GUIDELINES FOR ASSESSMENT OF EFFECTIVENESS OF SECURITY CONTROLS

GD 220

Department of IT
Government of India
Ministry of Communications & IT
Electronics Niktan, 6 CGO Complex
New Delhi – 110003

Introduction

Regular assessment of effective implementation and maintenance of the selected security controls for an information system is necessary to detect flaws in implementation and operation of the defined controls and the processes, which can help in taking necessary timely corrective actions and improvements in the controls and the associated processes. Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. The guidelines for assessment of effectiveness in the security controls defined in this document are recommended for use in information systems for eGovernance.

This guideline is one of the documents identified in the eGovernance Security Assurance Framework (eSAFE). The list of the documents is given below.

Document No.	Document Title
ISF 01	Information Security Assessment Framework
GD 100	Guidelines for Security Categorization of eGovernance Information Systems
GD 200	Catalog of Security Controls
GD 201	Baseline Security Controls for LOW IMPACT INFORMATION SYSTEMS
GD 202	Baseline Security Controls for MEDIUM IMPACT INFORMATION SYSTEMS
GD 203	Baseline Security Controls for HIGH IMPACT INFORMATION SYSTEMS
GD 210	Guidelines for Implementation of Security Controls
GD 220	Guidelines for Assessment of Effectiveness of Security Controls
GD 300	Guidelines for Information Security Risk Assessment and Management

Contents

1.0 Scope

1.1 Objective

The purpose of this document is to provide guidelines for assessment of effectiveness of the selected security controls based on GD200/201/202/203 for information systems for eGovernance of the state and central governments of India. The guidelines apply to all components of an information system that process, store, or transmit information.

1.2 Description

Security controls assessments are the principal vehicle used to verify that the implementers and operators of information systems are meeting their stated security goals and objectives. This guideline document is developed to facilitate security control assessments which will provide evidence about the effectiveness of security controls in organizational information systems and Information about the strengths and weaknesses of information systems which are supporting critical eGovernment applications in a global environment of sophisticated threats.

This document should not be considered as a comprehensive document for audit concepts, principles and techniques. It only focuses on the assessment of effectiveness of the security controls listed in the document GD 200 using the well known technique of use of checklist/questionnaire based on the “Look AT” and “Look For” directives. In this document some important “Look AT” and “Look For” directives have been listed to help the assessors to prepare their assessment checklist/questionnaire while assessing the effective implementation and operation of the individual security controls.

2.0 Target Audience

Information Security Auditors/Assessors, Managers and concerned employees of Govt. departments and the third party service providers of Information System Security.

3.0 Type of Document

It is a Guidelines document recommended for enforcement in systems for eGovernance.

4.0 Definitions and Acronyms

5.0 Assessment Guidelines

Assessment guidelines for each of the security controls of GD 200 are tabulated below

A.IA-1: USER IDENTIFICATION AND AUTHENTICATION

Control: All the computing devices (servers, desktops, network devices) shall uniquely identify and authenticate the user or any process that acts on behalf of any user.

Control Improvements:

(i) Multifactor authentication- The application shall support multifactor authentication mechanism for user authentication.

(ii) Re-authentication – The application shall re-authenticate the user under the specified conditions (e.g. after specified interval of idleness or inactivity, session timeout, while accessing/modifying sensitive data like credential changing etc.)

Implementation Guidelines :

- This control should be applied for all types of users (privilege, non-privilege, local, remote) or processes
- The user ID should be traceable to individual user or process
- In case one account user ID is shared by a group of people, there should an additional mechanism in place so that the actual user of the account can be traceable.
- For remote users (beyond the physical security boundary of the organization) or If the sensitivity of the application or data is very high the authentication must be multifactor based. The same is achieved by multiple authentication factors like 'biometric', 'smart card', 'access token' etc. along with 'password' **[Control improvement (i)]**
- For sensitive systems where financial transactions or access to sensitive data is necessary, re-authentication must be implemented under some conditions like very long idle time, accessing less sensitive to more sensitive data, changing credential etc. **[Control improvement (ii)].**
- Define the requirement of the control mechanisms in RFP and/or SRS.
- Conduct formal testing of the implemented control mechanisms.

- Assessment guidelines

Look at	Look for
• SRS (Software Requirement Specification) • Identification & authentication mechanisms used in the application • Identification and authentication (I&A) policy and procedure • Test records	• Adequacy of the Identification and authentication (I&A) policy and procedure • Application configuration settings for I&A as per defined policy/procedure • Verify test logs in support of the compliance to the control

A.IA-2: AUTHENTICATION HINT

Control: The application should not give any hint or information about the authentication during the authentication process to avoid possible exploitation/use of the hint by unauthorized individuals.

Control Improvements: None

Implementation Guidelines :

- Don't display the password in clear text when it is typed by the users
- Don't give any hint line "wrong username', "wrong password" etc. when user mistypes.
- Define the requirement of the control mechanisms in RFP and/or SRS.
- Conduct formal testing of the implemented control mechanisms.

Assessment guidelines	
Look at	Look for
• SRS (Software Requirement Specification) • Identification and authentication (I&A) policy and procedure • Login pages of the application • Test records	• No display of typed password in clear text • No display of hint in case user-id or password is wrong • Verify test logs in support of the compliance to the control

A.IA-3: HANDLING OF AUTHENTICATION FAILURE

Control: The application enforces a limit of consecutive invalid authentication attempts by a user during a specified short time period. The application automatically locks the account for a specified time interval, when the maximum number of unsuccessful attempts is exceeded.

Control Improvements:

(i) The application automatically locks the account until released by an administrator when the maximum number of unsuccessful attempts is exceeded

Implementation Guidelines :

- Implement a mechanism to lock the account if authentication failure occurs for specified no of attempts.
- The account is locked for a specified duration and unlocked automatically at the end of the specified duration.
- The account is locked permanently until unlocked by an administrator **[Control Improvement-(i)]**
- Define the requirement of the control mechanisms in RFP and/or SRS.
- Conduct formal testing of the implemented control mechanisms.

Assessment guidelines

Look at	Look for
• SRS (Software Requirement Specification) • Account lock-out policy • Login pages of the application • Test records	• Application setting for implementation of the account lockout policy • No of attempts required to lock the account for authentication failure • Time required for release of the locked account • Verify test logs in support of the compliance to the control

A.IA-4: ENFORCING USE OF QUALITY AUTHENTICATION SECRET

Control: The application enforces users to use quality authentication secret by providing a mechanism to verify that the secrets meet specified quality criteria

Control Improvements:

(i) **Maximum password age:** Enforcing expiry of the authentication secret after specified time period (typically 30 days)

(ii) **Password history:** Restricting re-use of specified number (typically 5) of earlier used authentication secrets.

(iii) **Minimum password age**: Restricting change of authentication secret in quick successions by specifying a minimum period (typically 1 day) after which the secret can be changed

Implementation Guidelines :

- Application should not allow creation or use of weak passwords by users
- It should enforce minimum length of the passwords (as per policy)
- It should consists of at least one alfa and one numeric character
- Force users to change the temporary password given during the account creation at the first log-on
- Enforce expiry of password after specified period**[Control Improvement -(i)]**
- Maintain a record/history of specified no of previously used passwords to prevent re-use.**[Control Improvement -(ii)]**
- Restrict change of passwords in quick successions by enforcing minimum password age.**[Control Improvement -(iii)]**
- Define the requirement of the control mechanisms in RFP and/or SRS.
- Conduct formal testing of the implemented control mechanisms.

Assessment guidelines

Look at	Look for
• SRS (Software Requirement Specification) • Password policy • Application password management mechanism • Test records	• Adequacy of the password policy • Configuration of the application password management mechanism as per defined policy • Verify test logs in support of the compliance to the control

A.IA-5: GENERATING QUALITY AUTHENTICATION SECRET

Control: The application shall provide a mechanism to generate secrets that meet defined quality metric and to enforce the use of the secret for specified functions

Control Improvements: None

Implementation Guidelines :

- A common vulnerability of web applications is caused by not protecting account session tokens.
- Application should be protected from interception, prediction, brute-force, and fixation of session attacks.
- Session ids should be unique to users, and issued after successful authentication
- Session ids should not leak any sensitive or personal information
- Session ids should be random and unpredictable.
- Session ids should be protected throughout its lifecycle.
- Session ids should change routinely and always during major transitions,
- For highly secure transactions re-authentication and a new session id should be issued prior to processing the requested transaction
- On log out, the session id should be over-written
- Define the requirement of the control mechanisms in RFP and/or SRS.
- Conduct formal testing of the implemented control mechanisms.

Assessment guidelines

Look at	Look for
• SRS (Software Requirement Specification) • Session Management Policy • Test records	• Adequacy and proper implementation of secure session management mechanisms • Compliance to the quality metrics defined for session ids/tokens • Weak session management mechanism • Verify test logs in support of the compliance to the control

A.AC-1: SYSTEM ACCESS NOTIFICATION

Control: The application displays an approved, system use notification message before granting access, informing potential users: (i) that the user is accessing a Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system

Control Improvements: None

Implementation Guidelines :

- During login or accessing the application it should display a banner with following messages
  - You are accessing Government Information System
  - Your usage may be monitored, recorded and subject to audit
  - unauthorized use of the system is prohibited and subject to criminal and civil penalties
  - Any other messages defined in policy
- Define the requirement of the control mechanisms in RFP and/or SRS.
- Conduct formal testing of the implemented control mechanisms.

Assessment guidelines

Look at	Look for
• SRS (Software Requirement Specification) • Access Control Policy • Application logging process	• Suitable banner and messages are displayed during login / access to the application as per the defined policy. • Verify test logs in support of the compliance to the control

A.AC-2: ACCESS ENFORCEMENT

Control: The application enforces access control to the system in accordance with the applicable policy

Control Improvements:

(i) Cryptography based access control policy

Implementation Guidelines :

- Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices,) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the application level
- Use cryptography based access enforcement mechanism; the cryptography used should be standard, strong and tested as per the organization policy e.g. FIPS 140-2 (as amended) compliant **[Control Improvement- (i)]**.
- Define the requirement of the control mechanisms in RFP and/or SRS.
- Conduct formal testing of the implemented control mechanisms.

Assessment guidelines

Look at	Look for
• SRS (Software Requirement Specification) • Access control policy • Test records	• Proper implementation of the access control policy • Verify test logs in support of the compliance to the access Control Requirement/Policy

A.AC-3: NOTIFICATION OF PREVIOUS LOGON

Control: The application notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.

Control Improvements: None

Implementation Guidelines :

- The application implements display of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon, once a user logs on successfully to give him confidence and a mechanism to verify that his account has not been compromised.
- Define the requirement of the control mechanisms in RFP and/or SRS.
- Conduct formal testing of the implemented control mechanisms.

Assessment guidelines	
Look at • SRS (Software Requirement Specification) • Access Control Policy • Test records	Look for • Verify the required notification is implemented • Verify test logs in support of the compliance to the control

A.AC-4: CONTROL OF CONCURRENT SESSIONS

Control: The application is capable of limiting the number of concurrent sessions for any user.

Control Improvements: None

Implementation Guidelines :

- The application implements a mechanism to limit the number of concurrent sessions of a user as per the requirement or defined policy of the organization.
- Define the requirement of the control mechanisms in RFP and/or SRS.
- Conduct formal testing of the implemented control mechanisms.

Assessment guidelines

Look at	Look for
• SRS (Software Requirement Specification) • Access Control Policy • Test records	• Verify that concurrent sessions are allowed as per defined policy • Verify test logs in support of the compliance to the control

A.AC-5: AUTHENTICITY OF COMMUNICATION SESSIONS

Control: The application provides mechanisms to protect the authenticity of sessions during communication.

Control Improvements: None

Implementation Guidelines :

- This control focuses on communications protection at the session, versus packet, level.
- The intent of this control is to implement session-level protection where needed (e.g., in service-oriented architectures providing web-based services).
- Implement the use of transport layer security SSL/(TLS) mechanisms, IPsec, virtual private networks (VPNs) and other methods of protecting communications sessions and secure web services
- Define the requirement of the control mechanisms in RFP and/or SRS.
- Conduct formal testing of the implemented control mechanisms.

Assessment guidelines

Look at	Look for
• SRS (Software Requirement Specification) • Session Management Policy • Test records	• Verify that authenticity of the session is maintained by suitable mechanism • Verify test logs in support of the compliance to the control

A.AC-6: AUTOMATIC SESSION TERMINATION

Control: The application automatically terminates a remote session after specified period of inactivity.

Control Improvements:

(i) Automatic session termination applies to both local and remote sessions

Implementation Guidelines :

- A remote session is initiated whenever application is accessed by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). This control automatically terminates the remote session after a specified idle time.
- The automatic session termination occurs for local sessions (connected from own network or the system console) also.**[Control Improvement - (i)]**
- Define the requirement of the control mechanisms in RFP and/or SRS.
- Conduct formal testing of the implemented control mechanisms.

Assessment guidelines

Look at	Look for
• SRS (Software Requirement Specification) • Session Management Policy • Test records	• Verify that session terminates after defined period of inactivity • Verify test logs in support of the compliance to the control

A.AC-7: AUTHENTICATION OF CONNECTING EQUIPMENT

Control: The application allows access from a specific node or equipment identified by suitable identifiers.

Control Improvements: None

Implementation Guidelines :

- The application has a mechanism to identify the connecting node/equipment by suitable identifiers like IP Address, MAC Address etc., and it can give access to the authorized nodes/equipment only.
- Define the requirement of the control mechanisms in RFP and/or SRS.
- Conduct formal testing of the implemented control mechanisms.

Assessment guidelines	
Look at • SRS (Software Requirement Specification) • Access Control Policy • Test records	Look for • Verify that application identifies the source node or equipment before giving access • Verify test logs in support of the compliance to the control

A.AC-8: ACCESS LOG

Control: The application logs all access events.

Control Improvements: None

Implementation Guidelines :

- Application should be capable of creating transaction logs for accesses and changes to the data.
- The log should typically contain UserID of user or process ID of process causing the event, Success or failure of attempt to access , Date/time of event, Type of event, Success or failure of event, address), name of data object written or deleted etc.
- Define the requirement of the control mechanisms in RFP and/or SRS.
- Conduct formal testing of the implemented control mechanisms.

Assessment guidelines

Look at	Look for
• SRS (Software Requirement Specification) • Logging Policy • Test records	• Verify that application logs all access events • Verify test logs in support of the compliance to the control

A.AC-9: ACCESS TIME RESTRICTION

Control: Restrict application access to users at authorized time only.

Control Improvements: None

Implementation Guidelines :

- Connection time controls should be considered for sensitive computer applications, especially from high risk locations, e.g. public or external areas that are outside the organization's security management.
- Examples of such restrictions include
  - Using predetermined time slots, e.g. for batch file transmissions, or regular interactive sessions of short duration;
  - Restricting connection times to normal office hours if there is no requirement for overtime or extended-hours operation;
  - Considering re-authentication at timed intervals.
- Limiting the period during which connections to computer services are allowed reduces the window of opportunity for unauthorized access.
- Limiting the duration of active sessions prevents users from holding sessions open to prevent re-authenticating.
- Define the requirement of the control mechanisms in RFP and/or SRS.
- Conduct formal testing of the implemented control mechanisms.

Assessment guidelines

Look at	Look for
• SRS (Software Requirement Specification) • Access Control Policy • Test records	• Verify that application has provision to restrict the access time • Verify test logs in support of the compliance to the control

A.AC-10: ENFORCING DATA INPUT BY HUMAN (CAPTCHA)

Control: Use CAPTCHA to enforce data input by human only not by computer programs or 'bots'.

Control Improvements: None

Implementation Guidelines :

- A CAPTCHA is a program that protects websites against bots by generating and grading tests that humans can pass but current computer programs cannot. For example, humans can read distorted text but current computer programs can't.
- A CAPTCHA can ensure that web application form fields cannot be filled up by machines/programs to crowd the backend database with junks and causing Denial of Service or other undesirable conditions.
- CAPTCHAs can also be used to prevent dictionary attacks in authentication pages. The idea is simple: prevent a computer from being able to iterate through the entire space of passwords by requiring it to solve a CAPTCHA after a certain number of unsuccessful logins.
- Define the requirement of the control mechanisms in RFP and/or SRS.
- Conduct formal testing of the implemented control mechanisms.

Assessment guidelines	
Look at • SRS (Software Requirement Specification) • Access Control Policy • Test records	Look for • Verify that CAPTCHA has been implemented as per policy • Verify test logs in support of the compliance to the control

A.DH-1: INPUT DATA VALIDATION

Control: The application checks validity of the input data to the application.

Control Improvements: None

Implementation Guidelines :

- Checks should be applied to the input of business transactions, standing data (e.g. names and addresses, credit limits, customer reference numbers), and parameter tables (e.g. sales prices, currency conversion rates, tax rates).
- The following guidelines should be considered:
  - dual input or other input checks, such as boundary checking or limiting fields to specific ranges of input data, to detect the following errors:
    - out-of-range values;
    - invalid characters in data fields;
    - missing or incomplete data;
    - exceeding upper and lower data volume limits;
    - unauthorized or inconsistent control data;
  - procedures for responding to validation errors;
  - procedures for testing the plausibility of the input data;
- Automatic examination and validation of input data can be considered, where applicable, to reduce the risk of errors and to prevent standard attacks like SQL injection, Cross Site Scripting, buffer overflow, command or code injection etc.
- Define the requirement of the control mechanisms in RFP and/or SRS.
- Conduct formal testing of the implemented control mechanisms.

Assessment guidelines

Look at	Look for
• SRS (Software Requirement Specification) • Coding standard • Test records	• Verify invalidated inputs are not allowed • Verify that input validation is not solely based on client side validation • Verify test logs in support of the compliance to the control

A.DH-2: PROTECTION OF TRANSMITTED DATA

Control: The application protects the integrity and confidentiality of the transmitted data (authentication credentials only) between the client and the server applications.

Control Improvements:

(i) The application protects all data during transmission using encryption mechanism

Implementation Guidelines :

- The application implements suitable mechanism to ensure protection of integrity and confidentiality of the authentication credentials like user-ID, passwords etc during transmission through communication channels.
- Cryptographic transmission channels like SSl/TLS may be used for this.
- The protection may be implemented for all data. **[Control Improvement- (i)]**.
- Define the requirement of the control mechanisms in RFP and/or SRS.
- Conduct formal testing of the implemented control mechanisms.

Assessment guidelines

Look at	Look for
• SRS (Software Requirement Specification) • Test records	• Verify suitable cryptographic means SSL/TLS has been used • Verify test logs in support of the compliance to the control

A.DH-3: APPLICATION PARTITIONING

Control: The application separates user functionality (including user interface services) from application management functionality.

Control Improvements: None

Implementation Guidelines :

- The application system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management).
- Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.
- Define the requirement of the control mechanisms in RFP and/or SRS.
- Conduct formal testing of the implemented control mechanisms.

Assessment guidelines

Look at	Look for
• SRS (Software Requirement Specification) • Solution Architecture • Test records	• Verify the Solution Architecture for proper separation • Verify test logs in support of the compliance to the control

A.DH-4: ERROR HANDLING

Control: The application identifies and handles error conditions in such a manner so that no sensitive information that could be exploited by adversaries is leaked through the error messages.

Control Improvements: None

Implementation Guidelines :

- Ensure that the application provides error-handling processes.
- The application code should not rely on internal system generated error handling. Errors are properly handled by the application.
- Ensure that the application does not leak information in error condition that can be used by an attacker.
- Error messages should not include variable names, variable types, SQL strings, source code etc..
- Define the requirement of the control mechanisms in RFP and/or SRS.
- Conduct formal testing of the implemented control mechanisms.

Assessment guidelines

Look at	Look for
• SRS (Software Requirement Specification) • Test records	• Verify that application does not leak information during Simulated Error Condition • Verify test logs in support of the compliance to the control

I.IA-1: USER IDENTIFICATION AND AUTHENTICATION

Control: All the computing devices (servers, desktops, network devices) shall uniquely identify and authenticate the user or any process that acts on behalf of any users.

Control improvements:

(i) The information system employs multifactor authentication for remote system access
(ii) The information system employs multifactor authentication for system access locally.

Implementation Guidelines :

- This control should be applied for all types of users (privilege, non-privilege, local, remote).
- The user ID should be traceable to individual user or a group of users (though not recommended).
- In case one account user ID is shared by a group of people, there should an additional mechanism in place so that the actual user of the account can be traceable.
- In some of the devices, by default the authentication scheme is not present or default system accounts are without password. Such default system accounts without password shall be disabled.
- Passwords are a very common way to provide identification and authentication based on the philosophy that the user only knows the password. As the choice of password is left to the user the same may be short (e.g. 'pw'), weak (e.g. 'password'), guessable (e.g. 'Pa$$w0rd).
- Password policy should be enforced so that all the system accounts are bound to have password of minimum quality (like number of character, complexity etc.) [Ref. control I.IA-4].
- The application software requires some system account and that should not be the account of highest privilege ('Administrator' for Windows or 'root' for Linux or UNIX OS).
- For remote users (beyond the physical security boundary of the organization) the authentication must be done in two stages; one on network level (e.g. VPN authentication) and other on system level (e.g. domain authentication or authentication on system accounts) **[Control improvement (i)].**
- If the sensitivity of the application or data is very high, strong authentication is need (decided through Risk Assessment). The same is required to be achieved by two factor authentication like 'biometric', 'smart card', 'access token' etc. along with 'password' [Control improvement (ii)]

Assessment guidelines

Look at	Look for
• Network devices and servers • Remote users permitted • Protocol used for remote Connections • Running applications • Shared Accounts, if any	• Whether they can be accessed without password • Whether they are controlled through VPN • Whether clear text protocol like telnet are used • Whether the application require 'Administrator' or 'root' during run time. • The sensitivity of the shared account and associated Risk Assessment in respect of use of such account

I.IA-2 NODE AUTHENTICATION FOR REMOTE ADMINISTRATION OF NETWORK DEVICES AND SERVERS

Control: In addition to user authentication, the identification of the equipment from which the remote administration is performed should be considered as an additional control for authentication, in case remote administration of servers and network devices is permitted.

Implementation Guidelines :

- Remote access to the system, especially for system administration, brings additional risk of unauthorized access. Hence, remote system administration over public network preferably be avoided as far as possible; if such activity is unavoidable the same should be carried out with extreme care. However, remote administration of the servers and network devices in LAN is very common practice.
- A machine in the network (LAN) is identified by its MAC address. Since, MAC is a non-routable protocol; MAC information cannot be transmitted from one network (Ethernet) to another. Hence, MAC based node authentication is useful only in LAN environment. Enforcement of this control (I.IA-2) will ensure that the communication for system administration have been initiated from known locations or equipment.
- In the event of remote administration over public network, IP based node authentication may be useful. This will restricts remote administration only from specified IP addresses. As IP addresses are easier to modify or spoof than MAC addresses, remote administration over public network should be limited to specific system administration activities only. The organization is required to perform risk assessment to identify comparatively low risk system administration activities and allow them to be conducted over public network; the rest of the activities (system administration) shall be conducted from LAN environment or through local console.
- It may be necessary to consider physical protection of the equipment to maintain the security of the list of equipment identifiers.

