Risk owners and other associated personnel shall have the responsibility to ensure continued currency of information pertaining to their particular risks

4. In addition, management from Organization shall review the risk register
on an annual basis 5. The effectiveness of the ISRM shall also be monitored
and reviewed annually

E. ANNEXURES

1. ANNEXURE 1 – RISK MODEL



		Impact ➔ Likelihood ↓	Insignificant 1	Minor 2	Moderate 3	Major 4	Critical 5
Likelihood	Event is expected in most circumstances - Chance > 90%	Almost Certain 5	5	10	15	20	25
	Event will probably occur in most circumstances - chance 51 - 90%	Likely 4	4	8	12	16	20
	Event could occur at some time – Chance 31 - 50%	Possible 3	3	6	9	12	15
	Event could occur at some time – Chance 11 - 30%	Unlikely 2	2	4	6	8	10
	Event may occur in exceptional circumstances – Chance (0 to 10%)	Rare 1	1	2	3	4	5
			Impact				
	Resolution Time and Team		Resolution would be achieved by the affected Team	Require coordinated input from functional Team	Require input from senior management	Would require dedicated project team	Would require input from Board/ Corporate Management
	Impact on P & L						
	Legal and Regulatory		Near Miss related to internal procedure breach	Procedural comment by regulator or minor procedural breach	Minor warning by regulator or other regulatory bodies	Major warning by regulator or other legislative bodies	Serious breach of regulations leading to formal sanctions or closure

1. Impact is the potential severity or effect of the risk.
2. Likelihood is the frequency or probability of risk occurring.
3. The ratings given to impact and likelihood (in a scale 1-5) produce an evaluation of net risk 4. Risk rating = likelihood * Impact (1-9: Low 10–15: Medium 16–25: High)
5. Types of Risk Inherent (Natural Risk in the Activity. Risk without any control in place) Residual (Balance Risk after implementation of present controls) Projected (Risk estimated after completion of Risk Treatment Plan)

Exceptions:

All exceptions to this policy shall be considered on an individual basis. For each exception, a duly filled Policy Exception form has to be approved. All exceptions shall include organization justification and benefits attributed to it. All exceptions shall be time bound and has to be reassessed and re-approved after the exception period as mentioned in the Policy Exception form. No exception shall be provided for a period more than one year.

Reference Documents

Policies

ISMS Policy

Topic Specific Policies

Procedures

-

Records / Templates

Risk Register

Standards / Guidelines

ISO 27001:2013 and 2022

ISO 27002:2013

ISO 22301:2019

================== x =============== x ================= x ===============