Assessment guidelines

Look at:	Look for:
• Areas of remote administration • Risk Analysis out put • Nodes (in LAN) wherefrom remote administration done	• Policy for remote administration • Issues of remote administration addressed • Whether the node is physically secured

I.IA-3: MANAGEMENT OF IDENTIFIER

Control: The user identifier shall be unique for each user so that the activities performed by the user on the information system can be traced back to an individual. There shall be a managed process of handling of user account

identified by an identifier. The managed process shall clearly state:

(i) Approval authority for creation of user accounts for information systems. The organization policy shall clearly define the approval authority for different information systems, considering their sensitivity.

(ii) The user account should also be suspended or disabled through a managed process

Implementation Guidelines :

- Assuming that the control I.IA-1 is in place i.e. all the systems are uniquely identify and authenticate the users before allow them to access the system. The users to the system must be explicitly associated. The organization is required to adopt a managed process for user registration.
- The use group accounts should be avoided as far as possible (as the individual activities cannot be traced back from the log of use of such accounts). In case, the group account is absolutely unavoidable, the same can be allowed only on a formal clearance from the competent authority, designated for information security of the organization.
- In addition to the mandatory aspects described in the control statement, the documented user registration process should include the following:
  - Authorization of the user from the system owner along with specific access rights ('read only', 'write', or 'full control' etc.) on the resources
  - Communication to the user about their access rights along with the condition of access, if any.
  - Maintenance of records of approval and implemented access rights
  - Removal or blocking the access right of the user, in the event of his change in role or separation with the organization.
  - Periodical checking of the access rights
  - Generic names like 'guest', 'everyone' etc. shall be avoided as a first line of protection of such accounts from unauthorized use.
  - Not issuing redundant user IDs to others.

Assessment guidelines

Look at	Look for
• User registration process • Records related to user registration activities	• Approved documented user registration process • The aspects/issues described under implementation guidance are defined in the document • The records supporting the defined and documented process.

I.IA-4: SPECIFICATION OF AUTHENTICATOR

Control: The authenticator of the user account shall be strong enough to protect the user account from unauthorized use by means of defining its minimum length and complexity [*combination of alphanumeric and special characters*].The minimum length and complexity should be in accordance with the organization's password policy.

The system enforces the realization of the specification of the authenticator as well as its validity through technological means.

Control improvements:

(i) Internationally approved hash function should be used to store the authenticators, so that the probability of guessing the authenticator from its hash is extremely difficult

(ii) Use of two factor authentication for accessing systems having greater sensitivity and where the identity of the user cannot be ensured through other means

Implementation Guidelines :

- It is necessary that all the information and information processing facilities shall be protected by suitable access control mechanism. 'User Identification and Authentication' is one of the means to extend access control over a user account.
- Weak password management leads to vulnerability of misuse of systems by unauthorized persons, with the associated risk of breaches of confidentiality, loss of integrity and availability of data. Where systems provide automatic controls over password quality and frequency of change, these should be used. The following aspects should be considered as attributes for password quality:
  - Passwords should have appropriate length and complexity (min. 8 characters, combination of alphabets, alphanumeric, special characters, etc.) for the required security and also should balance security and operational ease of access. In particular, they should not be able to be found in a dictionary or contain predictable sequences of numbers or letters.
  - The system should enforce good quality password as per the policy adopted by the organization
  - The system should store the password not in clear text and should eliminate use of weak hash (NTLM hash instead of LANMAN hash or salted MD5) [**Control improvement (i)].**
  - The authenticator shall not be based on anything easily guessable like person related information, e.g. names, telephone numbers, dates of birth etc.
  - System should not display the passwords on the screen when being entered
  - Store password files separately from application system data
  - For highly sensitive system, the 'root' or 'administrator' password shall be broken into two parts and each part will be available with two different persons to minimize the security risk by person.
  - In environments with a high risk of interception or intrusion (such as remote operator interfaces in a facility that lacks local physical security access controls), organizations should consider supplementing password authentication with other forms of authentication such as challenge/response or multi-factor authentication using biometric like thumb impression, physical tokens(RSA token), smart card or USB token having digital certificate [**Control improvement(ii)**]

Assessment guidelines

Look at	Look for
• The password policies of the systems • The system file storing the user password and its access rights • System log-in interface • Areas identified as high risk (if any)	• Log in interface complying the aspects stated in implementation guidance • Strength of password • Proper access rights of the password file • Implementation of two factor authentication scheme (if adopted for high risk areas)

I.IA-5: MANAGEMENT OF AUTHENTICATOR

Control: The organization should manage the 'information system authenticators' (e. g password) by

(i) Defining initial authenticator content
(ii) Establishing administrative procedures for distribution of initial authenticator, re-issuing of authenticator in the event of loss or compromise or damage of user authenticator
(iii) Establishing administrative procedures for revoking authenticators
(iv) Changing default authenticators upon information system installation
(v) Changing/refreshing authenticators periodically

Control improvements:

(i) The change of authenticator, if necessary, should be performed after completion of positive identification verification of the requestor
(ii) The users are required to change their default password /authenticator on first log in

Implementation Guidelines :

- Users generally use password for logging directly into a local device or computer
- System administrator should set a password while creating the account and communicate the same to the user of the account.
- Passwords should not be sent across any network unless protected by some form of FIPS-approved encryption or salted cryptographic hash specifically designed to prevent replay attacks.
- The organization should discourage use of group account and sharing of account credentials and enforce the use of individual user IDs and passwords to maintain accountability.
- The system should allow users to select and change their own passwords.
- The system should be configured in such a manner that it enforces mandatory change of password on first log on [**Control improvement(ii)**] and enforce change of password periodically (as per the Organization's Policy) and as well as should maintain a record of previous user passwords and prevent re-use.
- The organization should use secure protocol for transmission of accounts credentials, in case the authentication credential is required to be transmitted over network.
- The organization should adopt a managed process to verify the identity of the requestor for resetting or reissue of the account password [**Control improvements (i)]**.

- The default passwords of the devices (e.g. network routers, switches, Access point etc.) should be changed during installation and this practice should be integrated with the organizational procedure for installation of the computing and communication devices.
- The keeper of master passwords should be a trusted employee, available during emergencies. Any copies of the master passwords must be stored in a very secure location (a sealed envelope or a properly access controlled repository with limited access).
- The passwords of privileged users (such as network technicians, electrical or electronics technicians and management, and network designers/operators) should be most secured and be changed frequently.
- Authority to change master passwords should be limited to trusted employees. A password audit record, especially for master passwords, should be maintained separately from the control system (I.AL-2)

Assessment guidelines	
Look at • Documented user registration process • Records related to user registration activities • System log-in interface • Custodian of passwords of master accounts (like 'Administrator', 'root' , 'DB admin' etc.	Look for • Users' capability for changing his/her own password • Password dissemination method(including that over network) while creating new user account or after resetting (on request) • System enforcement of password change on first log-on or on expiry of password life • Logs of changing the passwords of master accounts

I.IA-6: AUTHENTICATION FOR EXTERNAL CONNECTION

Control: Additional authentication method to be used for the users' (persons/process) requests, originated from a network not under the physical security control of the organization. The clear text protocols like FTP, TELNET etc. shall be strictly avoided, especially while transmitting the authentication credentials. Instead suitable secure protocols should be used where threats for unauthorized disclosure data during transmission do not exist.

Control improvements:

(i) Use of virtual private network (VPN) for remote access from public domain
(ii) Use of two factor authentication mechanism (password plus RSA token) for remote access
(iii) Use of digital certificate as a means of authentication to the remote users
(iv) Use of dedicated private lines for remote access to ensure the source of connections
(v) Controlling of all remote accesses through a limited number of managed access control points protected with firewall
(vi) Mandatory logging of all remote access with sufficient detailing

Implementation Guidelines :

- Any remote users, accessing the organization network from untrusted networks should require to be authenticated additionally as permitted remote user. Once connected, they should be required to authenticate a second time at the internal network.
- For remote connection user of clear text protocols like TELNET should be avoided and instead encrypted channel protocol like SSH should be used.
- If remote connection is necessary from public domain use of VPN should be adopted. Separate VPN channel should be used for accessing information systems (internal) of different sensitivity.[**Control improvements(i)]**
- The organization should invoke logging mechanism for all remote access and critically review the same especially for the privileged users(like database administrator, system administrator.[**Control improvements(vi)]**
- Dedicated private lines can also be used to provide assurance of the source of connections. [**Control improvements(iv)]**

Assessment guidelines	
Look at • Management approval for remote use • Authentication scheme for accessing the system beyond the physical boundary of the organization. • Records in respect of allocation of remote access	Look for • Presence of additional layer of authentication for remote users across the organization's boundary • Security of the protocol used for remote access • Security of the protocol used for remote authentication • Logs of remote access to the critical information system (if permitted) and evidence for their regular review.

I.IA-7: USER REGISTRATION AND DEREGISTRATION

Control: A formal procedure will be in place to control the allocation of access rights to information systems and services. The procedure covers all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and as well as change in access rights. Special attention should be given, where appropriate for the need to control the allocation of privileged access rights.

Control improvements:

(i) Periodical verification [*periodicity and responsibility should be defined as a part of organizations security policy*] of the access rights of the users and endorsement of the same from the information system owner

(ii) Periodical [*periodicity and responsibility should be defined as a part of organizations security policy*] checking for redundant user IDs and accounts and blocking/disabling the same

Implementation Guidelines :

- A formal procedure for user registration and de-registration need to be adopted by the organization covering all stages of the user access life-cycle. The procedure should address the following issues:
  - Allocation of unique user IDs, as far as possible, to establish clear links to the users so that they can be held responsible for their actions; the use of group IDs should only be permitted where they are necessary for business or operational reasons, and should be approved and documented
  - Specific authorization from the system owner in respect of user access rights on the information system.
  - Periodic verification of the user access rights, so that they are appropriate to the business purpose and consistent with organizational security policy (e.g. not compromising the principle of segregation of duties) and also communicate the report to the information system owners. **[Control improvement (ii)]**
  - Written communication to the user about his/her access rights and subsequent acknowledgement for the same
  - Maintenance of record of all authorization
  - Immediate blocking of the access rights of the user who have changed the roles or jobs or left the organization
  - Periodically checking for redundant user IDs and accounts and removing or blocking the same. **[Control Improvement(i)]**

Assessment guidelines	
Look at • The documented user registration process • Related records	Look for • The user registration process is complying with the issues addressed in 'Implementation Guidance' • Evidence in support of the process being followed.

I.AC-1: ACCESS CONTROL POLICY

Control: The organization should develop; disseminate a formal and documented access control policy. The access control policy should address the purpose, scope, roles, responsibilities, coordination among organizational entities and also the compliance to the legal/statutory or contractual requirements.

Control improvements:

(i) Periodic review/update [periodicity and authority should be defined as a part of organizations security policy] of access control policy

Implementation Guidelines :

- Access control policy is always very organization specific. Hence, it is necessary to establish and document the access control rules and access rights for each user or group of user clearly.
- The logical access control policy should be established, considering the physical access control policy of the organization as its security level is heavily biased by that of associated physical access control mechanism.
- The security requirement of individual business application varies; hence, the access control policy should contain clear statement, in respect of the business requirement, being addressed by the policy. It should also address the following issues:
  - Standard user access profiles for common job roles in the organization
  - Management of access rights in a distributed and networked environment
  - Segregation of access control roles, e.g. access request, access authorization, access administration (including removal)
  - Periodicity of review of access control policy itself. **[Control improvement(i)]**

Assessment guidelines

Look at	Look for
• Documented Access Control Policy (logical) • Physical access control system in place	• The content of the policy addressing the issues described in the implementation guidance • Evidence of periodic review of the access control policy

I.AC-2: ACCOUNT MANAGEMENT

Control: The organization shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization shall review information system accounts as per the defined policy of the organization in respect of suitability of the account and its access rights.

Control improvements:

(i) The information system should automatically terminate temporary and emergency accounts after a pre-defined period unless otherwise specified
(ii) The information system should automatically disable inactive accounts after a period of inactivity
(iii) The organization should have automated mechanisms to audit the activities like account creation, modification, disabling and termination etc. and should notify, as required, to designated individuals

Implementation Guidelines :

- This control addresses the implementation aspect of documented access control policy.
- The organization should clearly assign the responsibilities of account management for different business applications including Operating systems.
- The activities defined in the control should be supported by suitable evidences like log or paper records.
- The review of access rights shall be conducted periodically as per the defined policy and the result of the review should be communicated to the owner of the business application.
- The information system may be so configured it will keep watch on its accounts and disable the same, if no activity found for a certain pre-defined period.[**Control improvements(ii)]**

Assessment guidelines

Look at	Look for
• Documented responsibilities for management of access control responsibilities of different information systems. • Records related to implementation of access control policy	• Evidences for account management as per policy • Review records of the user accounts for different information systems • Evidences of communication of the review results to the owner of the business information systems • Evidences in support of the activities related to dormant accounts

I.AC-3: ACCESS ENFORCEMENT

Control: No information system should be accessed without authorization as assigned in the access control policy laid down by the organization.

Control improvements:

(i) The activities of the privileged functions should not be allowed to be carried out over network from a point beyond the physical security boundary of the organization
(ii) Access to the information system should be controlled from a central authentication services
(iii) All the activities related to the privileged function should be automatically logged with sufficient details for future verification, if necessary. The logs should be appropriately protected
(iv) Authorization based on cryptographic techniques like use of digital certificate should be used for enforcement of access to the information system

Implementation Guidelines :

- Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) should be enforced through mechanisms like access control lists, access control metrics etc. and the same should be realized technologically in the information systems of the organization.
- The mechanisms should be employed to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) of the information system.
- This access enforcement to be employed in addition to that employed at the application level. This layered approach of authorization is necessary to improve information security level of the organization.
- To enforce access enforcement, it is mandatory to use proper file system (for the objects) within the organization (like NTFS or ext3 but not FAT32).
- The system configuration should be used to enforce privileged activities like system administration can only be performed from a predefined hosts only [**Control Improvement (i**)].
- Organization may adopt 'Directory Services' to centrally control the access to its all information systems. [**Control Improvement(ii)**]

Assessment guidelines

Look at	Look for
• The mechanisms used to enforce access control policies in OS level and as well as in application level • The system configurations of servers and network devices	• The specific system configurations, supporting enforcement of access control policies, including the same for remote access.

I.AC-4: SEGREGATION OF DUTIES

Control: Access to the information system shall be assigned in such a way that separation of duties is enforced for the related activities like authorization and creation of user accounts.

Control improvements:

(i) The access to the audit logs for privileged activities should not accessible to the user (privileged) who performs that activity

(ii) The audit logs should be transferred as soon as they are generated from the devices where the logs are generated

Implementation Guidelines :

- The organization should establish appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest and document the same. Examples of separation of duties include: (i) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security) (ii) security personnel who administer access control functions do not administer audit functions.
- Information systems should be invoked with auditing functionalities along with identification of log server so that the audit logs generated in the system are transferred to the log server as soon as they are generated. The administrative access of the log server should be kept separated.[**Control improvement(ii)**]

Assessment guidelines

Look at	Look for
• The organizations' approach towards identification of areas need for segregation of duties	• The evidences of implementation of this control.

I.AC-5: NETWORK SEGMENTATION

Control: The network architecture and segmentation should be based on different security level (depending on the nature of the information asset and anticipated security threats).

Control improvements:

(i) Sensitive networks should be physically separated from the rest of the organization network

Implementation Guidelines :

- The security of a large network can be controlled by dividing them into separate logical network segments, each protected by a defined security perimeter.
- The network segmentation should be defined based on a risk assessment and the different security requirements within each of the network segments. Such a network perimeter can be implemented by installing a secure gateway between the networks having different trust levels.
- The gateway should be configured to filter traffic between the segments and to block unauthorized access in accordance with the organization's access control policy. An example of this type of gateway is what is commonly referred to as a firewall.
- Another method of segregating separate logical domains is to restrict network access by using virtual local area networks for user groups within the organization.
- Networks can also be segregated using the network switches, having capability of creation of VLANs).
- The criteria for segregation of networks into segments should be based on the access control policy and access requirements. In addition, segregation of networks should be based on the value and classification of information stored or processed in the network, levels of trust, or lines of business, in order to reduce the total impact of a service disruption.
- Consideration should be given to the segregation of wireless networks from internal and private networks.
- As the perimeters of wireless networks are not well defined, a risk assessment should be carried out in such cases to identify controls (e.g. strong authentication, cryptographic methods, and frequency selection) to maintain network segregation.

Assessment guidelines

Look at	Look for
Network diagram indicating the computing resources and gateways	• Logic for network segregation is commensurable with the security requirement of the network segments. • The document control measures of the Network diagram

I.AC-6: NETWORK ROUTING CONTROL

Control: The organization should adopt a policy in respect of controlling the information flow within the system and between interconnected systems. The information system should enforce such policy wherever there is a difference in the level of trust.

Control improvements:

(i) Explicit routing rule should be deployed to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices)
(ii) Blocking outside traffic that claims to be from within the organization
(iii) Restriction of the traffic from Internet to the servers on Ext. DMZ only
(iv) Not passing any web requests to the Internet that is not from the internal web proxy

Implementation Guidelines :

- One of the golden rules of IT security is the "need-to-know principle", according to which user should only be allowed to access that data and run those programs for which they are authorized. This rule will ensure that information belonging to one department (e.g. sales, development, human resources, management etc.) cannot be automatically accessed by people from other departments. This golden rule should be implemented in network architecture through network segregation and enforcement of routing control on the network traffic at the gateway.
- Segregation of networks are done based on the value and classification of information stored or processed in the network. The network segment of the database servers is usually assigned with highest security level where as Internet is assigned with lowest security level.
- Security gateways can be used to validate source and destination addresses at internal and external network control points . The requirements for network routing control should be based on the access control policy.[**Control improvements(i)]**
- As a best practice the network traffic from the segment of lower security should be explicitly allowed to the segment of higher security level.[**Control improvements(ii)]**
- If there is no business requirement then the traffic between two networks having same trust level should not also be allowed. Traffic originated from Internet, if required to be allowed inside the organizational network the same should be contained in the De-militarized zone. .[**Control improvements(iii)]**

Assessment guidelines

Look at	Look for
• System configuration of the servers in a network segments • System configuration of the gateway hosts • Firewall rules (both External and Internal)	• Consistency of the system configurations with the network diagram • All the firewall rules are explicit and are in accordance with the principle of " need to know"

I.AC-7: NETWORK CONNECTION CONTROL

Control: For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications.

Control improvements:

(i) Linking network access rights to certain times of day or dates

Implementation Guidelines :

- The shared networks especially those extending across the organization's boundary are not sufficiently protected by physical security controls and hence inherently imposed security risks. Hence, the capability of users to connect to the resources of such network should be restricted.
- The restriction may be imparted based on various aspects like Time of connection. For example routine network administration activities like user creation, installation of new application software, change in firewall rule set etc should be restricted during normal office hours.
- The restriction may also be extended considering the type of resources for which access is sought.

Assessment guidelines

Look at	Look for
• Solution architecture for accessing network resources from outside the physical boundary of the organization • System configurations	• Evidences in the system configuration in support of the restrictions imposed as stated in 'Implementation guidelines'

I.AC-8: SECURE LOG-ON PROCESS

Control: Access to the operating systems should be controlled by a secure log-on procedure.

Control improvements:

(i) On successful logon, the information system should notify the user about the date and time of the last logon

(ii) On exceed of allowed number [*to be defined by the organization*] of unsuccessful log-on attempts, the secure log on process of the information system should automatically lock the account or the node for a period[*defined time period*], and delay next login prompt. Due to the potential for denial of service, automatic lockouts initiated by the information system should be a temporary affair and should automatically release after a predetermined time period [defined by the organization]

(iii) The information system should limit the number [*defined number*] of concurrent sessions for any user

(iv) The log on process of the information system should prevent further access to the system by initiating a session lock after [*defined time period*] of inactivity, and the session lock remains in effect until the user

reestablishes access using appropriate identification and authentication procedures

(v) The log on process should enforce automatic session termination both for local and remote sessions for a period [*defined time period*] of inactivity

(vi) The log on process should limit the maximum time allowed for the log-on procedure. If exceeded, the system should terminate the log-on process

Implementation Guidelines :

- The procedure for logging into an operating system should be designed to minimize the opportunity for unauthorized access. In order to avoid providing an unauthorized user with any unnecessary assistance, the log-on procedure should therefore disclose the minimum of information about the system.
- Information system's good log-on procedure should be configured in such a way, so that it should
    - Not display system or application identifiers until the log-on process has been successfully completed.
    - Displays a general notice warning that the computer should only be accessed by authorized users and not provide help messages during the log-on procedure that would aid an unauthorized user.
    - Not display the password being entered or consider hiding the password characters by symbols
    - Validate the log-on information only on completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect.
    - Limit the number of unsuccessful log-on attempts allowed, e.g. to three attempts, and consider the following action:[**Control improvement(ii) &(iii)**]
        - recording unsuccessful and successful attempts and also forcing a time delay before further log-on attempts are allowed or rejecting any further attempts without specific authorization [**Control improvement(iv)]**
        - Disconnecting data link connections, if at all got established.**[Control improvement(v)]**
        - Sending an alarm message to the system console if the maximum number of log-on attempts is reached
        - Limiting the maximum and minimum time allowed for the log-on procedure. If exceeded, the system should terminate the log-on; :[**Control improvement(vi)**]
    - On completion of a successful log-on, a good log-on procedure should preferably display the date and time of the previous successful log-on.[**Control improvement(i)]**

Assessment guidelines	
Look at	Look for
• The log-on interfaces of different information systems	• Evidence of implementation of aspect of a good log-on procedure as stated in the 'Implementation guidance'

I.AC-9: WIRELESS ACCESS CONTROL

Control: The organization shall establish restriction in usage of wireless technology because of its inherent insecurity. However, if at all wireless access is allowed, the same should be done under strict authorization.

Control improvements:

(i) The organization should change the keys/secrets associated with the wireless access points periodically [*organization-defined frequency, but at least once in six months*], through a managed process

(ii) The organization should periodically [*defined by the organization policy*] scan for unauthorized wireless access points and take appropriate action if such an access points are discovered. The scan should not be limited to only those areas, containing the high-impact information systems, but should also cover the adjacent areas

Implementation Guidelines :

- Inadequate authentication between clients and access points is the prime vulnerability or wireless network. Hence, strong mutual authentication between wireless clients and access points is needed to ensure that clients do not connect to a rogue access point deployed by an attacker, and also to ensure that un-authorized wireless users do not connect to the organization's wireless networks.
- The next issue in wireless network is inadequate data protection between clients and access points. Hence, sensitive data between wireless clients and access points should be protected using strong encryption. This will ensure that attackers will not be successful in getting the information, even though they are able to sniff the traffic transmitted over wireless network. Following implementation guidelines to be followed:
  - Enforcing MAC Address Filtering: This method uses a list of MAC addresses of client wireless network interface cards that are allowed to associate with the access point
  - Not broadcasting the SSID (Network ID): The first attempt to secure wireless network was the use of Network ID (SSID). The default feature of broadcasting of SSID by the access point may be disabled and the same can be issued to the clients looking for WLAN connectivity
  - Disabling DHCP service from WLAN access point, instead if required, the parent DHCP service (from wired LAN) shall be used
  - Using a network firewall to secure a wireless network
  - Use of WEP, WPA etc. as bare minimum security for authentication and protection of information on a wireless local area network (WLAN)
  - For WEP minimum key length should be 128 bit
- The organization should change the keys/secrets associated with the wireless access points at least once in six months, through a managed process. [**Control improvement(i)**]
- The organization should periodically [defined by the organization policy] scan for unauthorized wireless access points and take appropriate action if such an access points are discovered. The scan should not be limited to only those areas, containing the high-impact information systems, but should also cover the adjacent areas[**Control improvement(ii)**]

Assessment guidelines

Look at	Look for
• Formal authorization for use of wireless access • System configuration of the access point	• Evidences to enforce access restriction for wireless network • Evidences for use of encryption protocol for wireless communications

I.AC-10: REVIEW OF ACCESS RIGHTS

Control: The organization should review privileged users' access rights on all information system at regular intervals [*organization-defined frequency*] using a formal process. In addition to the periodic regular review, this review should be conducted after any changes, such as promotion, demotion, change (of responsibility) or termination of employment.

Control improvements:

All users' access rights should be reviewed at regular intervals and after any changes, such as promotion, demotion, change (of responsibility) or termination of employment

Implementation Guidelines :

- The users request for the access rights for business purpose and most of the cases the requirement is not in permanent nature. It is quite usual that revocation requests for access rights do not come the way their invocation requests are made. Hence, leaving an information system (data or resources) with excess access rights (both in terms of privileges and period) is a common fact in the organization.
- A review mechanism (for access rights) can minimize the security risk. It is necessary that authorizations for special privileged access rights should be reviewed more frequently than non-privileged access rights.
    - The organization should consider the following guidelines while reviewing the access rights:
        - Users' access rights should be reviewed at regular intervals, at least once in 6 months
        - Privilege allocations should be checked at regular intervals, at least once in 3 months
        - Authorizations for special privileged access rights should be reviewed at more frequent intervals, at least once in 3 months
        - User access rights should be reviewed and re-allocated when moving from one employment to another within the same organization
        - Changes to privileged accounts should be logged for periodic review.
        - Users' access rights should be reviewed after any changes in responsibility (such as promotion and demotion) and as well as for change in role[**control improvement**]

Assessment guidelines

Look at	Look for
• The defined process of review of access rights • Review records • Records of authorizations for special privileged access rights	• The evidences complying with the implementation guidance • The evidences of review of access rights in the event of change in employment or responsibility

I.AL-1: SELECTION OF AUDITABLE EVENT

Control: The information system should be configured to generate audit records for the pre-defined events [*organization to defined auditable events*].

Control improvements:

(i) The information system should have the capability to compile audit records from multiple hosts/components throughout the system into an organization wise, time-correlated audit trail

(ii) The organization should periodically [as defined by the organization] review and update the list of organization-defined auditable events

Implementation Guidelines :

- The organization should identify the information system components on which the auditing activities will be carried out.
- As auditing activity may affect information system performance, selection of the auditable events should be done after risk assessment.
- Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network.
- The devices from which the audit records are expected, should have a reliable clock to facilitate generation of time–correlated audit trails, if compiled from different hosts[**Control improvement(i)**]
- The auditable event initially selected (through Risk assessment) should be brought under regular review to ensure the relevancy of selected auditable events [Control improvement(ii)]

Assessment guidelines

Look at	Look for
Identified information system components for which auditing are invoked	• Consistency of selecting auditable events with the results of risk assessment • Reliability of the clock of the system generating auditable events • Records of review of the list auditable events

Implementation Guidelines

Control :

I.AL-2: AUDIT RECORD MANGEMENT

Control: The information system should produce audit records that contain sufficient information to establish what events occurred and when, the sources of the events, and the outcomes of the events.

Control improvements:

(i) The information system should generate the audit records in a commonly used standard format so that the same can be transported to different system
(ii) The information system should provide the capability to centrally manage the content of audit records generated by individual components throughout the system
(iii) The information system should provide the capability for inclusion of additional, more detailed information in the audit records for audit events identified by type, location, or subject

Implementation Guidelines :

- Audit records or log records are important data to investigate the security incidents, if any. Further, through audit data the security manager or administrator gain confidence that the information systems are behaving in intended manner. Each of the audit record or log should contain the minimum information like what is the event, when it has occurred, the sources of the events and the outcomes of the events.
- Organization often adopts control of segregation of duties in respect of system administration and review of audit logs. In such cases, it is necessary to relocate the audit logs out of the systems where they have been generated [I.AL-4]. Hence, it is necessary that the system should be configured in such a manner that they generate the audit logs in a standard format, so that the audit logs can be used in other system after relocation. RFC3164 is the common syslog format to be used [**Control improvement (i)**].
- The organization may configure a completely independent server (syslog server) to store all log data centrally. The administrative access of this syslog server should be kept separated from that of the hosts whose logs are being maintained in the central syslog server **[Control improvement (ii)].**

Assessment guidelines	
Look at • Audit logs or records maintained	Look for • Presence of necessary minimum information in an audit record, as stated in the implementation guidance • The compliance of the audit record format with RFC 3164 , if the records are required to be transmitted to the other system • Independency of log server (if present

I.AL-3: CAPACITY OF STORAGE FOR AUDIT LOGS

Control :

Control: The organization should allocate sufficient storage capacity for audit records and should configure the auditing scheme in such a way that the likelihood of exceeding the capacity is minimum.

Control improvements:

(i) The organization should make the provision for a dedicated storage system with sufficient capacity of storage in the system for audit logs from different hosts and network components of the information system

Implementation Guidelines :

- The default allocated space for audit log in the servers and network hosts are usually not sufficient to store the audit log for longer period. Hence, it is necessary to re-configure this allocation so that it is consistent with the organization's policy on retention of audit logs.
- If necessary, system may be configured in such a manner that the audit logs will be relocated to the other storage space periodically to minimize the risk of automatic overwriting.
- The organization may deploy a dedicated server for storing the audit logs; the back-up policy of the organization should consider this server (data) also [**control improvement(i)**]

Assessment guidelines

Look at	Look for
• System configuration of servers and network devices • System configuration of the log server (if any)	• Space allocated for storing the audit logs • Actions selected, in the event of exhaustion of the allocated space • If the logs are relocated, then presence of the target host, its configuration and as well as its physical and logical access control implemented.

I.AL-4: PROTECTION OF AUDIT /LOG DATA

Control: The information system should protect audit/log information from unauthorized access, modification/tampering and deletion.

Control improvements:

(i) Automatic transfer of system audit log (as soon as they are generated) to a system under different administrative control than the server or host from where the audit log is generated

(ii) Protection of audit log by encryption on audit storage

Implementation Guidelines :

- Some audit logs may be required to be archived as part of the record retention policy or because of the requirements to collect and retain evidence. System logs need to be protected, because if the data can be modified or data in them deleted, their existence may create a false sense of security.
- Usually the 'Administrator' or 'root' user of the system has full access to the audit logs, which also contains the audit data of administrative activities. Hence, it is recommended to establish different power users with different role, instead of one super user account. The role of 'log- administrator' can be defined, which can be separated from other administrators. Access control of the audit logs list should be so designed that prevent unauthorized access or deletion of data
- In case, organization assigns a completely independent server (syslog server) to store all log data centrally. The administrative access of this syslog server should be kept separated from that of the hosts whose logs are being maintained in the central syslog server **[Control improvement (i)].**
- Symmetric key encryption available with standard encryption packages like OpenSSL, PGP etc may be used to encrypt the audit log, if felt necessary after risk assessment [**Control improvement(ii)**]

Assessment guidelines

Look at	Look for
• Record retention policy for Audit logs • Access controls on audit logs of different system • Logical and physical access control of the log server, if any	• Evidence of retention of audit logs as per the policy • Evidence of separate access right on log files • Evidence of use of standard encryption on audit log, if necessary

I.AL-5: TIME SYNCHRONIZATION OF INFORMATION SYSTEMS

Control: The clocks of all relevant information processing systems within an organization or security domain should be synchronized with an agreed accurate time source.

Control improvements:

(i) A clock linked to a radio time broadcast from a national atomic clock can be used as the master clock for logging systems

Implementation Guidelines :

- A network time protocol can be used to keep all of the servers in synchronization with the master clock.
- All the desktops, servers and network devices of the network should work with time-synchronization; this will ensure integrity of the time stamp of audit logs. The hosts should be enabled with Network Timing Protocol (NTP) which will synchronize the internal clocks of the hosts with the clock of an identified NTP server.
- In most of cases, a server is identified as NTP server and its clock is treated as reference clock of the organization. However, internal NTP server may further be synchronized with national /International reference clock.

Assessment guidelines

Look at	Look for
• Any device configured for providing master timing service • System configuration of the servers and network devices	• The relevant setting in NTP services conforming to the organization policy of having one master clock. • The setting reference clock of the NTP server

I.AL-6: RETENTION OF AUDIT RECORDS

Control: The organization should retain audit records for [*organization-defined time period*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Implementation Guidelines :

The retention period for audit logs depend on the organizational need in respect of legal, audit, and/or other operational purposes. Hence, there should be a management approval for different audit logs.

Assessment guidelines

Look at	Look for
• The documented policy for retention of audit records	• The evidences complying to the policies

I.SC-1: TRUSTED SERVICE

Control: The organization should adopt appropriate measure to ensure authenticity of the platform through which it disseminates information.

Implementation Guidelines :

- Digital certificate from an authorized agency establishes the identity of a person or entity.
- The most common use of certificates is for HTTPS-based web sites.
- A web browser validates that an SSL (Transport Layer Security) web server is authentic; so that the user can feel secure that the web site is who it claims to be
- HTTPS communication channel is encrypted; hence, the user also gains confidence that their interaction with the web site has lesser risk from eavesdroppers.
- This security is important for electronic commerce. In practice, a web site operator obtains a certificate by applying to a certificate provider with a certificate signing request.
- The certificate request is an electronic document that contains the web site name, contact email address, and company information.
- The certificate provider signs the request, thus producing a public certificate.
- This public certificate is served to any web browser that connects to the web site and proves to the web browser that the provider believes it has issued a certificate to the owner of the web site.
- Authenticity of information in electronic form can be ensured through use digital certificate obtained through PKI and installing the certificate with the application through which the information is disseminated.

Assessment guidelines	
Look at • The digital certificate used for "Trusted Service" • The site using the "digital certificate"	Look for • Authenticity of the Certification Authority • Content of the certificate, commensurable with the site • Implementation of the digital certificate used with the site giving trusted service.

I.SC-2: USE OF STRONG PROTOCOLS

Control: Clear text protocols should be avoided for transmission of the confidential data over internet.

Implementation Guidelines :

- The protocols like TELNET, FTP, and HTTP have inherent security weakness as they transmit data in clear text;
- Sensitive information like account password can be sniffed (by attacker sitting inside LAN) and may be misused for unauthorized access to the information system. Hence such protocol should be avoided and instead protocols like SSH, SFTP or HTTPS should be used where no clear text transmission is permitted.
- As bear minimum the authentication session or log in session should be protected through use of strong protocols SSH or SSL.

Assessment guidelines

Look at	Look for
• Vulnerability assessment reports of the server and network devices • Authentication schemes used to access the server and network devices over network (other than console)	• Presence of weak protocol, if any (non-compliance) • The authentication session is not in clear text

I.SC-3: CONFIDENTIALITY OF STORED DATA

Control: The information system should enforce strong control mechanism to protect confidential data.

Implementation Guidelines :

- Different information system uses security mechanism to avoid leakage of confidential data (e.g. password). By default most operating systems stores the account passwords in the form of cryptographic hashes.
- In other cases, the organization should protect their confidential data through encryption, using algorithm from internationally accepted package like OpenSSL and key length of 128 bit (minimum).

Assessment guidelines

Look at	Look for
• Organizations' approach towards storage of confidential data in electronic form	• The mechanism used for protection of confidentiality of the stored data • The algorithm and key length used for encryption of the stored data are complying with the implementation guidance.

I.SI-1: SYSTEM INTEGRITY

Control: The organization should adopt organization specific standards for secure configuration of the Operating System for its hosts. This includes servers, routers and desk tops. The organization specific standards can be drawn from International best practices and the same should be brought under document control system of the organization.

Control improvements:

(i) Periodic configuration audit on the Operating system of servers, desktops and network devices to ensure compliance with the organizational standards
(ii) Centralized enforcement and control of server and desk top policies

Implementation Guidelines :

- The default configuration of network devices and servers are not aimed towards robust security. Hence, they need to be hardened through modification of the configuration of their default state.
- The secure state may vary from one organization to other depending on the Security Policies adopted by them. The standards can be drawn from International best practices like www.cisecurty.org
- The organization should evolve secure configuration of their servers, desktops and network devices and test them before deployment, so that the necessary services of the organization and business activities are not affected by this hardening activity.
- Once tested the configurations should be accepted as standard secure configuration of the devices (for the organization)
- One can deploy secure configuration of the servers and desktops individually or through centrally managed systems, like Microsoft Active Directory Services **[Control improvement (ii)]**
- Network hosts are usually not brought under same directory services where servers and desktops are operating, hence, their secure configuration should be deployed separately.

Assessment guidelines

Look at	Look for
• The defined and approved 'standard system configuration' (hardening standard) for different Operating Systems used in the organization (for both servers and network devices).	• Evidences of the implementation of the standard configuration on the host.

I.SI-2: PROTECTION OF SYSTEM INTEGRITY

Control: The system integrity shall be protected through restriction of use of highest privileged accounts like (Root, Administrator) to the system to minimize the risk from system administrator's mistake.

Implementation Guidelines :

- As a security best practice, administrators should use their individual accounts for day to day system administration activities. The administrators' account should have necessary high privilege, commensurable with their role.
- The highest privileged accounts like 'administrator' or 'root' are necessary only with some specific cases and the same should be used only for those specific requirements only.

Assessment guidelines

Look at	Look for
• Accounts used by the administrators • Accounts available in the servers and network devices.	• Presence of accounts other than "administrator" or "root" in the systems which are used for system administrator. • The privileges associated with the accounts used for administration of the servers and network host.

I.SI-3: RESTRICTION IN REMOTE ADMINISTRATION

Control: The remote administration from a site beyond the physical security control of the organization should be strictly restricted and if at all the same is allowed, it should be conducted using secure communication mechanism.

Control improvements:

The remote administration shall be allowed only from the specific terminals/desk top in the LAN, The administration shall be allowed only from local console for critical systems

Implementation Guidelines :

- If remote administration from a site beyond the physical security control of the organization is allowed, the e area and scope of remote administration should be clearly defined and documented and the same should be approved by management
- The use of remote administration tools (like VNC or RDP or SSH) should be consistent with organizational policy and documented in the security plan for the information system.
- The organization should maintain records for all remote maintenance and administration activities [I.AL].
- The following other techniques controls should be considered for improving the security of remote administration:
  - encryption and decryption of communications
  - strong identification and authentication techniques[I.IA-2]
  - Disconnection of remote connection, if verification fails
- When remote administration is completed, the information system shall terminate all sessions and remote connections invoked during that activity.
- If password-based authentication is used to conduct remote administration and maintenance, on emergency need the organization changes the passwords following each remote maintenance service.
- Implementation guidance I.IA-2 to be used for authentication of the node used for remote administration[**Control improvement**]

Assessment guidelines

Look at	Look for
• The defined and approved scope of remote administration of the servers and network devices • Tools used for remote administration	• Evidence of termination of all live sessions on completion of remote administration • Logs for remote administration conducted

I.SI-4: PATCHING OF OS AND APPLICATION SOFTWARE

Control: The organization should adopt a policy on periodic review and application of necessary security patches issued by the respective vendors of the Operating Systems and Application Software.

Control improvements:

(i) The organization should verify the patches on a test bed before deployment

(ii) The organization should employ automated mechanisms to review the status of the authorized and applicable patches of the system

Implementation Guidelines :

- The organization should assign explicit responsibility to keep track of the patches, released times to time, by the respective vendors.
- The security patches related to the operating systems should be deployed
- An automatic mechanism for patch (authorized) deployment and review for the same for all servers and desk tops should be used (for example WUS service for Microsoft Systems) to ensure patch compliance **[Control improvement(ii)]**
- The organization may decide not to apply a security patches for the services which are not enabled on the devices. [I.SI-1].
- For critical systems, a system state backup should be taken before application of the patch to enable system roll back in the event of failure patch application.
- For mission critical services, the security patches, hot fixes etc should be reviewed and tested in a separate test bed before application to the live system. **[Control improvement(i)]**

Assessment guidelines

Look at	Look for
• Defined responsibility to keep track of the patches • Approach for approval of the patches • Review mechanism for deployment of patches • Identified critical system (if any), for which provision of roll back should be adopted.	• Test records of successful patches on test bed (if adopted) • Records of review of regular patch management

I.SI-5: CONTROL OF MALICIOUS SOFTWARE

Control: The organization shall adopt suitable controls to prevent and detect the introduction of malicious code.

Control improvements:

(i) Content filtering & download restriction
(ii) Restriction in use of removable media
(iii) Control of mobile codes

Implementation Guidelines :

Explanation:

- Software and information processing facilities are vulnerable to the introduction of malicious code, such as computer viruses, network worms, Trojan horses, and logic bombs. Users should be made aware of the dangers of malicious code.
- Managers should, where appropriate, introduce controls to prevent, detect, and remove malicious code.
- Desktops running with administrative privileges are more vulnerable to the malicious codes; hence, normal computing devices should not be used with administrative accounts.
- Servers should not be kept in logged –on condition
- The organization shall employ malicious code protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network.
- The desktops' anti-virus software should be properly configured to protect the system from infections from all possible interfaces like external devices (USB, CD, SD/micro-SD cards), LAN, Internet browsing, e-mail etc**.[Control improvement(i)&(ii)]**
- The signature of the malicious software shall be updated time to time through a managed process and the same should be reviewed regularly.
- The systems should be periodically scanned for possible infections.
- Normal users should not be allowed to install any additional software on the desktop of their own. Only software from trusted source should be installed by the system administrators.
- Browsing from the servers should be discouraged especially from File server, database servers.
- The desk top browsers should be configured to restrict the execution of un-trusted mobile codes like unsigned Web Applets, ActiveX codes.**[Control improvement(iii)]**

Assessment guidelines

Look at	Look for
• The anti-virus control in place • The privileges under which the desktops are commonly running	• Status of antivirus on sample machines • Review records in respect of proper functioning of antivirus control.

• Users' restrictions imposed in respect of installation of new software, use of freeware and use of removable devices etc. • Brower configuration in respect of restricted use of mobile codes	• Users' awareness level in respect of the threats of malicious codes.

I.SI-6: INTEGRITY OF DATA	
Control: The organization should adopt security mechanism to detect the loss of integrity of information.	
Implementation Guidelines : • The organization should adopt suitable security controls like hash/message digest (MD5, SHA-1, SHA2 etc.) and apply on the critical information like configuration file of the routers, firewalls, Security policy templates for servers and desktops and maintain snapshot of hashes of the same with proper access control. • Any changes in the hash value will indicate the loss of integrity of the corresponding information.	
Assessment guidelines	
Look at • Information /data on which where this control is made applicable • Access control extended on the message digests of critical information	Look for • Defined responsibility for this act.

O.SP-1: INFORMATION SECURITY POLICY

Control: Information security policy shall be approved by the top management and published and communicated to all concerned (employees and external parties) with information system.

Implementation Guidelines :

- The information security policy document should state the top management commitment specifying management intent, goal and principles of information security in line with business strategy and objectives and the same should be approved by the management
- The policy document should contain
    - Overall objectives, scope and importance of information security
    - A brief description of the security policies and practices relevant to information system including but not limited to the following:
        - Compliance to legislative , regulatory and contractual
        - Security education, training and awareness
        - Business continuity management
        - Consequences of information security policy violations
    - Responsibility of information security management including reporting information security incidents
    - Reference of the documents which may support security policy
- The security policy should be communicated to all level of users of the information system in a appropriate form which relevant, accessible and understandable
- In case the information security policy is distributed outside the boundary of the information system, care should be taken not to disclose the sensitive information

Assessment guidelines

Look at	Look for
• Information security policy document	• The document is approved by the management • The document is communicated to all level of users • The document is accessible and understood by all level of users • The document contains all relevant and important policies in brief • The responsibility of information security management has been addressed • In case the policy is distributed outside, and it contains sensitive information, the appropriate measures to prevent disclosure of sensitive

	information is taken

O.SP-2: OPERATIONAL PROCEDURE

Control: To ensure correct and secure operation of the information system, operating procedures shall be identified, documented, maintained and made available to the all users who need them

Implementation Guidelines :

- Operating procedure which are required to ensure correct and secure operation of information system should be appropriately identified and documented
- These should be treated as formal documents and should undergo change through formal change management
- These procedures procedure should be accessible to all level of users who need for correct and secure operation of information system
- The operating procedure should specify the detailed instruction of activities like
    - Processing and handling of information
    - Back up process
    - Handling error and exception conditions
    - Media handling
    - Mail handling
    - Equipment maintenance
    - Start-up and close down procedure
    - Management of confidential output
    - Any other procedure which is relevant for secure and correct operation
- The detailing and extent of the procedure should depend on the complexity of the information system, its size and requirements of the various users
- The responsibility of identifying the appropriate procedure and approval authority should be defined

Assessment guidelines

Look at	Look for
• Operating procedures under the scope of information system	• The operating procedures are appropriately documented, authorized and controlled • These are relevant and adequate and complete • The handling and management of, and compliance with documented procedures shall be checked

	• Availability of documented procedure for some of the important services like operation and management of network service, which is generally outsourced.

O.SP-3: SEGREGATION OF RESPONIBILITY	
Control: The procedure with responsibilities shall be defined in such as way that initiating of an event shall be separated from authorization.	

Implementation Guidelines :
• While defining and implementing any procedure for correct and secure operation of information system, care should be taken that no single person can access, use or modify information system without authorization. This type of segregation of responsibility would reduce vulnerability to user error and misuse of all kinds.
• Example of segregation of duties and responsibilities are:
  ○ Dividing the job between tow or more users
  ○ Use of two keys or passwords by separate users in sensitive area
• In small information system, where segregation can be difficult to implement, the principle should be applied as far as practicable with additional controls monitoring (O.SP-5: MONITORING AND REVIEW)	

Assessment guidelines	
Look at • Documented procedure and / or practiced procedure	Look for • Principle of segregation of responsibility has been defined as well as practiced for major activities • In case of small organization, where segregation is not possible to implement, addition monitoring has been implemented.

O.SP-4: ACCEPTABLE USAGE POLICY
Control: The usage policy of assets and services associated with the information system shall be defined and implemented.
Implementation Guidelines : • The usage policy of assets and services associated with the information system preferably in the form of "Dos and Don't" shall be defined

- All users including third parties should be aware on the usage policy and should be formally communicated to all of them
- All users should follow rules of acceptable usage policy
- The acceptable usage policy should include the usage policy of electronic mail, internet and mobile devices , and other assets and information as applicable

Assessment guidelines	
Look at • Usage policy • Records of usage of selective assets and services	Look for • The usage policy is adequate and understood by all level of users including 3rd party • The formal communication to al users • Compliance to the usage policy for selected assets and services

O.SP-5: MONITORING AND REVIEW

Control: Monitoring and review of policy, procedures and applicable controls shall be in place to , evaluate the effectiveness and identify area of improvement at defined frequency and in response to changes to the organizational and business , legal conditions or technical environment

Implementation Guidelines :

- The operating procedures and applicable control / security measure should be monitored by respective group who are responsible while policy and high level procedure should be reviewed by top management periodically.
- The review and monitoring should be at least on the following area:
    - The effectiveness of the policy/ procedure/ control
    - The cost and impact of controls on business efficiency.
    - Effect on changes to technology.
- The frequency of the monitoring / review should be :
    - Regular at a defined interval (e.g Log may be reviewed daily or once in a week, procedure may be reviewed once in six months)
    - In the event of significant security incidents.
    - On disclosure of new vulnerabilities
    - *After changes in the organizational or technical infrastructure* or legal conditions
- *The results of the monitoring / review should be maintained*
- In case, monitoring / reviews reveal deviation in policy, procedure and / or in security controls, the appropriate corrective and / or preventive actions should be taken to improve

Assessment guidelines	
Look at • Monitoring and review process and result	Look for • The monitoring and review process are effective i.e meet its defined objectives • The procedure exists to react to any incidents, new vulnerabilities or threat, changes in technology or organizational or legal conditions etc. • The adequacy for the periodicity of review/ monitoring wrt to overall risk situation • The corrective action / preventive action in case of deviation, exists and adequate • Plans for distributing updated policies / procedures and that all users are made ware of the changes

O.SO-1: SECURITY FRAMEWORK

Control: An information security organizational framework shall be established to initiate and control information security activities associated the information system and to ensure that

(i) Information security organization structure is established to plan, implement and independently review the security activities

(ii) Security objectives for the information system are identified and met

Adequate resources are provided and roles and responsibilities at various levels in security organizational structure are defined and approved

Control Improvements:

(i) The contacts with external security specialists / groups including relevant authorities shall be established for information security activities

Implementation Guidelines :

- The top management should establish security organization structure specifying roles and responsibility of security forum, each individual group including coordinator commonly known as CISO (Chief information security officer) , who will be responsible to plan, implement and review the security activities as given below:
  - Ensure the security goals are identified. meet the requirements of the information system and are integrated in relevant processes
  - formulate , review and approve information security the policy
  - Review the effectiveness of implementation

- Provide necessary resources
- Approve the specific roles and responsibilities across the organization
- Initiate plan and program to maintain security Awareness.
- Coordinate the implementation across the organization

- The security activities undertaken by security forum, each individual group including CISO should be maintained in form of minutes.
- The security organization should establish contacts with *special* interest groups or other specialist security forums and professional association to
  - Improve the knowledge about best practices
  - Stay up to date and relevant
  - Receive early warning
  - Provide suitable liaison points when dealing with information security incidents

Assessment guidelines	
Look at	Look for
• Minutes of forum / individual group • Top management directives and internal communication • Communication with special interest group	• Security needs are identified, adequately addressed and continuously reviewed in line with top management directives • The degree of authority / responsibility the forum and each group have • Minutes of the meeting are formally recorded and any action raised is tracked by a defined process • The periodicity of the meeting • Degree of communication with special interest group, its relevance and adequacy

O.SO-2: AUTHORIZATION OF INFORMATION SYSTEM

Control: The authorization process for introducing of new information system or information system facilities and its upgrades shall be defined and implemented in security organization framework.

Implementation Guidelines :

- New information system or information system facilities and its upgrades may lead to security risk; these should be controlled and approved and authorized and by appropriate level to ensure that new system / upgrades fits

into the security environment and complies with security policies and controls.

- Approval and authorization should be documented.
- New facilities should have appropriate user management authorization.
- New hardware, software should be checked to ensure they are in compliance with other system
- Authorization and necessary control should be clearly defined for use of personal/private computing system
- The authorization process should be integrated with change management process

Assessment guidelines	
Look at	Look for
• Authorization process of new system/ upgrades • Records of approval and authorization for new system/ upgrades	• The process of authorization is adequate and effective • The relevant records are maintained • Appropriate authority is defined and also implemented

O.PS-1: PERSONNEL SECUIRTY PROCEDURES

Control: A formal documented personnel security procedure that addresses purpose, scope coordination among various functions of the information system, roles and responsibilities of the employees, contractors and third party users, various controls applicable and its means of implementation and compliances shall be established.

Implementation Guidelines :

- The objective of a documented personnel security procedure is to establish a guideline about the general behavior of all personnel across the organization in context of Information security and to minimize the risks which are envisaged from human beings.
- The term personnel applies to all those who have direct/ indirect access to the Information /Information Processing facilities and it includes employees of the organization (permanent or employed under contractual agreements), persons providing any service on behalf of a service provider's organization, consultants, auditors, trainees, customers, visitors etc.
- The procedure should address issues :
    - Personnel Security policies
    - Responsibilities and liabilities of different functional roles regarding security measures like data protection, confidentiality, ethics, appropriate use of organization's equipments and facilities etc.
    - Implementation of personnel security policies and personnel Security related controls
- The documented procedure may have reference to Govt. orders, directives, and regulations etc. which are

applicable to employees as conditions of employment. It can also refer to other security policies, procedures of the organization.

Assessment guidelines	
Look at • Documented Personnel security procedure	Look for • Availability • Adequacy of the issues addressed • Responsibilities/liabilities defined

O.PS-2: SCREENING

Control: The screening on individual users (employee, contractor or third party) requiring access to information and information system shall be carried out before authorizing access.

Control Improvements:

(i) The basic screening of individual users shall include a check of curriculum vitae for completeness and accuracy and availability of satisfactory character reference
(ii) Other independent identity like passport, driving license shall be used for screening
(iii) The check of criminal records shall be carried out as a part of detailed screening
(iv) The credit checks and clearance from government body shall be required

Implementation Guidelines :

- Screening of personnel is important and can prevent selection of wrong persons
- Extent of screening process may depend on the position for which a person is being considered and the risk associated with the role due to its defined responsibilities and activities
- The verification process should be planned taking the applicable legal restrictions into consideration.
- The screening process shall be applicable for employees as well as service providers and third party users although those may be different in nature.
- Where screening of personnel is not under the control of the organization e.g. due to contract with an agency, the organization should clearly communicate the agency about its responsibilities for screening of personnel.

Assessment guidelines

Look at	Look for
• Documented Personnel security procedure • Records of screening	• screening method is defined and documented • Verification methods are adequate • Records of verification are available • Complies with the defined procedure • Decisions are commensurate with verification findings

O.PS-3: TERMS AND CONDITIONS OF THE EMPLOYMENT

Control: The individual user (employee, contractor and third party) shall agree and sign the terms and conditions of their employment contract, which shall state their and management responsibilities for information security.

Control Improvements:

(i) The agreement is required to be reviewed / updated periodically and as and when there is a change/transfer/ termination of responsibility of the user takes place

Implementation Guidelines :

- It is important that the organization identifies security and legal responsibilities of employee, contractor and third party regarding handling of information and use of information processing facilities in the organization.
- A brief account of those should be communicated to the employees, contractors and third party users as part of employment contract so that they are also aware of their responsibilities. Such responsibilities, appropriate to the nature of access they will have to the information systems of the organization, should be included in terms and conditions of employment.
- The terms and conditions should be agreed and signed by the employees, contractors and third party users.
- It is also important to specify that agreed responsibilities may extend to outside the organization's premises and outside normal working hours e.g. in case of home-working/ remote working.
- Applicability of the responsibilities included in the terms and conditions for a defined period even after end of the employment should also be considered, where appropriate.
- The terms and conditions should also include consequences of not complying with the agreed security and legal responsibilities.

Assessment guidelines

Look at	Look for
• Employment Contracts/agreements	• Terms and conditions of employment includes

	responsibilities for security • Responsibilities cover security relevant aspects of the job including responsibilities related to legal requirements (e.g. copyright, legal use of software), working outside the organization and beyond normal working hours • Actions in case of disregarding security responsibilities by employees are specified • Process for updating responsibilities in case of change in role

O.PS-4 CONFIDENTIALITY AGREEMENTS
Control: The confidentiality or non-disclosure agreement addressing the needs for protection of information system shall be signed by the individual user (employee, contractor and third party). **Control improvements:** (i) The requirements for confidentiality and non-disclosure agreements shall be reviewed periodically and when changes occurs that influence the requirements
Implementation Guidelines : • Personnel, be the employees, contractors or third party users and having access to sensitive information, may reveal information during or even after the employment. To make all personnel bind themselves legally to be refrained from such activities, the organization should get a confidentiality or non-disclosure agreement signed by the personnel before authorizing or allowing access. • The content of the agreement should be carefully decided. This arrangement may not prevent revealing information by personnel but signing an agreement by an individual put some kind of inhibition and the signed agreement becomes worth in legal combat. • This should be applicable for individual employees, contractor personnel and third party users (despite existence of any agreement between the organization and the contractor/third party agency).
Assessment guidelines

Look at	Look for
• Signed Non-disclosure agreement	• Signed agreements are available for employees, contractor and third party users • Content is relevant and adequate

O.PS-5: INFORMATION SECURITIES, AWARENESS, EDUCATION & TRAINING

Control: The individual user of the information system (employee and where relevant, contractor and third party) shall be provided with appropriate security awareness, training and education and regular updates on security policies and procedure

Control Improvements:

(i) The effectiveness of the training provided shall be evaluated

Implementation Guidelines :

- Many information security problems or incidents occur due to inadequate knowledge of users about security policies and procedures. The organization should organize security awareness training programmes for its employees and where relevant for its contractors and third party users.
- The training programmes may be general awareness training, management training or technical training intended for a specific target group.
  General awareness training may cover :
  - General concepts on Information security
  - Information security objectives, policies of the organization
  - Security Framework of the organization
  - Essential policies and procedures and their updates
  - Legal responsibilities e.g. use of legal software, ensuring copyright law etc.
  - Recognizing Information security problems and incidents and their reporting

Management Training may cover :
- Awareness on Information security
- Risk assessment
- Information security implementation
- Auditing.

Technical training may cover :
- Correct use of Information processing facilities e.g. selection of secure passwords, secured email use, protection from virus etc.
- Correct use of applications
- Role specific training on security e.g. for network administrators, system administrators, application developers etc.

- Security Awareness training may be introduced as a part of formal induction training programme in the organization. But organizing such training should an on-going process through periodic updates. Such training should be suitable and relevant to the person's role, responsibilities and skill.

• Records of training should be maintained.

Assessment guidelines	
Look at	Look for
• Documented Personnel security procedure • Training records	• Policy on Information security awareness exists • Type of training conducted – Internal or external • Subject and topics discussed • No. of participants • Training activities comply with policy

O.PS-6: DISCIPLINARY PROCESS

Control: A formal disciplinary process shall be established for personnel failing to comply with information security policies and procedures.

Implementation Guidelines :

- There should be a defined disciplinary process in place. Any non-compliance with security policies or procedures by personnel should be properly dealt.
- All personnel should be made aware about existence of the process and its details.

Assessment guidelines	
Look at	Look for
• Documented Personnel security procedure • Record of security incidents	• Existence of a defined disciplinary process • Criteria for disciplinary action • Awareness of personnel about the process • Incidents of security breach • Implementation of any disciplinary action

O.PS-7: TERMINATION PROCESS

Control: All employees, contractors and third party users shall return all the information assets in their possession and their access right to information and information system shall be removed upon termination/change of their employment, contract or agreement.

Control Improvements:

(i) Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned

Implementation Guidelines :

- There should be a formal termination process in the organization to ensure that all information system-related assets are returned and all access rights (Physical or logical) are withdrawn. Information system-related assets include mobile computing devices, portable storage media, keys, identification cards, access cards, software, manual, corporate documents etc.
- The process should be applicable for employees, contractors or third party users and upon exit due to retirement, transfer, expiry of employment, contract or agreement.
- Withdrawal of logical access right s to information systems and services may not be applicable in all situations. But its need should be taken into consideration in the termination process.

Assessment guidelines

Look at	Look for
• Termination Process • Record of termination	• The process is documented • Availability of records • Effective implementation of the documented process

O.PE-1: PHYSICAL & ENVIRONMENTAL PROTECTION POLICY & PROCEDURE

Control: A formal documented physical and environmental protection policy that addresses purpose, scope, , coordination among various activities/ functions associated with the information system, roles and responsibilities, various controls applicable and its means of implementation and compliances shall be established.

Implementation Guidelines :

- The physical and environmental protection policy and procedure should define the arrangement of protection of physical computer systems and related buildings and equipment from unauthorized access as well as from fire and other natural and environmental hazards.
- Extent of protection arrangement may vary depending on the assets reside in an area. Additional security measures are required to be in place to protect critical or sensitive systems, where required.
- Objective of physical security measures are not only the protect areas containing information and information processing hardware, but also locations of wiring used to connect different elements of the system, supporting services (such as electric power), backup media and any other elements required for the system's operation.

Assessment guidelines	
Look at	Look for
• Documented physical and environmental policy	• The policy is documented • Implementation issues of physical security are covered • Responsibility is defined • Monitoring/review of physical access is addressed

O.PE-2: PHYSICAL ACCESS PERIMETER

Control: Security perimeters shall be established to protect areas that contain information systems to prevent unauthorized physical access, damage and interference.

Implementation Guidelines :

- There should be clearly defined perimeters in the premises.
- No. of perimeters may be decided based on sensitivity of the information and information processing facilities contained in an area.
- The external perimeter of the building or site should be sound, of solid construction to prevent unauthorized break in entry. Doors and windows which are not used regularly should be adequately strong and protected.
- More than one perimeter may be devised and planned based on risk assessment. In setting up perimeters, the following arrangement may be considered :
    - Manned physical security arrangement at the main entrance to the building or site
    - A manned reception area or reception desk
    - Physical barriers inside the premises to separate areas hosting information and information systems of different sensitivity
- All fire doors should be equipped with arrangement of alarm, monitoring and as per established standard of fire safety arrangement.
- Multiple security perimeters provide more confidence in protection against security compromise over a single

perimeter protection arrangement.

Assessment guidelines	
Look at	Look for
• Physical & environmental Policy and Procedure • Perimeter controls	• Whether perimeter arrangement is defined • Nature of control • Controls are suitable and adequate to protect the assets accessible • Monitoring/ review arrangement • Possibility of circumventing the perimeter controls

O.PE-3: AUTHORIZATION OF PHYSICAL ACCESS

Control: A list of personnel with authorized access to the facilities where information system reside shall be maintained with authorization credentials.

Control Improvements:

(i) The access list and authorization credential shall be reviewed and approved by authorized person periodically (at least annually)

(ii) The authorization credential for all users to information system shall appropriately be selected

Implementation Guidelines :

- Physical access to areas where information systems resides is permitted to personnel based on policy of the organization. There should be a systematic process for authorizing physical access and issue of appropriate authorization credentials. The areas, where authorization for physical access is required, respective authorization authority and use of approved authorization credential should be identified. The authorization credentials may include badge, identification card, access control card etc.
- The list of authorized access should be reviewed periodically. There should be a process to remove the personnel from the list who no longer require access.

Assessment guidelines	
Look at	Look for
• Physical & Environmental Policy & Procedure • List of authorized access • Record of authorization	• Availability of Physical access policy/guidelines • Responsibility defined • Authority for approving and reviewing access is defined • Periodicity of reviewing access list is defined

• Record of Review of the list	• Availability of the list • Permitted access complies with the policy • Authorization is according to the requirement • Review done by defined authority and according to defined periodicity

O.PE-4: PHYSICAL ACCESS CONTROL

Control: All physical access points (including designated entry/exit points) to the facilities where information system resides shall be controlled and the individual access shall be granted after verification of access authorization. The strength of physical access control mechanism shall be commensurate with criticality of the facility and shall be determined through Risk Assessment.

Control Improvements:

(i) The access control logs shall be maintained for exceptions
(ii) All access logs shall be maintained

Implementation Guidelines :

- The benefit of control on the entry/exit points to facilities containing information systems is to ensure physical access to the facilities to authorized personnel only.
- The organization may use different means to establish the control ranging from manual control to electronic control. Manual control may be arrangement of lock & key, manned control for allowing entry only after verification of authorization and recording of entry details. Electronic control may be installation of proven secured technology-based devices at the doors e.g. biometric devices, access control card readers etc.
- Whatever means adopted by the organization, that should be based on risk assessment and appropriate for achieving the required level of security of the area where physical access is controlled.

Assessment guidelines

Look at	Look for
• Physical & Environmental Policy & Procedure • Record of access	• Controls are defined for employees, visitors , and contractors • Adequacy of the controls to restrict unauthorized entry • Availability of access logs for both successful access as well as unsuccessful access

	• Access/Authorization complies with the policy

O.PE-5: ACCESS CONTROL FOR DISPLAY MEDIUM

Control: The physical access to the information system device that display information shall be controlled to prevent unauthorized individual from observing the display output.

Implementation Guidelines :

There should be a policy in place to restrict personnel from leaving information system display devices containing sensitive information. Viewing such information by unauthorized personnel may lead to leakage of information.

The policy should be communicated to personnel working with sensitive information.

Technical measures may also be adopted to hide information on display devices after a certain period of inactivity with the device.

Assessment guidelines

Look at	Look for
• Physical & environmental Policy and Procedure	• Policy on access control for display medium • Awareness of personnel about the policy • Whether policy is complied with

O.PE-6: MONITORING PHYSICAL ACCESS

Control: The physical access to the information system shall be monitored to detect and respond to physical security incidents.

Control Improvements:

(i) The real-time physical intrusion alarm and surveillance equipment shall be monitored
(ii) The automated mechanism to recognize potential intrusion shall be employed to initiate appropriate response actions

Implementation Guidelines :

- It is important to make arrangement for periodic review of the physical access logs. It helps the organization to detect any occurrence of unauthorized access or any suspicious attempt of security violation.
- In case of detection of any successful unauthorized access or suspicious attempt of unauthorized access should be considered as a security incident and it should be treated according to security incident response procedure of the organization.
- Real time detection of any physical access violation can be achieved through continuous arrangement of monitoring. Automated alert generation may be considered to identify such situations.

Assessment guidelines	
Look at • Physical & environmental Policy and Procedure • Physical access log • Evidence of review	Look for • Whether review of physical access logs is addressed and responsibility for this action is defined. • Availability of physical access log • Complies with defined policy

O.PE-7: CONTROL OF VISITOR

Control: The physical access to the information system shall be granted only by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.

Control Improvements:

(i) The access records of the visitors shall be maintained
(ii) The visitors shall be escorted by the designated personnel and the visitor's activity, if required, shall be monitored

Implementation Guidelines :

- There should be defined guidelines for visitors' access inside the premises.
- If visitors are allowed access beyond designated public areas, there should be visible identification arrangement
- It is necessary to clearly define whether guidelines for visitors should be applicable for contractors when regular visits of contractors become necessary according to agreements.
- Visitors should be escorted.
- Visitor's records should be maintained.

Assessment guidelines	
Look at • Guidelines for visitors access • Record of visitors access	Look for • Availability of documented visitors guidelines • Adequacy of information maintained

O.PE-8: PROTECTION AGAINST FIRE

Control: Appropriate protection against fire shall be identified and applied. The information system shall be suitably placed in order to minimize such threat.

Control Improvements:

(i) The fire clearance from appropriate authority shall be taken
(ii) Appropriate fire suppression (e.g firefighting equipment) and detection (e.g smoke detector) mechanism shall be deployed

Implementation Guidelines :

- The organization should make appropriate arrangement for fire/smoke detection and firefighting. Fire detection and firefighting devices should be placed suitably.
- Automatic fire extinguishing arrangement may be installed in locations hosting critical information system resources where personnel are not present on continuous basis.
- As precautionary measures, storage of hazardous and combustible material should be avoided in locations close to secure areas.
- Fire detection and protection system should be compliant with applicable law and regulation.

Assessment guidelines	
Look at • Fire detection and protection system	Look for • Availability of arrangement • Adequacy of arrangement • Validity of the fire fighting elements • Verification record of expected functionalities

O.PE-9 : PROTECTION AGAINST ELECERICAL HAZARDS	
Control: Protection against damage from electrical hazards shall be designed and applied.	
Implementation Guidelines : • Electrical power distribution elements should be located at safe distances from information processing systems so that damage of IT infrastructure due to electrical hazards can be avoided. • Appropriate fire resistant materials (e.g. conduits) should be used for laying electrical power cables • Materials (e.g. switches, distribution box, MCB, wire etc.) used for electrical wiring should be of proper rating. • There shall be appropriate arrangement for cooling where excessive heat is generated during normal functioning of electrical equipments/devices (Electrical power stabilizers, regulators, UPS units).	
Assessment guidelines	
Look at • Electrical Power supply arrangement • Incident records	Look for • Availability of diagrams of power distribution • Incidents related to electrical hazards

O.PE-10: PROTECTION AGAINST OTHER EXTERNAL AND ENVIRONMENTAL THREAT
Control: Physical protection against damage from temperature, flood, earthquake, explosion, civil unrest and other form of natural and man-made disaster shall be designed and applied and the information system shall appropriately positioned to minimize such threat.
Implementation Guidelines : • The organization should make arrangement for protecting information processing facilities from different environmental threats. • Temperature at the locations where information processing facilities reside should be regularly monitored and maintained within an acceptable limit. • Locations for Information processing facilities and information resources should be carefully planned to avoid damage from flood, water logging, rampage arising from civil unrest etc. • Information systems should be protected from damage due to seepage of water resulting from broken plumbing line, rain or other sources.

Assessment guidelines	
Look at	Look for
• Location of Information processing facilities, storage areas	• Susceptibility to damage from environmental threats • Occurrence of any incident of damage from such threats

O.PE-11: WORKING IN SECURE AREAS

Control: Physical protection and guidelines for working in the areas where information system resides shall be designed and applied.

Implementation Guidelines :

- Information systems are made secured with arrangement of physical security perimeters, introducing different means of control for monitoring and restricting physical access. Extents of such controls are decided depending on the impact level of compromising such measures.
- Secure areas are those areas which contain large concentration of information system elements with higher level of impact than other areas e.g. server room, communications room or any other area involving sensitive work.
- This control is intended to provide an additional layer of physical security to the secure areas in organization.
- Organization should have documented guidelines for enhanced security arrangement of the secure areas
- The following guidelines should be considered in design and development of enhanced security arrangement :
    - Indication or display pointing to the location of the secure areas should be avoided
    - An additional physical perimeter and restricted entry control should be provided
    - Working of individuals alone in secure area should be avoided to prevent opportunities for malicious activities
    - Vacant secure area should be physically locked and equipped with fire extinguishing devices that activate automatically and notify activation
    - Use of photographic or video/audio recording devices in secure areas should be restricted without appropriate authorization

Assessment guidelines	
Look at	Look for
• Documented guideline for physical security of secure	• Availability of documented guideline

areas • Implemented controls	• Adequacy of the controls • Compliance with documented guideline

O.PE-12: SUPPORTING UTILITIES

Control: The information system shall be protected from power failure and other disruption caused by failure in supporting utilities.

Implementation Guidelines :

- Availability of uninterrupted electrical power supply and support utility services e.g. telecommunication services, air conditioning, water supply, sewage etc. is important to ensure functioning of information systems.
- Suitable power supply, as per requirement of equipment should be arranged.
- Arrangement of uninterruptible power supply (UPS) or generator to support continuous operation of equipment necessary for the critical operations for a maximum period of probable power cut should be made available
- Multiple feed for power supplies and alternate service provider for telecommunication service should be considered to avoid single point of failure.
- UPS/Generator and Support utilities should be regularly verified and maintained to ensure proper functioning and reduce risk of their malfunction or failure.
- Organization should arrange and maintain automatic emergency lighting that is activated in event of power failure to illuminate essential areas like emergency exits, evacuation paths etc.

Assessment guidelines

Look at	Look for
• Power supply support arrangement	• Availability of backup power supply source • Adequacy of backup capacity to support essential operations • Availability of multiple feed power supply and alternate telecommunication service • Availability of record related to inspection/maintenance of supporting utilities

O.PE-13: CABLING SECURITY

Control: Power and telecommunications cabling carrying data or supporting information services shall be protected

from interception or damage.

Control improvements:

(i) All cable runs shall be located under raised flooring and appropriately marked

(ii) Communications cabling raceways shall be separated from electrical line without any intersection as far as possible. In case of any intersection, proper shielding shall be used to protect electrical interferences

Implementation Guidelines :

- Power and telecommunication cables need special care as any damage or fault with those may lead to loss of availability of information system services.
- Power cables and communication cables should be segregated to avoid interference. They should not be exposed and easily accessible particularly in public areas.
- Communication cables running through public access areas should be protected with conduits to prevent risk of interception leading to loss of confidentiality.
- Communication cables connected to patch panels or equipment should be identifiable with suitable marking arrangement

Assessment guidelines	
Look at	Look for
• Cable laying arrangement	• Protection when routed between departments,/ buildings or through public access area • Segregation of power and communication cable • Proper harnessing and marking of network cables when connected to equipment/network switches/patch panels/termination points • Possibility of occurrence of handling error

O.PE-14: EQUIPMENT MAINTENANCE

Control: The information system shall be correctly maintained to ensure its continued availability and integrity.

Implementation Guidelines :

- Intent of this control is to prevent interruption of business operations and services due to sudden failure of computing and communications equipment.
- Organization should have control on all maintenance activities, whether performed on site or location external to organization

- Maintenance should be carried out in accordance with manufacturer's instructions and specifications
- Maintenance of any category, routine or repair should be carried out by authorized maintenance personnel
- In case of off-site repair of information system or information system components, the organization should remove all information from the associated storage media using approved procedures.
- There should be arrangement to check potentially impacted security controls to verify proper functioning of the controls after maintenance is performed on information system
- Record should be maintained of all reported faults and maintenance works.

Assessment guidelines	
Look at • Maintenance procedure • Record of maintenance	Look for • Availability of maintenance procedure • Adequacy of the procedure • Availability of records • Compliance to procedure • Maintenance carried out at external location and compliance of actions with procedure

O.PE-15: WORKING OFFSITE

Control: Wherever applicable, appropriate physical and environmental controls (application, infrastructure and/or operation & management) as identified through Risk Assessment shall be established to the information system while working at offsite location

Implementation Guidelines :

- While working at off-site location (outside the organization's premises), care should be taken to ensure protection of the information processing assets as well as business information contained in it.
- Appropriate measures in respect of physical and environmental protection, access control, back up, virus protection, encryption of stored information etc. should be considered.
- Organization should have documented policy/defined guideline in respect of working in offsite locations based on risk assessment.
- Working at off-site location should be authorized by management.

Assessment guidelines	
Look at	Look for

• Policy/guideline on off-site working	• Availability of documented guideline • Adequacy

O.PE-16: SECURE DISPOSAL OR RE-USE OF DEVICES

Control: All devices containing storage media shall be checked to ensure that any sensitive data and licensed software have been removed prior to disposal.

Control Improvements:

(i) Low label formatting shall be carried out prior to disposal of storage media
(ii) The sensitive data in the storage media shall be encrypted before its disposal
(iii) The storage media shall be physically destroyed before its disposal

Implementation Guidelines :

- Unless care is taken in disposal or re-use of equipment, information stored in the devices may be compromised. Organization should have a policy in respect of disposal and reuse of devices
- Whenever devises are disposed, may be upon being declared as unfit for use or as a result of organizational condemnation process, existence of any storage media in the device containing sensitive information or licensed software should be considered.
- The information in the storage media should be made non-retrievable before it is disposed.
- Actions to make the information non-retrievable may be done according to the organization policy.
- In case of reuse of devices e.g. due to change in ownership or custody, the similar action should be considered.
- Proven methodologies should be adopted for destruction of information instead of normal delete or format function
- Physical destruction of the storage media instead of destroying information may also be considered based on risk assessment
- Installed Licensed software in the equipment, when decided for disposal

Assessment guidelines

Look at	Look for
• Disposal and reuse policy • Record of disposal/reuse	• Availability of policy • Action for removal of information and licensed software are taken as per the policy • Use of proven methodology to make information

	non-retrievable

O.PE-17: DELIVERY AND REMOVAL

Control: The information system related items entering and exiting the facility shall be controlled and authorized. The access point shall be controlled and if possible, shall be isolated from the information system and media library to avoid unauthorized physical access. Appropriate records of those items entering or exiting shall be maintained

Implementation Guidelines :

- Delivery areas can introduce vulnerability to the organization. Organization should have adequate control in the delivery areas.
- The following guidelines can be considered for implementation of the control :
  - Delivery areas should be physically isolated and entry point to the delivery area should be separate from normal entry points
  - Entry to the delivery area from outside should be restricted to identified and authorized personnel.
  - Delivery points should be located outside so that delivery personnel are not required to be given access to the locations where information resources reside.
  - Incoming materials should be registered and moved to inside after inspection.
  - Movement of incoming or outgoing material from the delivery area to the main building/location of information systems and vice-versa should be done by identified and authorized personnel.

Assessment guidelines

Look at	Look for
• Delivery area	• Location • Its isolation from other working area/entry points • Restriction in accessing delivery area • Control in movement of personnel and items from delivery to other working areas and vice-versa

O.MS-1: MEDIA HANDLING PROCEDURE

Control: Appropriate procedure shall be established to protect removable media associated with the information

system during its life cycle.

Implementation Guidelines :

- Procedures should be established for handling, processing, storing, transmitting and disposal of information consistent with its classification.
- The procedure should consider the following:
  - Handling and labeling of all media including HDD, CD, flash drive, hard copy information
  - The restriction of access to prevent unauthorized access
  - Storage of media as per manufacturer's specification
  - Clear marking of all media
  - Authorization to remove the media from the organization and a record of such revoval

Assessment guidelines	
Look at	Look for
• Media handling procedure	• The procedure is adequate covering all types of media during full life cycle(handling, processing, storing, transmitting and disposal) and in place • Adequate protection has been taken for sensitive information (in all forms) in line with the classification scheme • Relevant records for authorization to release of such media • Access restriction in exception conditions like transmission through couriers

O.MS-2: CLASSIFICATION AND LABELING OF MEDIA

Control: The information contained in media shall be appropriately classified and labeled in terms of legal requirements, sensitivity and criticality to protect effectively during its life cycle.

Implementation Guidelines :

- The information contained in the media should be classified as per business requirements
- The classification should be based on sensitivity i.e based on confidentiality and/or criticality i.e based on availability and /or legal requirements i.e requirements based on integrity, availability and confidentiality
- The level of sensitivity ,(e.g confidential, internal and public) or level of Criticality (e.g critical , non-critical) should be defined
- All information contained in the media should be labeled appropriately. When physical labeling is not possible, electronic means of labeling should be used.
- The protection should be consistent with the classification

Assessment guidelines	
Look at	Look for
• Classification & labeling guidelines	• The classification and labeling guidelines is in place and consistent to the business needs • The grading of classification and labeling are consistent with the existing level of protections • All assets (information) are covered under classification and labeling • The classification and labeling scheme is readily accessible, understood by all users and regularly reviewed

O.MS-3: SECURE MEDIA STORAGE

Control: The media shall be stored in a safe and secure environment, in accordance with manufacturer specification.

Control Improvement:

(i) Fire proof cabinet shall be used to protect the media containing information

Implementation Guidelines :

- The media containing data presents serious vulnerability to loss of data and breaches of confidentiality. Adequate measures should be taken to store these media in safe manner (e.g locked almirah or cabinet) and secure environment (e.g to keep these media in the environment specified by the manufactures)
- Fire proof cabinet should be used to protect these media from risk of fire

Assessment guidelines	
Look at	Look for
• Procedure/ Practices to storing various media	• Measures to protect loss of data and / or breaches of confidentiality for the data contained in the media during storage • Appropriate physical and / or environmental protection as applicable has been taken • Fire proof cabinet is used to protect media when there is risk of fire and the availability of data is very important

O.MS-4: SECURE MEDIA DISPOSAL

Control: The media containing sensitive information shall be disposed of securely and safely when it is no longer required.

Control Improvement :

(i) Low label formatting shall be carried out prior to disposal of electronic storage media and shredding or incineration shall be done for other media
(ii) The sensitive data in the electronic storage media shall be encrypted before its disposal
(iii) The electronic storage media shall be physically destroyed before its disposal

Implementation Guidelines :

- Serious breaches of confidentiality may take place when any media containing sensitive data are not disposed securely and safely i.e without appropriate action in regard to the destruction of the information.
- The appropriate actions, depending on the impact to the organization, can be
    - Low level formatting of the electronic storage media and shredding or incineration for other media e.g paper media
    - The encryption of sensitive data in electronic storage media before its disposal
    - Destruction of media containing high sensitive information before its disposal
- A records of sensitive items should be maintained at the point of destruction

Assessment guidelines	
Look at • Disposal policy / procedure for various media and its implementation	Look for • General disposal arrangement in place • The responsibility to check the process of disposal particularly for most sensitive level of information • Disposal of media done by outsourced party and relevant risk has been identified • Relevant records, if any for media contained sensitive information at the point of destruction

O.CM-1: CONFIGURATION MANAGEMENT PROCEDURE

Control: A formal documented configuration management procedure shall be defined addressing purpose, scope, roles & responsibilities, coordination among various activities/ functions associated with the information system, various controls applicable and its means of implementation and compliances shall be established.

Implementation Guidelines :

- The formal configuration management procedure should address the following:
  - The scope covering hardware, software, information, services, documentation etc. with relevant information including applicable controls
  - Role & responsibilities for recording, controlling and managing configuration of the all information assets
  - Various activities / functions such as monitoring, verifying and auditing configuration data

Assessment guidelines	
Look at • Configuration management procedure and its implementation	Look for • The procedure is adequate and is in place • All type of assets are covered • Methodology used for recording, controlling and managing configuration data • Monitoring and verification records • Configuration audit data & audit frequaency

O.CM-2: CONFIGURATION BASELINING

Control: A current baseline configuration of the information system and its components shall be developed, documented and maintained.

Control Improvements:

(i) The automatic mechanism / tools shall be employed to maintain an up-to-date, complete, reliable, accurate and readily available configuration of the information system

Implementation Guidelines :

- A baseline configuration of the information system along with all its components should be available
- The baseline configuration should also provide relationship among various components and a well-defined and documented specification to which the information system is built
- The base line configuration should be maintained
- Any deviation from the baseline configuration, if any should be documented
- A suitable configuration management tool should be used to maintain to capture and maintain current, reliable, accurate configuration database

Assessment guidelines

Look at	Look for
• Baseline configuration policy and its implementation • Baseline configuration of various components • Usage of configuration tool	• Well defined and baseline specification of various components • The relevant data has been maintained • Any deviation from defined baseline configuration • In case of any configuration tool used, the same is able to capture and maintain current, reliable and accurate data – verification of configuration database

O.CM-3: CONFIGURATION CHANGE CONTROL

Control: The changes to the information system shall be controlled by the use of formal change control procedure.

Control Improvements:

(i) The automatic mechanism/ tools shall be employed to initiate changes/ change request, to notify the appropriate approval authority and to record the approval and implementation details

Implementation Guidelines :

- The changes to the information system including its components should be authorized, documented and controlled through the defined change management process. The configuration change control should include

the following steps :

- The systematic proposal for change to the information system, including upgrades and modifications
- Justification and impact analysis in regard to security issues
- Approval of the change for Implementation
- Test/evaluation
- Implementation of change
- Review after implementation

- Access privileges and physical and logical access restrictions associated with changes to the information system should be enforced as per defined policy.
- The tool should be used for medium and / or large information system to implement the change control workflow

Assessment guidelines	
Look at	Look for
• Configuration change control procedure and its implementation • Configuration change control records	• The change control procedure for configuration is adequate and is in place • All steps as mentioned in the procedure are followed for selected change control records

O.CM-4: MONITORING CONFIGURATION CHANGES

Control: The changes in configuration of the information system shall be monitored through configuration verification and audit processes.

Implementation Guidelines :

- The changes in configuration of the information and its constituent components should be monitored at each stage namely, prior to the change implementation, during implementation and post implementation. These may include the following :
  - Scope of change
  - Review of the impact analysis
  - Verification of security features of the information system whether the same are functioning correctly
  - Unauthorized changes , if any
  - Audit activities associated with configuration change to the information system

Assessment guidelines	
Look at	Look for

• Configuration policy & procedure • Monitoring and verification records • Configuration audit records	• Adherence to the policy • Aspects of monitoring as defined in the procedure • Assignment of Responsibility • Finding of monitoring and corrective and preventive actions in case of deviation • Audit plan , responsibility and frequency • Audit finding and corrective and preventive actions in case of deviation

O.CM-5: OPTIMUM CONFIGURATION

Control: The information system shall be configured to provide only essential capabilities and specifically prohibits and /or restricts the use of the defined functions, ports, protocols, and/or services. A list of prohibited and/or restricted functions, port, protocols etc. shall be defined and listed.

Control Improvements:

(i) The information system shall be reviewed at defined frequency to identify and eliminate unnecessary functions, ports, protocols, and/or services

Implementation Guidelines :

- The information system or its constituent components (e.g. technology products like firewall, router, and/or tools) should be configured with those functionalities / capabilities / services which are only essential. The configuration additional functionalities / capabilities / services may pose security threat. The configuration of essential functionalities / capabilities / services should be consistent with business & operational requirements.
- These should be authorized by appropriate authority and documented and enforced in all components of the information system.
- Any change in the configuration should be carried out through change control procedure.
- As preventive measure, the restricted and / or restricted functions, port, protocol, services etc. should be defined and listed to avoid any accidental usage.
- The configuration of the information system and its constituent should be reviewed at defined frequency (at least once in six months) to identify and eliminate unnecessary functions, ports, protocols, and/or services

Assessment guidelines

Look at	Look for
• Documented essential configuration of information system and its constituent components • List of prohibited / restricted functions, port, protocol, services • Review records	• Authorization by appropriate authority • In accordance with business and operational requirements • Consistent with best practice • The adequacy of prohibited / restricted functions, port, protocol, services and its authorization

	• Review frequency as per defined policy • Finding on unnecessary functions, ports, protocols, and/or services and corrective actions, if any

O.CM-6 INVENTROY OF INFORMATION SYSTEM COMPONENTS
Control: A current inventory of the component of the information system along with the ownership shall be developed, documented and maintained. **Control Improvements:** (i) The automatic mechanism / tools shall be employed to maintain an up-to-date, complete, reliable, accurate and readily available inventory of the information system
Implementation Guidelines : • The inventory of components of the information system should be necessary for the accountability and security reasons. Appropriate protection can only be properly applied to the information system and its subsequent components if the inventory of these assets is maintained with detailed information appropriate to security and accountability requirements. The relevant information may include type of asset, format, location, backup information, license information and business value. • In addition, ownership and information classification should be agreed and documented for each of the asset. Based on the information of the asset, its business value and its security classification and level of protection commensurate with the importance of the asset should be identified. • The inventory of the components of the information system should reflect the current state of the system and consistent with scope of the information system. The detailing of information associated with the inventory of assets should such that subject to tracking and reporting. An appropriate tool should be deployed (for medium / large information system) to maintain current , complete , reliable and accurate inventory of the information system.

Assessment guidelines	
Look at	Look for
• The inventory of the information system including the constituent component	• Consistent with scope of information system and adequate coverage of all type of assets • The detailing of information associated with the inventory is commensurate with defined policy and security requirements • Ownership and classification have been appropriate as indicated in the inventory • Is it effectively tracked and necessary information are recorded for disposal and by whom and when etc. • Inventory database is current and accurate

	• Responsibility for maintenance of inventory • In case of deployment of tool for inventory of assets, the inventory maintained • Protection mechanism for inventory to be checked, in case of computer or tool based inventory, what about the access control and backup. If paper based, where it is kept, how is it protected against loss, and, what happen , when the record is replaced and it retention • The asset inventory identifies the bare minimum information as defined policy

O.IM-1: INCIDENT MANAGEMENT PROCEDURES

Control: A formal incident response procedures that addresses purpose, scope, roles & responsibilities, various sub-processes such as incident reporting and notification, incident handling (investigation, response, recovery and lesson learned) and associated controls shall be documented and established.

Implementation Guidelines :

- Organization should have a formal incident response policy that defines what events are considered as incidents, organizational structure for incident response, roles and responsibilities and the incident reporting requirements.
- Based on the incident response policy, a formal procedure should be developed to delineate the specific actions, techniques, checklists, and forms to be used for reporting and responding to incidents.
- The Procedure should include determining appropriate priority for handling incidents based on the criticality of the affected resources and the current and potential technical effect of the incident.
- In addition to prioritization guidelines, there should be an escalation process for those instances when the incident response team fails to respond to an incident within the designated time.
- It should address all the associated controls of incident management

Assessment guidelines

Look at	Look for
• Incident response policy/procedure	• Availability of a formal documented policy/procedure • Adequacy of the issues addressed

O.IM-2 TRAINING ON INCIDENT RESPONSE

Control: The personnel shall be trained in the field of incident response with respect to the information system periodically (at least annually) in accordance with the roles and responsibility assigned

Control Improvements:

(i) The simulated events/drills shall be included in incident response training to facilitate effective response in crisis situation

Implementation Guidelines :

- Organization should have an identified team to respond to incidents. The members of the team should be trained and should have adequate technical and problem solving skill. Excellent teamwork, organizational, communication, and speaking skills are is also important as well.
- A team leader with adequate skill to assume oversight of and final responsibility for the quality of the technical work performed by the entire incident response team should be identified.
- There should be arrangement for periodic training for refreshing knowledge of the team members
- Record of training should be maintained

Assessment guidelines

Look at	Look for
• Management authorization for team • Training record of the team	• Availability • Training coverage of all the team members • Adequacy of training

O.IM-3: INCIDENT REPORTING

Control: The security incidents, events, weaknesses of information system shall be reported through appropriate management channels to relevant authority

Control Improvements:

(i) The automatic mechanism / tools to support reporting mechanism shall be implemented

Implementation Guidelines :

- The process of reporting of security incidents should be documented. The point of contact for incident reporting and means of reporting should be clearly defined.
- All employees, contractors and third part users should be aware of their responsibility for reporting incidents and the procedure for reporting

- Convenience of reporting means and availability of alternatives should be taken into consideration while deciding reporting procedure to make the reporting procedure effective
- Organization should provide training to the personnel to identify and recognize incidents (Ref. O.PS-5: INFORMATION SECURITIES, AWARENESS, EDUCATION & TRAINING)
- In addition to incidents, weaknesses and vulnerabilities in the information system should also be reported.

Assessment guidelines	
Look at	Look for
• Incident response policy/procedure • Awareness of personnel	• Incident reporting procedure is defined • Adequacy in defining point of contact, means of reporting • Awareness of responsibility about incident reporting, point of contact and procedure of reporting

O.IM-4: INCIDENT RESPONSE

Control: The incident response shall include detection, analysis, containment, eradication and recovery.

Control Improvements:

(i) The automatic mechanism / tools to support incident response shall be employed

Implementation Guidelines :

- There should be a defined process in place to respond to incidents. Identified incident response team should take actions according to the defined procedure. The process should include the activities - detection, analysis, containment, eradication and recovery
- The most challenging aspects of incident response process is detection. Detection is determining that an incident has occurred. Detection of incidents can be achieved through different means. Those may be detected through manual means, e.g. User reports. There may be incidents having covert signs that cannot be easily detected without automation. Automated detection capabilities include network-based and host-based intrusion detection systems (IDS), antivirus software, and log analyzers.
- When a potential incident is reported, the incident response team should work quickly to analyze and validate it, documenting each step taken. The team should rapidly perform an initial analysis to determine the incident's scope, attack methods, and targeted vulnerabilities. This analysis should provide enough information for the team to prioritize subsequent activities, including the containment of the incident. When in doubt, incident handlers should assume the worst until additional analyses indicate otherwise. The incident response team should maintain records about the status of incidents, along with other pertinent information.
- Containment is limiting an incident from spreading and causing further damage to resources. An essential part of

containment is decision making, such as shutting down a system, disconnecting it from the network, or disabling certain system functions. Containment strategies are decided based on the type of incident. The criteria for choosing the appropriate strategy should be documented clearly to facilitate quick and effective decision making.

- Eradication is eliminating components of an incident such as deleting malicious code and disabling breached user accounts. Eradication may be necessary after an incident has been contained. For some incidents, eradication is either unnecessary or is performed during recovery.
- In recovery, systems are restored to normal operation. It may also be necessary to harden the system for preventing similar incidents. Recovery may involve actions like :
    - Restoring systems from clean backups
    - Rebuilding systems from scratch;
    - Replacing compromised files with clean versions
    - Installing patches
    - Changing passwords
    - Tightening network perimeter security (e.g., firewall rule sets).

Assessment guidelines	
Look at	Look for
• Incident response procedure • Incident response record	• Incident response activity is addressed • Adequacy of definition • Practice as per defined procedure

O.IM-5: INCIDENT MONITORING

Control: The information security incident shall be tracked and documented on an ongoing basis by designated personnel.

Implementation Guidelines :

- Organizations should collect data on incidents. The data collected over time can be used for different purposes. For example, a study of incident characteristics over a period provides an overview of security weaknesses and threats in the organization, changes in incident trends etc. The data can also be used for risk assessment or performance measurement of the incident response team.
- Data collection should be carefully considered to make the process effective and beneficial to the organization. Collection of data that is actionable should be focused on. For example, an absolute numbers of incidents are less informative - understanding how they represent threats to and vulnerabilities of the business processes of the organization is what matters.

Assessment guidelines

Look at	Look for
• Incident response procedure • Record of monitoring	• Whether monitoring activity is defined • Record of monitoring is available • Adequacy of information • Analysis and effective use of information

O.IM-6 COLLECTION OF EVIDENCES
Control: The evidence shall be collected, retained and presented after an incident to conform the rules for evidence laid down in the relevant jurisdiction(s) when a follow-up action (disciplinary or legal) against a person or organization is required to be taken.
Implementation Guidelines : • The control is intended to focus on the process of collection of data to establish occurrence of an incident if consequence of an incident leads to a disciplinary/legal action. • It is not always obvious at the initial stage of an incident response that the incident will result in legal action. The incident response team primarily focuses on recovery as quickly as possible. So the in the process, collection of legally acceptable evidences are ignored. • The team members should be trained and skilled to realize contemplated legal action while handling incidents and necessary established procedure with all precautionary measures should be followed to avoid intentional or accidental destruction of evidences. • Organization may also seek expert advice in deciding evidence those are required to be collected and appropriate procedure for collection, preservation and presentation of evidences to make those acceptable in court.

Assessment guidelines	
Look at	Look for
• Incident response procedure	• Whether the control has been addressed • Adequacy of the process

O.SA-1: SYSTEM & SERVICE ACQUISITION & MAINTENANCE POLICY

Control: The policy on acquisition and maintenance of information system and its associated services shall be defined and established to ensure that the security requirements are identified and met during system development and maintenance life cycle.

Implementation Guidelines :

- The security requirements should be identified and taken into account for development of various applications, infra-structure and services. As a part of acquisition and maintenance policy, the initial analysis of the requirements needs to identify security issues and these are required to be specified along with functional requirements. The security requirements and controls introduced in the design stage are significantly cheaper to implement and maintain than those included during or after implementation.
- In case of ready product or service is purchased from the market, the security requirements should be specified in the contract of the suppliers. (0.SA-6 may be referred for further details)
- During maintenance phase, there may be need to enhance and/or modify the system and associated services, security requirements should not be comprised with the additional functionality.

Assessment guidelines

Look at	Look for
• System and service acquisition policy	• The policy is established and in place • The policy addresses the identification of security requirements for information system and services from the project stage. • The policy of acquisition when system / service acquired from outside – consistent with top security policy • Policy of acquisition during maintenance phase

O.SA-2: ACQUISITION & MAINTENANCE PROCESS

Control: The acquisition and maintenance process shall define and establish (i)Security needs and relevant controls (ii) Design and development process (iii) Testing and evaluation methodology (iv) Documentation.

Implementation Guidelines :

The acquisition and maintenance process of the information system including various application, infrastructure and services at least should follow the steps as given below:

- Security needs and relevant controls: The security need for the system under acquisition and maintenance should be identified based on the business requirements, legal & regulatory requirements and risk assessment. The corresponding security controls are selected to satisfy the security needs. These

are documented in software requirement specification.

- Design and development process: Security controls as identified in the requirement stage are detailed through design process. The implementation of these identified controls is carried out through development process. The deliverable of this process may be high level design & low level design document and implementation guidelines.
- Testing and evaluation methodology: The information system and its components should be tested once these are designed and implemented to ensure that the controls so implemented are adequately meets the security requirements. Test and evaluation methodology specify the test and evaluation approach in general (e.g white box testing , black box testing etc.) and test procedures in particular for various system based on security requirements. The testing process has been referred in detail in O.SA-04
- Documentation: These may include, but not limited to the following :
  - Requirement specification document
  - Design document (HLD, LLD, Implementation guidance etc.)
  - Test & evaluation approach and test result
  - User and administrator and installation guidance
  - Any other documents to meet specific requirements e.g legal, regulatory and statutory requirements

Some of the steps of the acquisition and maintenance process may be outsourced and managed through appropriate contracts. In case of any certified product to be considered under acquisition process, the acquisition process may be relaxed.

Assessment guidelines	
Look at	Look for
• Information system and /or its components and its acquisition / maintenance process • Requirement specification for selected system • HLD/LLD/ Implementation guidance • Test methodology & test procedure • Acquisition / maintenance process documentation • Outsourcing contracts	• The acquisition/ maintenance process is in place • Security requirements has been documented in SRS, the requirement specification doc is approved • The detailed design document including implementation guidance is available and adequate, complete • Test methodology and procedure are effective to cover verification of security requirements • All relevant documentation is available • In case of outsourcing of some processes, the contract with outsourcing partners addresses the adherence of these requirements

O.SA-3: CONFIGURATION MANAGEMENT OF INFORMATION SYSTEM	
Control: The configuration management of the information system under development shall follow the configuration management policy and procedure defined in "Configuration Management" (O.CM)	
Implementation Guidelines : • The information system and / or its components under development and associated documentation should be under configuration management to control changes to the system during development, tracks security flaws, ensure that the change are authorized in accordance with O.CM. • If the development process is outsourced, the configuration management of information system under development should be managed by outsourced partner and the contract should address accordingly.	
Assessment guidelines	
Look at • System and services acquisition policy • Configuration management & its plan • Acquisition contracts • Security flaw tracking records • System change authorization records • Other relevant documents or records	Look for • Configuration management process and its plan is consistent with system acquisition policy • In case of outsourced development, the contract is consistent with acquisition policy and addresses the requirement of configuration management • All the records on security flaw tracking records are available and necessary corrective actions are taken to rectify security flaw • All the changes are authorized by appropriate authority

O.SA-4: SECURITY TESTING OF INFROMATION SYSTEM
Control: The information system under development shall be tested adequately to ensure the security requirements and controls identified during requirement analysis have been implemented and working without any problem.

Implementation Guidelines :

- The security testing of information system and / or its components should be carried out to verify the correct functioning of security requirements and controls identified during requirement analysis.
- The test plan, test methodology and appropriate test cases should be developed to have systematic approach of security testing and adequate coverage of the requirements.
- The test result should be reviewed and approved by appropriate authority.

Assessment guidelines	
Look at	Look for
• Security requirement specification of information system and/or its components • Test plan ,test approach and test cases • Test result	• All security requirements are adequately tested i.e adequate coverage exists • Test plan and test approach is consistent with the policy • The test result is compliant with the requirements; if not further corrective action and its verification i.e 2nd cycle testing etc.

O.SA-5: TECHNICAL VULNERABILITY OF INFORMATION SYSTEM

Control: The risk of exposure of information system (s) under operation to potential technical vulnerability shall be periodically evaluated and appropriate actions as applicable, shall taken timely to mitigate the risk.

Implementation Guidelines :

- The information system (s) or its components in use should be evaluated periodically (at least once in a year) for its technical vulnerabilities.
- A current and complete inventory of information system (s) and its components with relevant information (asset ID, version no, current state of deployment, ownership etc) should be available as a part of configuration management to initiate the vulnerability assessment.
- The role and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching etc. should be defined and established.
- The vulnerability assessment should be integrated with the change management as with the change/ updating of information of the asset inventory, updating of relevant information resources which will be essential for assessment, should be carried out.
- A specific timeline should be defined to react notification of the potentially relevant vulnerability. The appropriate action should be taken in case a potential vulnerability is identified.

Assessment guidelines	
Look at • Vulnerability assessment process • Vulnerability assessment findings	Look for • Frequency of assessment and its compliance • Coverage of all the assets • Responsibility of the assessment • In case of detection of potential vulnerability, the corrective actions and its verification and independence of responsibility of those who carries assessment and who takes actions • The integration of change management and vulnerability process

O.SA-6: ADDRESSING SECUIRTIES IN 3RD PARTY AGREEMENT

Control: Agreement with third party and/ or outsourced party involving accessing, processing, communicating or managing the information system (or a part of it and /or the associated components) or adding product or service to the information system, shall cover all security requirements.

Implementation Guidelines :

- Risk to the information system (or a part of it and /or the associated components or adding products or services) should be identified when external party is employed to access, process or use or managing the system considering the following aspects:
  - Type of access (Physical/logical/network connectivity
  - Sensitivity of the information involved and criticality of business process
  - Protection of other information where access from external party have not been granted.
  - Authorization process
  - External party personnel
  - Controls employed by external parties.
  - Condition for continuation of external parties in case of an security incident
  - Legal regulatory and other contractual requirement
- The appropriate control s to migrate such risk should be also implemented before granting access.
- These controls/ security requirements should be addressed in the agreement with the external party to ensure that these are legally binding and complied. Some of the important issues are:
  - Protection of information assets from Malwares
  - Physical Protection of information assets
  - Provision for the transfer of personnel
  - Reporting structure and reporting format
  - Target level of services and unacceptable level of services.
  - Return / destruction of IT assets at the end of agreement period
  - Restriction of copying and disclosure

- Requirement for undergoing user's awareness training
- Legal regulatory and other contractual requirement including IPR
- Right to monitor , revoke access right
- Right to audit
- Service continuity issues

- The service details and delivery level should be mentioned in the agreement

Assessment guidelines	
Look at	Look for
• Risk assessment from external party (3rd party and outsourced party) • Sample agreement/contract with 3rd party	• Responsibility for reviewing risk assessment • Content of the agreement with 3rd party / outsourced party particularly employed for processing / managing information system and check all the relevant issues as mentioned in implementation guidelines • The relevant issues are consistent with the security requirements based on risk assessment and defined policy • Confidentiality agreement and background check of 3rd party person

O.SA-7: MANAGEMENT OF 3RD PARTY SECUIRTY & DELIVERY SERVICE

Control: The security controls, service definition and the delivery levels included in the third party agreement shall be implemented.

Control Improvements:

(i) The service performances of the third party shall be monitored regularly
(ii) The necessary changes, if required, in third party services shall also be incorporated based on monitoring result

Implementation Guidelines :

- The management of security and delivery service by third party includes the agreed security arrangement, service definition and aspect of service management.
- The controls / requirements as entered in third party agreement / contract (refer O.SA-7 also) shall be implemented and reviewed periodically (at least once in a year). The security problem, if any as reported by third party should also be reviewed.
- The service report produced by the third party should be reviewed and regular meeting should be arranged
- The service performance i.e delivery levels as agreed by third party should be periodically (quarterly /biannually / annually) should be monitored to check its adherence to the requirements of the agreement.

The service report should be reviewed

- The third party audit trails and records of security events should be reviewed.
- The problems arising out of monitoring and review should be resolved and appropriate actions should be taken.
- Process of managing changes to third party service needs to take account of
  - Enhancements to the current services offered
  - Development of any new applications and systems
  - Modification of organization's policies and procedures
  - New control to resolve information security incidents and to improve of security
- Implementing and reviewing authority should be defined as the responsibility ultimately belongs to the owner of the information system

Assessment guidelines	
Look at	Look for
• Third party agreement / Contract • Service report • Analysis of third party performance • Corrective action to resolve any problem • Change in agreement / contract in respect of service, system, security control	• The agreement is valid and complete (i.e contains all aspects of security requirements, service definition and service level) • Service reports are reviewed at defined periodicity, problems if any are resolved • Third party performance are monitored at defined interval and improvement suggestion, if any is available • In case of any problem, appropriate corrective actions are taken • How the changes in the agreement / contract in respect of service, system and security controls , if any, are taking place

BC-1: BUSINESS CONTINUITY POLICY AND PROCEDURES

Control: A managed process with business continuity policy and procedures shall be developed, documented and maintained for business continuity of the information system that addresses the information security requirements.

Implementation Guidelines :

- Business continuity management aims at managing risk to ensure that all time information system continue to function, at least, a pre-determined minimum level. The business continuity management process involves reducing the risk at an acceptable level and planning for the recovery of the business processes associated with information system when a risk materializes and disruption to the business occurs.
- A managed business continuity process should consist of the following phases:

- Initiating BCM: Policy setting , defining the scope and resource allocation and project planning are the important activities planned by top management in this phase
- Business impact analysis and risk assessment: Business Impact analysis identifies critical business processes and potential damages or loss that may caused as a result of a disruption to the critical business processes while risk assessment provides information on the likelihood that a disaster or service disruption will actually occur.
- Business continuity strategy: is a balance between the cost of risk reduction and recovery option to support the recovery of critical business processes with the agreed time scale. Based on the business requirements, the recovery option may be: do nothing, manual work around, reciprocal arrangement, gradual recovery, intermediate recovery (warm standby), Immediate recovery (hot standby)
- Implement standby arrangement: Recovery is based on series of standby arrangements like negotiating with third party for recovery facilities, standby accommodation, preparing and installing stand-by computers etc. Refer O.BC-6 , O.BC-7 and O.BC-8
- Develop recovery plan: include key detail such as data recovery point, a list of dependent system, nature of dependency and their data recovery points, System hardware & software requirements, configuration details etc.
- Implement risk reduction measures: include such as installation of UPS and backup power, fault tolerant system, offsite storage and achieving, RAID arrays and disk mirroring etc.
- Develop business continuity plan: documenting continuity plan and procedure, refer O.BC-2
- Testing and updating the plan: Review , assessment and re-assessment of plans, Refer O.BC-4 and O.BC-5
- Training: Training , education and awareness to all BCP members and general users, Refer O.BC-3

Assessment guidelines

Look at	Look for
• Business continuity management process • BCP key members & interview with them • Business continuity plan	• BCM is in place and whether it is being maintained and applied across the boundaries • Various activities like impact analysis & risk assessment, testing, training etc exist in BCM process • Documentation associated with the process • Scope and details of the plan meet business and security requirements • A Business continuity plan is available • Business continuity plan captures all phases

O.BC-2: BUSINESS CONTINUITY PLAN

Control: A business continuity plan for the information system addressing roles and responsibility, assigned Individual with contact information and activities associated with restoring the system after disruption or failure, shall be developed and implemented. Designated personnel shall review and approve the plan and distribute the copy of the plan to the key personnel.

Control Improvements:

(i) The business continuity plan of the information system shall be coordinated with other plan like Incident response plan, emergency action plan etc.

Implementation Guidelines :

- The business continuity plan should be the reference documents indicating BCM policy and procedures covering the various issues like scope, objectives, roles and responsibilities, critical business processes, impact analysis & risk assessment, recovery strategy with recovery timelines, risk mitigation, testing, re-assessment and training
- BCP also defines roles and responsibility of all key members and contacts details for various activities associated with recovery plan(s)
- The document should also describe a clear description of the circumstances under which they are activated.
- The BCP of the information system may be linked with other plans like incident response plan, emergency action plan, Change management plan and may be a part of the bigger plan of larger organization. In that case, the interface with other plans should be mentioned in the document.
- The business continuity plan should be reviewed at every stage and approved by the top management
- The copy of the BCP should be distributed to all key members and hard copy should also be available

Assessment guidelines

Look at	Look for

• Business continuity plan with
  ○ Impact analysis and risk assessment
  ○ Recovery plans
  ○ Testing process
  ○ Re-assessment process
  ○ Training process
	• Business continuity plan – approved and authorized by the top management and follows document control procedure
	• BCP is consistent with the identified business and security requirements
	• Timelines associated with the plans are sufficient for the business requirements and realistic
	• All possible disaster scenario have been considered
	• Responsibilities of key members are defined
	• All procedures defined in the plans are documented and implemented according to the implementation schedule
	• Testing and re-assessment process are consistent

	with defined policy • BCP training plan for key members and other employees exists

O.BC-3: BUSINESS CONTINUITY TRAINING

Control: The personnel shall be trained on business continuity plan of the information system in accordance with the roles and responsibility assigned periodically (at least annually)

Control Improvements:

(i) The simulated events on business continuity training shall be incorporated to facilitate effective response in crisis situation/ disaster scenario

Implementation Guidelines :

- Training and awareness i.e programme of briefing to all staff should be provided periodically (at least once in a year) on various issues like need for vigilance, on emergency procedures and on security guidelines & procedure
- Demonstration and drill on various disaster scenario (e.g fire drill, desktop walkthrough) should be carried out periodically and following a change
- Specific competence based training should be provided to key personnel and their groups who are responsible to implement and execute the recovery plans at disaster scenario
- To improve the effectiveness of training to ensure timely response in crisis situation / disaster scenario, training could be provided simulation disaster scenario

Assessment guidelines

Look at	Look for
• BCP related training records • Interview with BCP key members and general staff	• BCP training records are consistent with disaster scenario and recovery plan as defined in BCP document • Appropriate coverage of the training • Adequate awareness on BCP issues for general staff and BCP key members in specified domain • Improved effectiveness of BCP training in simulated disaster scenario, if any

O.BC-4: BUSINESS CONTINUITY PLAN TESTING AND EXERCISES

Control:

(i) The business continuity plan for the information system shall be tested and/or exercised periodically (at least annually) using test and/or exercise scenarios to determine the effectiveness and readiness to execute the plan

(ii) The test and/or exercise results of the business continuity plan shall be reviewed and necessary corrective actions shall be initiated

Control Improvements:

(i) The tests and/or exercises on business continuity plan shall be coordinated with other plans like Incident response plan, emergency action plan etc.

(ii) The tests / exercises of the business continuity plan shall also be executed at alternate processing site

Implementation Guidelines :

- Periodic testing of business continuity plan is essential to have assurance of satisfactory recovery when it is required
- The frequency of the testing should be carried out at least annually. A test plan with various test scenario at disaster condition and time frame and expected result should be maintained
- The variety of techniques should be used to ensure confidence on the recovery plan. Depending on the significance and importance, these may be table top testing, simulations, technical recovery testing, testing recovery at alternate site, tests on suppliers facilities and services and complete rehearsal
- The findings of the test result should be recorded and reviewed and in case of not meeting the expected value, the necessary corrective actions should be taken
- The testing of BCP should be integrated with other plans like incident response, emergency action plan, salvage plan etc

Assessment guidelines

Look at	Look for
• Business Continuity plan • BCP test plan • Test result • Corrective actions	• BCP test plan and schedule are consistent with the BCP policy • Coverage of all possible test scenario and test frequency as per defined policy • Test techniques used are appropriate and adequate • Finding of the test results consistent with the requirements / expected value • In case of any problems, these are analyzed and corrected

O.BC-5: BUSINESS CONTINUITY PLAN UPDATE

Control: The business continuity plan for the information system shall be reviewed periodically (at least annually) and revised to address changes in information system and associated environment including business and organizational (where the information system resides) requirements.

Implementation Guidelines :

- The business continuity plan for information system should be reviewed at least annual and the responsibility should be defined for regular review of each business plan.
- The business continuity management plan should be updated when there are
    - Acquisition of new equipment
    - Upgrading of system
    - Changes in
        - Key Personnel
        - Address and telephone number
        - Business strategy
        - Location, facilities and resources
        - Legislation
        - Contractors, suppliers and key customers
        - Processes
        - Risk (Operational and financial)
- Updating of BCP should be done through formal change management process

Assessment guidelines

Look at	Look for
• Business continuity plan • Review process of the BCP and review members • Formal change records for updating of BCP	• Review of BCP has been carried out at defined periodicity and designated authority • Review process considers the various issues which may lead to updating of BCP and availability of review records • Review members are aware on the various issues which lead to updating of BCP of • Any formal change records available corresponding to amendment / updating of BCP

O.BC-6: ALTERNATE STRORAGE SITES

Control: The alternate storage site shall be identified and storage of back-up information shall be shall be arranged based on business requirements (in terms of recovery time objectives [RTO] and recovery point objectives [RPO]

Control Improvements:

i) The alternate storage site shall be geographically separated from the primary storage site so that both sites are not likely to be affected by same/similar hazards
ii) The storage site shall be configured to ensure timely and effective recovery operation
iii) The alternate storage site shall be tested for possible disaster scenario

Implementation Guidelines :

- The identification and selection of alternate storage site are the strategic business decision.
- Three key objectives while planning alternate storage site :
  - Recovery point objectives (RPO) : The data loss tolerance of a business process or an organization in general
  - Recovery Time Objectives (RTO) : Down time tolerance of a business process or an organization in general.
  - Critical data point: The point to which data must be recovered following a system loss.
- Appropriate arrangement (e.g agreement) should be in place so that storage of information system backup to the alternate site is effected as per defined plan and recovery is possible under disaster scenario. The frequency of information system backups and transfer rate of backup information to the alternate site should be commensurate with RTO and RPO
- The alternate storage site should preferably be separated form primary storage site to ensure both sites are not affected by same and/or similar hazards at the same time
- The storage site should be configured with the primary site in such a way that recovery operation meets the specified RTO and RPO
- The relevant procedure should be in place to address alternate site and its recovery under disaster scenario
- The storage site should be tested for possible disaster scenario to provide an assurance that it would work satisfactorily at disaster scenario.

Assessment guidelines

Look at	Look for
• Business Continuity plan • Procedure / policy addressing alternate storage site • Other relevant document like agreement with alternate site • Configuration data • Test results	• The alternate storage site is in place and agreement to support at disaster condition exists • The arrangement with alternate site is consistent with business requirements i.e RTO & RPO • The frequency of backups and transfer of data is consistent and realistic with business requirements • Location of alternate site is strategic one to ensure that the site is not likely to be affected by the same

	and similar type of hazards • The existing configuration of the alternate site is working satisfactorily to meet the business requirements • The test results of the storage site I in compliance with the expected value and in case there is nay problem found, necessary mitigation action has been taken.

O.BC-7: ALTERNATE PROCESSING SITES

Control: The alternate processing site shall be established to ensure the resumption of information system operations for critical business functions within specified period in terms of information shall be shall be arranged based on business requirements (in terms of recovery time objectives [RTO] and recovery point objectives [RPO]) when primary processing facilities are not available.

Control Improvements:

i) The alternate processing site shall be geographically separated from the primary storage site so that both sites are not likely to be affected by same/similar hazards
ii) The storage site shall be configured so that it is ready to be used as the operational site with minimum support
iii) The alternate storage site shall be tested for possible disaster scenario

Implementation Guidelines :

- The identification and selection of alternate processing site are the strategic business decision
- The alternate processing site is generally considered for **critical business functions**
- Three key objectives while planning alternate processing site :
    - Recovery point objectives (RPO) : The data loss tolerance of a critical business process or an organization in general
    - Recovery Time Objectives (RTO) : Down time tolerance of a critical business process or an organization in general.
    - Critical data point: The point to which critical data must be recovered following a system loss**.**
- Appropriate arrangement (e.g agreement) should be in place so that the resumption of information system operations for critical business functions is effected as per defined plan and timelines.
- The alternate processing site should preferably be separated from primary processing site to ensure both sites are not affected by same and/or similar hazards at the same time
- The alternate processing site should be configured with the primary site to support the minimum required information system operational capability and is ready to use as the operational site .
- The relevant procedure should be in place to address alternate processing site and its recovery under disaster scenario for critical functions
- The alternate processing site should be tested for possible disaster scenario to provide an assurance that it would

work satisfactorily at disaster scenario.

Assessment guidelines	
Look at	Look for
• Business Continuity plan • Procedure / policy addressing alternate processing site • Other relevant document like agreement with alternate processing site • Configuration data • Test results	• The alternate processing site is in place and agreement to support at disaster condition exists • The arrangement with alternate processing site is consistent with business requirements i.e RTO & RPO • Location of alternate processing site is strategic one to ensure that the site is not likely to be affected by the same and similar type of hazards • The existing configuration of the alternate processing site is working satisfactorily to meet the business requirements • The test results of the storage site in compliance with the expected value and in case there is nay problem found, necessary mitigation action has been taken.

O.BC-8: INFORMATION SYTEM BACKUP & RECOVERY

Control: Bach-up of information (user-level and system- level information) and software contained in the information system shall be taken at defined frequency and protected at storage location.

Control Improvements:

i) The back-up information shall be tested at a specified frequency in accordance with agreed back-up policy to verify media reliability and information integrity
ii) The backup information shall be selectively used in the restoration of information system functions as a part of contingency plan testing
iii) The backup copies of the operating system and other critical information system software shall be stored in a separate facility or in a fire-proof container that is not collocated with the operational software
iv) The system backup information shall be protected from unauthorized modification

Implementation Guidelines :

- The primary objective of the backup operation is to ensure availability of essential information, data and software in disaster scenario and /or media failure
- A back up policy and associated procedure if required should be defined
- The scope of backup information (user level and system level) should be defined

- The extent (full, differential etc) and frequency of backup should be based on business and security requirements and criticality of the information. Frequency of back up at alternate storage site depends on RTO and RPO
- Backup information should be given appropriate level of physical and environmental protection consistent with the standards applied to the main site. The back up of critical information system and operating system should preferably be stored in separate place and / or kept in a fire proof cabinet. The fire-proof cabinet used for keeping back up data should preferably be place other that operational area.
- Back up information should be regularly tested (e.g quarterly for small and medium information system and monthly for large information system) to check the information is available at emergency situation. The objective is to check the reliability of the media (mostly depends on manufacturer's specification) and integrity of the data
- The back up data should be used on sample basis during contingency testing (as a part of BCP testing) to provide better assurance
- The appropriate mechanism (e.g digital signature, cryptographic hashes) should be used to protect the integrity of the back up information.
- The retention and archival of back up information should be consistent with business policy and legal requirements

Assessment guidelines

Look at	Look for
• Back up policy and procedure and practices • Back up log • Back up test result and /or log	• Back up policy / procedure and practice is in place and consistence with business requirements • Scope and frequency as per defined policy • Frequency of backup testing as per defined policy and effectiveness of data restoration process, any records available • Testing of back up media to ensure it is working properly or as per manufacturer' spec. • Back up storage site is adequately protected and the protection is in consistent with primary site • Fire proof cabinet is in place and it is not in the same operational area • Appropriate mechanism is used to protect integrity of the back up information • Usage of back up data in business continuity process on ample basis and result is in compliance with defined policy • Corrective actions taken / proposed when back up fails • The retention and archival of back up data meets the business requirement and legal requirement, if applicable

O.CO-1: COMPLIANCE TO SECURITY POLICIES AND PROCEDURES

Control: A compliance process shall be established to implement and improve information security.

Control Improvements:

i) The process of compliance shall be assessed by independent certification agent

Implementation Guidelines :

- The Information system should be audited to verify all applicable security policies, procedures, practices and controls are adequate, implemented and effective. The audit process ensures that the information system complies applicable security requirements
- The frequency of the audit should be at least once in year, however, more audit can be carried out to meet business requirements and contractual requirements. The frequency of the audit should be consistent with risk, criticality of the information, changes in the technology and any other factors which impact the information system.
- Audit principles should be based on the requirements of ISO 19011 i.e audit plan/ schedule, audit observation report and non-compliance report should be maintained. Auditor should be trained , knowledgeable and independent
- Responsibility for managing audit should be defined
- The corrective actions should be taken when non-conformity is found in the system
- The audit should ensure the improvement of the security system
- The compliance audit of information system for security should be planned by third party certification body to have better assurance

Assessment guidelines	
Look at • Security policy, procedures and practices • Audit plan • Audit observation • Compliance and non-compliance report • List of auditors and their training records • Corrective actions	Look for • The compliance audit is in place and conducted as per defined frequency and audit plan • Responsibility to mange audit is defined • The frequency is consistent with the risk, criticality etc. • Audit observation report is maintained and ensures all areas / controls / activities have been audited • Non-compliance report is available and corrective actions are verified to check the compliance and improvements • Auditors are competent and independence is maintained • In case of third party certification, the status of the non-compliance observed by the third party auditors.

O.CO-2: LEGAL COMPLIANCE

Control: A compliance process shall be established to implement legal, statutory, regulatory and contractual requirements during design, operation, use and management of information system.

Control Improvements:

i) The process of compliance shall be assessed by independent third party agent

Implementation Guidelines :

- All legal , statutory , regulatory and contractual requirements associated with the information system should be identified
- Once the legal , statutory , regulatory and contractual requirements are identified, these should be transformed into security requirements in perspective of information system i.e confidentiality, availability and integrity requirements of information which are required to be implemented in the information system
- The legal compliance audit should be performed by the legal experts
- The frequency of the audit should be at least once in year, however, more audit can be carried out to meet business requirements and contractual requirements
- The legal compliance report should be available and maintained
- The responsibility for managing the legal compliance should be defined
- The corrective actions should be taken when non-conformity is found in the legal compliance audit
- The legal compliance audit on information system should be carried out by third party agency to have better assurance and /or to adhere to the government directives, if any.

Assessment guidelines

Look at	Look for
• Legal compliance policy • Compliance and non-compliance report • Corrective actions , if any	• The legal compliance audit is in place and conducted as per defined frequency • Responsibility to mange audit is defined • The frequency is consistent with the risk, criticality and prevailing norms etc. • Legal compliance report is complete and done by the expert • In case of non-compliance, any corrective action pending • In case of 3rd party agency audit, any pending issues

Annexure-1: Mapping between various relevant documents and standards

Table 1: Mapping of Application Controls (GD 200) with GD 201, GD 202, GD 203, NIST 800-53 & ISO 27001 (Annexure Controls)

Family	Low Impact Baseline	Medium Impact Baseline	High Impact Baseline	Addl. Control (through RA)	NIST SP 800-53	ISO/IEC 27001 (Annexure Controls)
A.IA-1: USER IDENTIFICATION AND AUTHENTICATION	☑	☑	☑, (i)	(ii)	IA-2	--
A.IA-2: AUTHENTICATION HINT	☑	☑	☑	x	IA-6	--
A.IA-3: HANDLING OF AUTHENTICATION FAILURE	X	☑	☑	(i)	AC-7	--
A.IA-4: ENFORCING USE OF QUALITY AUTHENTICATION SECRET	X	☑, (i)	☑, (i)	(ii), (iii)	--	--
A.IA-5: GENERATING QUALITY AUTHENTICATION SECRET	☑	☑	☑	x	--	--
A.AC-1: SYSTEM ACCESS NOTIFICATION	☑	☑	☑	x	AC-8	--
A.AC-2: ACCESS ENFORCEMENT	☑	☑	☑	(i)	AC-3	A.11.6.1
A.AC-3: NOTIFICATION OF PREVIOUS LOGON	X	X	☑	x	AC-9	--
A.AC-4: CONTROL OF CONCURRENT SESSIONS	X	X	X	☑	AC-10	--
A.AC-5: AUTHENTICITY of COMMUNICATION SESSIONS	X	☑	☑	x	SC-23	--
A.AC-6: AUTOMATIC SESSION TERMINATION	X	☑	☑	(i)	AC-12	A.11.5.5
A.AC-7: AUTHENTICATION OF CONNECTING EQUIPMENT	X	X	X	☑	IA-3	--
A.AC-8: ACCESS LOG	X	☑	☑	x	--	A.10.10.1, A.10.10.4

Family	Low Impact Baseline	Medium Impact Baseline	High Impact Baseline	Addl. Control (through RA)	NIST SP 800-53	ISO/IEC 27001 (Annexure Controls)
A.AC-9: ACCESS TIME RESTRICTION	X	X	x	☑	--	A.11.5.6
A.AC-10: ENFORCING DATA INPUT BY HUMAN (CAPTCHA)	x	x	x	☑	--	--
A.DH-1: INPUT DATA VALIDATION	☑	☑	☑	x	--	A.12.2.1
A.DH-2: PROTECTION OF TRANSMITTED DATA	X	☑	☑	(i)	SC-8, SC-9	A.12.2.3, A. 10.9.1, A.10.9.2
A.DH-3: APPLICATION PARTITIONING	X	X	☑	x	SC-2	A.11.6.2
A.DH-4: ERROR HANDLING	☑	☑	☑	x	SI-11	A.12.2.4 A.12.5.4

Table 2: Mapping of Infrastructure Controls (GD 200) with GD 201, GD 202, GD 203, NIST 800-53 & ISO 27001 (Annexure Controls)

Family	Low Impact Baseline	Medium Impact Baseline	High Impact Baseline	Addl. Control (through RA)	NIST SP 800-53	ISO/IEC 27001 (Annexure Controls)
I.IA-1: USER IDENTIFICATION AND AUTHENTICATION	☑	☑	☑, (i)	(ii)	IA-2	A 11.5.2
I.IA-2: NODE AUTHENTICATION FOR REMOTE ADMINISTRATION OF NETWORK DEVICES AND SERVERS	x	x	x	☑	IA-3	A 11.4.3
I.IA-3: MANAGEMENT OF IDENTIFIER	x	☑	☑	x	IA-4	A 11.2.1
I.IA-4: SPECIFICATION OF AUTHENTICATOR	☑,	☑	☑, (i)	(ii)	IA-5	A 11.5.3
I.IA-5: MANAGEMENT OF AUTHENTICATOR	☑	☑, (i)	☑, (i), (ii)	x	IA-5	A 11.5.3
I.IA-6: AUTHENTICATION FOR EXTERNAL CONNECTION	☑	☑, (i)	☑, (i), (ii)	(iii),(iv),(v), (vi)	AC-17	A 11.4.2 A.11.7.2

Family	Low Impact Baseline	Medium Impact Baseline	High Impact Baseline	Addl. Control (through RA)	NIST SP 800-53	ISO/IEC 27001 (Annexure Controls)
I.IA-7: USER REGISTRATION AND DEREGISTRATION	☑	☑, (i),(ii)	☑, (i), (ii)	x	--	A 11.2.1 A 11.2.2 A 11.2.3
I.AC-1: ACCESS CONTROL POLICY	☑	☑	☑, (i)	x	AC-1	A 11.1.1 A.11.4.1 A.11.4.4 A.11.5.4 A.12.4.2 A.12.4.3 A.15.3.2
I.AC-2: ACCOUNT MANGEMENT	☑	☑	☑, (i)	(ii), (iii)	AC-2	A 11.3.2
I.AC-3: ACCESS ENFORCEMENT	☑	☑, (i), (ii)	☑, (i), (ii), (iii)	(iv)	AC-3	A 11.4.5
I.AC-4: SEGREGATION OF DUTIES	☑	☑	☑,(i)	(ii)	--	A 10.1.3
I.AC-5: NETWORK SEGMENTATION	x	x	☑	(i)	--	A 11.4.5 A.10.1.4 A.10.6.1
I.AC-6: NETWORK ROUTING CONTROL	☑	☑	☑	(i) , (ii), (iii), (iv)	AC-4	A 11.4.7 A.10.6.1
I.AC-7: NETWORK CONNECTION CONTROL	x	☑	☑, (i)	x	--	A 11.5.6 A.10.6.1 A.11.4.6
I.AC-8: SECURE LOG-ON PROCESS	☑	☑, (i)	☑, (i), (ii),(iii)	(iv),(v),(vi)	AC-7, AC-8, AC-9, AC-10, AC-11, AC-12	A 11.5.1
I.AC-9: WIRELESS ACCESS CONTROL	☑	☑	☑, (i)	(ii)	AC-18	--
I.AC-10: REVIEW OF ACCESS RIGHTS	x	☑	☑	(i)	AC-2, AC-13	A 11.2.4
I.AL-1: SELECTION OF AUDITABLE EVENT	☑	☑	☑, (i)	(ii)	AU-2	A 10.10.1 A.10.10.2
I.AL-2: AUDIT RECORD MANAGEMENT	☑	☑	☑, (i), (ii)	(iii)	AU-3	A10.10.1
I.AL-3: CAPACITY OF STORAGE FOR AUDIT LOGS	☑	☑	☑, (i)	x	AU-4	A 10.3.1
I.AL-4: PROTECTION OF AUDIT /LOG DATA	☑	☑	☑, (i)	(ii)	AU-9	A 10.10.3 A.15.1.3

Family	Low Impact Baseline	Medium Impact Baseline	High Impact Baseline	Addl. Control (through RA)	NIST SP 800-53	ISO/IEC 27001 (Annexure Controls)
I.AL-5: TIME SYNCHRONIZATION OF INFORMATION SYSTEMS	☑	☑	☑	(i)	AU-8	A 10.10.6
I.AL-6: RETENTION OF AUDIT RECORDS	☑	☑	☑	x	AU-11	A 10.10.1
I.SC-1: TRUSTED SERVICE	x	x	x	☑	--	--
I.SC-2: USE OF SRTONG PROTOCOLS	x	x	☑	x	--	--
I.SC-3: CONFIDENTIALITY OF STORED DATA	x	x	☑	x	--	A 10.7.3 A.10.7.4
I.SI-1: SYSTEM INTEGRITY	☑	☑, (i)	☑, (i)	(ii)	SI-1	A.10.9.3 A.11.5.4 A.12.2.2 A.15.3.2
I.SI-2: PROTECTION OF SYSTEM INTEGRITY	☑	☑	☑	x	--	A.11.5.5
I.SI-3: RESTRICTION IN REMOTE ADMINISTRATION	☑	☑	☑	(i)	--	A 11.6.1
I.SI-4: PATCHING OF OS AND APPLICATION SOFTWARE	☑	☑	☑, i	(ii)	SI-2	A 12.6.1
I.SI-5: CONTROL OF MALICIOUS SOFTWARE	☑	☑	☑, (i)	(ii), (iii)	SI-3	A 10.4.1 A.10.4.2
I.SI-6: INTEGRITY OF DATA	x	x	x	☑	--	A.10.9.3 A.12.2.2 A.12.2.4

Table 3: Mapping of Operations and Management Controls(GD 200) with GD 201, GD 202, GD 203, NIST 800-53 & ISO 27001 (Annexure Controls)

Family	Low Impact Baseline	Medium Impact Baseline	High Impact Baseline	Addl. Control (through RA)	NIST SP 800-53	ISO/IEC 27001(Annexure Controls)
O.SP-1: INFORMATION SECURITY POLICY	☑	☑	☑	x	AC-1, AT-1, CP-	A.5.1.1 A.12.3.1 A.12.3.2 A.15.1.6
O.SP-2: OPERATIONAL PROCEDURE	☑	☑	☑	x	AC-1,AT-1,AU-11,IA-1,IR-1,MA-1,PE-1,PL-1,PS-1,SI-1	A.10.1.1
O.SP-3: SEGREGATION OF RESPOSIBILITY	x	☑	☑	x	AC-5	A.10.1.3
O.SP-4: ACCEPTABLE USAGE POLICY	☑	☑	☑	x	AC-20, PL-4	A.7.1.3 A.10.8.4 A.11.3.2 A.11.7.1 A.15.1.5
O.SP-5: MONITORING AND REVIEW	☑	☑	☑	x	AU-6,CA-7,IR-5	A.5.1.2, A.15.2.1 A.15.3.1
O.SO-1: SECURITY FRAMEWORK	☑	☑	☑, (i)	x	PL-1.PL-2, PL-3,AT-5	A.6.1.1, A. 6.1.2, A.6.1.3, A.6.1.6 A.6.1.7 A.6.1.8
O.SO-2: AUTHORRIZATION OF INFORMATION SYSTEM	☑	☑	☑	x	CA-1	A.6.1.4
O.PS-1: PERSONNEL SECURITY POLICY AND PROCEDURES	☑	☑	☑	x	PS-1	A.8.1.1 A.8.2.1 A.15.1.1
O.PS-2: SCREENING	☑, (i)	☑, (i),(ii)	☑, (i),(ii), (iii)	(iv)	PS-2	A.8.1.2
O.PS-3: TERMS AND CONDITIONS OF THE EMPLOYMENT	☑	☑	☑	(i)	PS-3	A.8.1.3
O.PS-4: CONFIDENTIALITY AGREEMENTS	☑	☑	☑	(i)	PL-4, PS-6, SA-9	A.6.1.5
O.PS-5: INFORMATION SECURITY AWERNESS, EDUCATION & TRAINING	☑	☑	☑	(i)	AT-2,AT-3,AT-4	A.8.2.2
O.PS-6: DISCIPLINARY PROCESS	☑	☑	☑	x	PS-8	A.8.2.3
O.PS-7: TERMINATION PROCESS	☑	☑	☑	(i)	PS-5, AC-2	A.8.3.1 A. 8.3.2 A.8.3.3

Family	Low Impact Baseline	Medium Impact Baseline	High Impact Baseline	Addl. Control (through RA)	NIST SP 800-53	ISO/IEC 27001(Annexure Controls)
O.PE-1: PHYSICAL & ENVIORMENTAL PROTECTION POLICY & PROCEDURE	☑	☑	☑	x	PE-1	A.9.2.1
O.PE-2: PHYSICAL ACCESS PERMETER	☑	☑	☑	x	PE-3	A.9.1.1
O.PE-3: AUTHORIZATION OF PHYSICAL ACCESS	☑	☑	☑, (i)	(ii)	PE-2	A.9.1.2 A.9.1.6 A.11.4.4 A.9.1.3
O.PE-4: PHYSICAL ENTRY CONTROL	☑	☑	☑, (i)	(ii)	PE-3	A.9.1.2 A.9.1.3
O.PE-5: ACCESS CONTROL FOR DISPLAY MEDIUM	x	x	x	☑	PE-5	A.9.1.2 A.11.3.3
O.PE-6: MONITORING OF PHYSICAL ACCESS	x	x	☑	(i), (ii)	PE-6	A.9.1.2
O.PE-7: CONTROL OF VISITOR	x	☑	☑, (i)	(ii)	PE-7	A.9.1.2
O.PE-8: PROTECTION AGAINST FIRE	☑, (i)	☑, (i)	☑, (i)	(ii)	PE-13	A.9.1.4 A.9.1.3
O.PE:9: PROTECTION AGAINST ELECTRICAL HAZARDS	☑	☑	☑	x	---	---
O.PE-10: PROTECTION AGANST OTHER EXTERNAL & ENVIORMENTAL THREAT	x	x	x	☑	PE-13,PE-15	A.9.1.4 A.9.1.3
O.PE-11: WORKING IN SECURE AREAS	☑	☑	☑	x	PE-3	A.9.1.5
O.PE-12: SUPPORTING UTILITIES	☑	☑	☑	x	PE-9,PE-10, PE-11,PE-12	A.9.2.2
O.PE-13: CABLING SECURITY	x	☑, (I, (ii)	☑,(i), (ii)	x	PE-4,PE-9	A.9.2.3
O.PE-14: EQUIPMENT MAINTENANCE	☑	☑	☑	x	MA-1 TO MA-6	A.9.2.4
O.PE-15: WORKING OFFSITE	☑	☑	☑	x	PE-17	A.9.2.5
O.PE-16: SECURE DISPOSAL OR RE-USE OF EQUIPMENT	☑, (i)	☑, (i), (ii)	☑, (i), (ii), (iii)	x	MP-6	A.9.2.6
O.PE-17: DELIVERY AND REMOVAL	☑	☑	☑	x	PE-16	A.9.1.6, A.9.2.7

Family	Low Impact Baseline	Medium Impact Baseline	High Impact Baseline	Addl. Control (through RA)	NIST SP 800-53	ISO/IEC 27001(Annexure Controls)
O.MS-1: MEDIA HANDLING PROCEDURE	☑	☑	☑	x	MP-1 TO MP-5	A.7.2.1, A.7.2.2, A.10.7.1, A.10.7.2, A.10.7.3 A.10.8.3
O.MS-2: CLASSIFICATION AND LABELING OF MEDIA	x	☑	☑	x	RA-2 AC-16, MP-2, MP-3, SC-16	A.7.2.1, A.7.2.2
O.MS-3: SECURE MEDIA STORAGE	☑	☑	☑, (i)	x	MP-4	A.10.7.1
O.MS-4: SECURE MEDIA DISPOSAL	☑, (i)	☑, (i), (ii)	☑, (i), (ii), (iii)	x	MP-6	A.10.7.2
O.CM-1: CONFIGURATION MANAGEMENT PROCEDURE	☑	☑	☑	x	CM-1	A.12.4.1, A.12.5.1, A.12.4.3
O.CM-2: CONFIGURATION BASELINING	☑	☑	☑	(i)	CM-2	A.7.1.1, A.15.1.2
O.CM-3: CONFIGURATION CHANGE CONTROL	X	☑	☑, (i)	x	CM-3	A.10.1.2, A.12.4.1, A.12.5.1, A.12.5.2, A.12.5.3 A.12.4.3
O.CM-4: MONITORING CONFIGURATION CHANGES	X	X	X	☑	CM-4	A.10.1.2
O.CM-5: OPTIMUM CONFIGURATION	☑	☑	☑	(i)	CM-7	--
O.CM-6: INVENTORY OF INFORMATION SYSTEM COMPONENTS	☑	☑	☑	(i)	CM-8	A.7.1.1 A.7.1.2 A.15.1.2
O.IM-1: INCIDENT MANAGEMENT PROCEDURES	☑	☑	☑	x	IR-1	A.13.1.1 A.13.2.1
O.IM-2: TRAINING ON INCIDENT RESPONSE	☑	☑, (i)	☑, (i)	x	IR-2	A.13.1.1

Family	Low Impact Baseline	Medium Impact Baseline	High Impact Baseline	Addl. Control (through RA)	NIST SP 800-53	ISO/IEC 27001(Annexure Controls)
O.IM-3: INCIDENT REPORTING	☑	☑	☑, (i)	x	IR-6	A.13.1.1 A.13.1.2 A.10.10.5 A.6.1.6 A.6.2.2 A.6.2.3
O.IM-4: INCIDENT RESPONSE	☑	☑	☑, (i)	x	IR-4	--
O.IM-5: INCIDENT MONITORING	x	☑	☑, (i)	x	IR-5	A.13.2.2
O.IM-6: COLLECTION OF EVIDENCES	☑	☑	☑	x	AU-9, IR-4	A.13.2.3
O.SA-1: SYSTEM & SERVICE ACQUISTION AND MAINTENANCE POLICY	☑	☑	☑	x	SA-1	A.12.1.1 A.15.1.1
O.SA-2: ACQUISITION AND MAINTENANCE PROCESS	x	☑	☑	x	SA-3	A.12.1.1 A.10.3.2
O.SA-3: CONFIGURATION MANAGEMENT INFORMATION	x	x	☑	x	SA-10	A.12.5.1 A.12.5.2
O.SA-4: SECURITY TESTING OF INFORMATION SYSTEM	x	☑	☑	x	SA-11	A.10.3.2 A.12.5.1 A.12.5.2
O.SA-5: TECHNICAL VULNERABILITY OF INFORMATION SYSTEM	x	x	x	☑	RA-3	A.12.6.1 A.15.2.2
O.SA-6: ADDRESSING SECURITIES IN 3RD PARTY AGREEMENT	x	x	x	☑	PS-7	A.6.2.3 A.10.6.2 A.10.8.1 A.10.8.2 A.12.5.5
O.SA-7: MANAGEMENT OF 3RD PARTY SECURTY & SERVICE DELIVERY	☑	☑, (i), (ii)	☑, (i), (ii)	x	SA-9	A.10.2.1 A.10.2.2 A.10.2.3
O.BC-1: BUSINESS CONTINUITY POLICY AND PROCEDURES	☑	☑	☑	x	CP-1	A.5.1.1 A.10.4.1 A.14.1.1 A.14.1.2 A.14.1.3 A.15.1.1

Family	Low Impact Baseline	Medium Impact Baseline	High Impact Baseline	Addl. Control (through RA)	NIST SP 800-53	ISO/IEC 27001(Annexure Controls)
O.BC-2: BUSINESS CONTINUITY PLAN	☑	☑	☑, (i)	x	CP-2	A.10.4.1 A.10.8.5 A.14.1.3 A.14.1.4 A.13.1.1
O.BC-3: BUSINESS CONTINUITY TRAINING	x	☑	☑, (i)	x	CP-3	A.14.1.3 A.14.1.4
O.BC-4: BUSINESS CONTINUITY PLAN TESTING AND EXERCISES	☑	☑	☑, (i)	(ii)	CP-4	A.14.1.5
O.BC-5: BUSINESS CONTINUITY PLAN UPDATE	☑	☑	☑	x	CP-5	A.14.1.5
O.BC-6: ALTERNATE STORAGE SITE	x	☑, (i), (ii)	☑, (i), (ii)	(iii)	CP-6	A.10.5.1
O.BC-7: ALTERNATE PROCESSING SITE	x	☑, (i), (ii)	☑, (i), (ii)	(iii)	CP-7	A.14.1.4 A.14.1.5
O.BC-8: INFORMATION SYSTEM BACK UP AND RECOVERY	☑	☑, (i), (ii)	☑, (i), (ii), (iii)	(iv)	CP-9	A.10.5.1
O.CO-1: COMPLIANCE TO SECURITY POLICY AND PROCEDURES	☑	☑	☑, (i)	x	CA-2,CA-7	A.15.2.1
O.CO-2: LEGAL COMPLIANCE	☑	☑, (i)	☑, (i)	x	AC-1,AT-1,CA-1 1,IA-1,IR-1,MA-1,PE-1,PL-1,PS-1,SC1,SI-1,PL-5	A. 15.1.1

Table 4: Mapping of ISO 27001 (Annexure Controls) with GD 200 eSAFE Controls

ISO 27001: 2005 Clauses		GD 200 eSAFE Controls
A.5	**Security Policy**	
A.5.1	**Information Security Policy**	
A5.1.1	Information Security Policy document	O.SP-1: Information security policy O.BC-1: BUSINESS CONTINUITY POLICY AND PROCEDURES
A5.1.2	Review of the information security policy	O.SP-5: MONITORING AND REVIEW
A.6	**Organization of information security**	
A.6.1	**Internal organization**	
A.6.1.1	Management commitment to information security	O.SO-1: SECURITY FRAMEWORK
A.6.1.2	Information security coordination	O.SO-1: SECURITY FRAMEWORK
A.6.1.3	Allocation of information security responsibilities	O.SO-1: SECURITY FRAMEWORK
A.6.1.4	Authorization process for information processing facilities	O.SO-2: AUTHORRIZATION OF INFORMATION SYSTEM
A.6.1.5	Confidentiality agreements	O.PS-4: CONFIDENTIALITY AGREEMENTS
A.6.1.6	Contact with authorities	O.SO-1: SECURITY FRAMEWORK O.IM-3: INCIDENT REPORTING
A.6.1.7	Contact with special interest groups	O.SO-1: SECURITY FRAMEWORK
A.6.1.8	Independent review of information security	O.SO-1: SECURITY FRAMEWORK
A.6.2	**6.2 External parties**	
A.6.2.1	Identification of risks related to external parties	O.SA-6: ADDRESSING SECURITIES IN 3RD PARTY AGREEMENT
A.6.2.2	Addressing security when dealing with customers	O.IM-3: INCIDENT REPORTING
A.6.2.3	Addressing security in third party agreements	O.IM-3: INCIDENT REPORTING O.SA-6: ADDRESSING SECURITIES IN 3RD PARTY AGREEMENT
A.7	**Asset management**	
A.7.1	**Responsibility for assets**	

ISO 27001: 2005 Clauses		GD 200 eSAFE Controls
A.7.1.1	Inventory of assets	O.CM-2: CONFIGURATION BASELINING O.CM-6: INVENTORY OF INFORMATION SYSTEM COMPONENTS
A.7.1.2	Ownership of assets	O.CM-6: INVENTORY OF INFORMATION SYSTEM COMPONENTS
A.7.1.3	Acceptable use of assets	O.SP-4: ACCEPTABLE USAGE POLICY
A.7.2	**Information classification**	
A.7.2.1	Classification guidelines	O.MS-1: MEDIA HANDLING PROCEDURE O.MS-2: CLASSIFICATION AND LABELING OF MEDIA
A.7.2.2	Information labelling and handling	O.MS-1: MEDIA HANDLING PROCEDURE O.MS-2: CLASSIFICATION AND LABELING OF MEDIA
A.8	**Human resources security**	
A.8.1	**Prior to employment**	
A.8.1.1	Roles and responsibilities	O.PS-1: PERSONNEL SECURITY POLICY AND PROCEDURES
A.8.1.2	Screening	O.PS-2: SCREENING
A.8.1.3	Terms and conditions of Employment	O.PS-3: TERMS AND CONDITIONS OF THE EMPLOYMENT
A.8.2	**During employment**	
A.8.2.1	Management responsibilities	O.PS-1: PERSONNEL SECURITY POLICY AND PROCEDURES
A.8.2.2	Information security awareness, education and training	O.PS-5: INFORMATION SECURITY AWERNESS, EDUCATION & TRAINING
A.8.2.3	Disciplinary process	O.PS-6: DISCIPLINARY PROCESS
A.8.3	**Termination or change of employment**	
A.8.3.1	Termination responsibilities	O.PS-7: TERMINATION PROCESS
A.8.3.2	Return of assets	O.PS-7: TERMINATION PROCESS
A.8.3.3	Removal of access rights	O.PS-7: TERMINATION PROCESS
A.9	**Physical and environmental security**	
A.9.1	**Secure areas**	
A.9.1.1	Physical security perimeter	O.PE-2: PHYSICAL ACCESS PERMETER
A.9.1.2	Physical entry controls	O.PE-3: AUTHORIZATION OF PHYSICAL ACCESS O.PE-4: PHYSICAL ENTRY CONTROL O.PE-5: ACCESS CONTROL FOR DISPLAY MEDIUM O.PE-6: MONITORING OF PHYSICAL ACCESS O.PE-7: CONTROL OF VISITOR

ISO 27001: 2005 Clauses		GD 200 eSAFE Controls
A.9.1.3	Securing offices, rooms and facilities	O.PE-3: AUTHORIZATION OF PHYSICAL ACCESS O.PE-4: PHYSICAL ENTRY CONTROL O.PE-8: PROTECTION AGAINST FIRE O.PE-10: PROTECTION AGANST OTHER EXTERNAL & ENVIORMENTAL THREAT
A.9.1.4	Protecting against external and environmental threats	O.PE-8: PROTECTION AGAINST FIRE O.PE-10: PROTECTION AGANST OTHER EXTERNAL & ENVIORMENTAL THREAT
A.9.1.5	Working in secure areas	O.PE-11: WORKING IN SECURE AREAS
A.9.1.6	Public access, delivery and loading areas	O.PE-3: AUTHORIZATION OF PHYSICAL ACCESS O.PE-17: DELIVERY AND REMOVAL
A.9.2	**Equipment security**	
A.9.2.1	Equipment siting and protection	O.PE-1: PHYSICAL & ENVIORMENTAL PROTECTION POLICY & PROCEDURE
A.9.2.2	Supporting utilities	O.PE-12: SUPPORTING UTILITIES
A.9.2.3	Cabling security	O.PE-13: CABLING SECURITY
A.9.2.4	Equipment maintenance	O.PE-14: EQUIPMENT MAINTENANCE
A.9.2.5	Security of equipment off-premises	O.PE-15: ALTERNATE WORKS SITE
A.9.2.6	Secure disposal or re-use of equipment	O.PE-16: SECURE DISPOSAL OR RE-USE OF EQUIPMENT
A.9.2.7	Removal of property	O.PE-17: DELIVERY AND REMOVAL
A.10	**Communications and operations management**	
A.10.1	**Operational procedures and responsibilities**	
A.10.1.1	Documented operating procedures	O.SP-2: OPERATIONAL PROCEDURE
A.10.1.2	Change management	O.CM-3: CONFIGURATION CHANGE CONTROL O.CM-4: MONITORING CONFIGURATION CHANGES
A.10.1.3	Segregation of duties	I.AC-4: SEGREGATION OF DUTIES O.SP-3: SEGREGATION OF RESPOSIBILITY
A.10.1.4	Separation of development, test and operational facilities	I.AC-5: NETWORK SEGMENTATION
A.10.2	**Third party service delivery management**	
A.10.2.1	Service delivery	O.SA-7: MANAGEMENT OF 3RD PARTY SECURTY & SERVICE DELIVERY

ISO 27001: 2005 Clauses		GD 200 eSAFE Controls
A.10.2.2	Monitoring and review of third party services	O.SA-7: MANAGEMENT OF 3RD PARTY SECURTY & SERVICE DELIVERY
A.10.2.3	Managing changes to third party services	O.SA-7: MANAGEMENT OF 3RD PARTY SECURTY & SERVICE DELIVERY
A.10.3	**System planning and acceptance**	
A.10.3.1	Capacity planning	I.AL-3: CAPACITY OF STORAGE FOR AUDIT LOGS
A.10.3.2	System acceptance	O.SA-2: ACQUISITION AND MAINTENANCE PROCESS O.SA-4: SECURITY TESTING OF INFORMATION SYSTEM
A.10.4	**Protection against malicious and mobile code**	
A.10.4.1	Controls against malicious software	I.SI-5: CONTROL OF MALICIOUS SOFTWARE O.BC-1: BUSINESS CONTINUITY POLICY AND PROCEDURES O.BC-2: BUSINESS CONTINUITY PLAN
A.10.4.2	Controls against mobile code	I.SI-5: CONTROL OF MALICIOUS SOFTWARE
A.10.5	**Back-up**	
A.10.5.1	Information back-up	O.BC-6: ALTERNATE STORAGE SITE O.BC-8: INFORMATION SYSTEM BACK UP AND RECOVERY
A.10.6	**Network security management**	
A.10.6.1	Network controls	I.AC-7: NETWORK CONNECTION CONTROL
A.10.6.2	Security of network services	O.SA-6: ADDRESSING SECURITIES IN 3RD PARTY AGREEMENT
A.10.7	**Media handling and security**	
A.10.7.1	Management of removable computer media	O.MS-1: MEDIA HANDLING PROCEDURE O.MS-3: SECURE MEDIA STORAGE

ISO 27001: 2005 Clauses		GD 200 eSAFE Controls
A.10.7.2	Disposal of media	O.MS-1: MEDIA HANDLING PROCEDURE O.MS-4: SECURE MEDIA DISPOSAL
A.10.7.3	Information handling procedures	I.SC-3: CONFIDENTIALITY OF STORED DATA O.MS-1: MEDIA HANDLING PROCEDURE
A.10.7.4	Security of system documentation	I.SC-3: CONFIDENTIALITY OF STORED DATA
A.10.8	**Exchanges of information**	
A.10.8.1	Information exchange policies and procedures	O.SA-6: ADDRESSING SECURITIES IN 3RD PARTY AGREEMENT
A.10.8.2	Exchange agreements	O.SA-6: ADDRESSING SECURITIES IN 3RD PARTY AGREEMENT
A.10.8.3	Physical media in transit	O.MS-1: MEDIA HANDLING PROCEDURE
A.10.8.4	Electronic messaging	O.SP-4: ACCEPTABLE USAGE POLICY
A.10.8.5	Business information systems	O.BC-2: BUSINESS CONTINUITY PLAN
A.10.9	**Electronic commerce services**	
A.10.9.1	Electronic commerce	A.DH-2: PROTECTION OF TRANSMITTED DATA
A.10.9.2	On-line transactions	A.DH-2: PROTECTION OF TRANSMITTED DATA
A.10.9.3	Publicly available information	I.SI-1: SYSTEM INTEGRITY I.SI-6: INTEGRITY OF DATA
A.10.10	**Monitoring**	
A.10.10.1	Audit logging	A.AC-8: ACCESS LOG I.AL-1: SELECTION OF AUDITABLE EVENT I.AL-2: AUDIT RECORD MANAGEMENT I.AL-6: RETENTION OF AUDIT RECORDS

ISO 27001: 2005 Clauses		GD 200 eSAFE Controls
A.10.10.2	Monitoring system use	I.AL-1: SELECTION OF AUDITABLE EVENT
A.10.10.3	Protection of log information	I.AL-4: PROTECTION OF AUDIT /LOG DATA
A.10.10.4	Administrator and operator logs	A.AC-8: ACCESS LOG
A.10.10.5	Fault logging	O.IM-3: INCIDENT REPORTING
A.10.10.6	Clock synchronization	I.AL-5: TIME SYNCHRONIZATION OF INFORMATION SYSTEMS
A.11	**Access control**	
A.11.1	**Business requirement for access control**	
A.11.1.1	Access control policy	I.AC-1: ACCESS CONTROL POLICY
A.11.2	**User access management**	
A.11.2.1	User registration	I.IA-3: MANAGEMENT OF IDENTIFIER I.IA-7: USER REGISTRATION AND DEREGISTRATION
A.11.2.2	Privilege management	I.IA-7: USER REGISTRATION AND DEREGISTRATION
A.11.2.3	User password management	I.IA-7: USER REGISTRATION AND DEREGISTRATION
A 11.2.4	Review of user access rights	I.AC-10: REVIEW OF ACCESS RIGHTS
A.11.3	**User Responsibilities**	
A.11.3.1	Password use	I.AC-2: ACCOUNT MANGEMENT
A.11.3.2	Unattended user equipment	O.SP-4: ACCEPTABLE USAGE POLICY
A.11.3.3	Clear desk and clear screen policy	O.PE-5: ACCESS CONTROL FOR DISPLAY MEDIUM
A.11.4	**Network access control**	
A.11.4.1	Policy on use of network services	I.AC-1: ACCESS CONTROL POLICY
A.11.4.2	User authentication for external connections	I.IA-6: AUTHENTICATION FOR EXTERNAL CONNECTION
A.11.4.3	Equipment identification in networks	I.IA-2: NODE AUTHENTICATION FOR REMOTE ADMINISTRATION OF NETWORK DEVICES AND SERVERS

ISO 27001: 2005 Clauses		GD 200 eSAFE Controls
A.11.4.4	Remote diagnostic and configuration port protection	I.AC-1: ACCESS CONTROL POLICY O.PE-3: AUTHORIZATION OF PHYSICAL ACCESS
A.11.4.5	Segregation in networks	I.AC-3: ACCESS ENFORCEMENT
A.11.4.6	Network connection control	I.AC-7: NETWORK CONNECTION CONTROL
A.11.4.7	Network routing control	I.AC-6: NETWORK ROUTING CONTROL
A.11.5	**Operating system access control**	
A.11.5.1	Secure log-on procedures	I.AC-8: SECURE LOG-ON PROCESS
A.11.5.2	User identification and authentication	I.IA-1: USER IDENTIFICATION AND AUTHENTICATION
A.11.5.3	Password management system	• I.IA-2: NODE AUTHENTICATION FOR REMOTE ADMINISTRATION OF NETWORK DEVICES AND SERVERS • I.IA-4: SPECIFICATION OF AUTHENTICATOR • I.IA-5: MANAGEMENT OF AUTHENTICATOR
A.11.5.4	Use of system utilities	I.AC-1: ACCESS CONTROL POLICY I.SI-1: SYSTEM INTEGRITY
A.11.5.5	Session time-out	A.AC-6: AUTOMATIC SESSION TERMINATION I.SI-2: PROTECTION OF SYSTEM INTEGRITY
A.11.5.6	Limitation of connection time	A.AC-9: ACCESS TIME RESTRICTION
A.11.6	**Application and information access control**	
A.11.6.1	Information access restriction	A.AC-2: ACCESS ENFORCEMENT I.SI-3: RESTRICTION IN REMOTE ADMINISTRATION
A.11.6.2	Sensitive system isolation	A.DH-3: APPLICATION PARTITIONING
A.11.7	**Mobile computing and tele-working**	
A.11.7.1	Mobile computing and communications	O.SP-4: ACCEPTABLE USAGE POLICY
A.11.7.2	Tele-working	I.IA-6: AUTHENTICATION FOR EXTERNAL CONNECTION
A.12	**Information systems acquisition, development and maintenance**	

ISO 27001: 2005 Clauses		GD 200 eSAFE Controls
A.12.1	**Security requirements of information systems**	
A.12.1.1	Security requirements analysis and specification	O.SA-1: SYSTEM & SERVICE ACQUISTION AND MAINTENANCE POLICY O.SA-2: ACQUISITION AND MAINTENANCE PROCESS
A.12.2	**Correct processing in applications**	
A.12.2.1	Input data validation	A.DH-1: INPUT DATA VALIDATION
A.12.2.2	Control of internal processing	I.SI-6: INTEGRITY OF DATA I.SI-1: SYSTEM INTEGRITY
A.12.2.3	Message integrity	A.DH-2: PROTECTION OF TRANSMITTED DATA
A.12.2.4	Output data validation	I.SI-6: INTEGRITY OF DATA
A.12.3	**Cryptographic controls**	
A.12.3.1	Policy on the use of cryptographic controls	O.SP-1: Information security policy
A.12.3.2	Key management	O.SP-1: Information security policy
A.12.4	**Security of system files**	
A.12.4.1	Control of operational software	O.CM-1: CONFIGURATION MANAGEMENT PROCEDURE O.CM-3: CONFIGURATION CHANGE CONTROL
A.12.4.2	Protection of system test data	I.AC-1: ACCESS CONTROL POLICY
A.12.4.3	Access control to program source code	I.AC-1: ACCESS CONTROL POLICY O.CM-1: CONFIGURATION MANAGEMENT PROCEDURE O.CM-3: CONFIGURATION CHANGE CONTROL
A.12.5	**Security in development and support processes**	

ISO 27001: 2005 Clauses		GD 200 eSAFE Controls
A.12.5.1	Change control procedures	O.CM-1: CONFIGURATION MANAGEMENT PROCEDURE O.CM-3: CONFIGURATION CHANGE CONTROL O.SA-3: CONFIGURATION MANAGEMENT INFORMATION O.SA-4: SECURITY TESTING OF INFORMATION SYSTEM
A.12.5.2	Technical review of applications of operating system changes	O.CM-3: CONFIGURATION CHANGE CONTROL O.SA-3: CONFIGURATION MANAGEMENT INFORMATION O.SA-4: SECURITY TESTING OF INFORMATION SYSTEM
A.12.5.3	Restrictions on changes to software packages	O.CM-3: CONFIGURATION CHANGE CONTROL
A.12.5.4	Information leakage	A.DH-4: ERROR HANDLING
A.12.5.5	Outsourced software development	O.SA-6: ADDRESSING SECURITIES IN 3RD PARTY AGREEMENT
A.12.6	**Technical Vulnerability Management**	
A.12.6.1	Control of technical vulnerabilities	I.SI-4: PATCHING OF OS AND APPLICATION SOFTWARE O.SA-5: TECHNICAL VULNERABILITY OF INFORMATION SYSTEM
A.13	**Information security incident management**	
A.13.1.1	Reporting information security events	O.IM-1: INCIDENT MANAGEMENT PROCEDURES O.IM-2: TRAINING ON INCIDENT RESPONSE O.IM-3: INCIDENT REPORTING O.BC-2: BUSINESS CONTINUITY PLAN
A.13.1.2	Reporting security weaknesses	O.IM-3: INCIDENT REPORTING
A.13.2	**Management of information security incidents and improvements**	
A.13.2.1	Responsibilities and procedures	O.IM-1: INCIDENT MANAGEMENT PROCEDURES
A.13.2.2	Learning from information security incidents	O.IM-5: INCIDENT MONITORING
A.13.2.3	Collection of evidence	O.IM-6: COLLECTION OF EVIDENCES

ISO 27001: 2005 Clauses		GD 200 eSAFE Controls
A.14	**Business continuity management**	
A.14.1	**Information security aspects of business continuity management**	
A.14.1.1	Including information security in the business continuity management process	O.BC-1: BUSINESS CONTINUITY POLICY AND PROCEDURES
A.14.1.2	Business continuity and risk assessment	O.BC-1: BUSINESS CONTINUITY POLICY AND PROCEDURES
A.14.1.3	Developing and implementing continuity plans including information security	O.BC-1: BUSINESS CONTINUITY POLICY AND PROCEDURES O.BC-2: BUSINESS CONTINUITY PLAN O.BC-3: BUSINESS CONTINUITY TRAINING
A.14.1.4	Business continuity planning framework	O.BC-2: BUSINESS CONTINUITY PLAN O.BC-3: BUSINESS CONTINUITY TRAINING
A.14.1.5	Testing, maintaining and reassessing business continuity plans	O.BC-4: BUSINESS CONTINUITY PLAN TESTING AND EXERCISES O.BC-5: BUSINESS CONTINUITY PLAN UPDATE O.BC-7: ALTERNATE PROCESSING SITE
A.15	**Compliance**	
A.15.1	**Compliance with legal requirements**	
A.15.1.1	Identification of applicable legislation	O.PS-1: PERSONNEL SECURITY POLICY AND PROCEDURES O.SA-1: SYSTEM & SERVICE ACQUISTION AND MAINTENANCE POLICY O.BC-1: BUSINESS CONTINUITY POLICY AND PROCEDURES O.CO-2: LEGAL COMPLIANCE
A.15.1.2	Intellectual property rights (IPR)	O.CM-2: CONFIGURATION BASELINING O.CM-6: INVENTORY OF INFORMATION SYSTEM COMPONENTS

ISO 27001: 2005 Clauses		GD 200 eSAFE Controls
A.15.1.3	Protection of organizational records	I.AL-4: PROTECTION OF AUDIT /LOG DATA
A.15.1.4	Data protection and privacy of personal information	NA
A.15.1.5	Prevention of misuse of information processing facilities	O.SP-4: ACCEPTABLE USAGE POLICY
A.15.1.6	Regulation of cryptographic controls	O.SP-1: Information security policy
A.15.2	**Compliance with security policies and standards, and technical compliance**	
A.15.2.1	Compliance with security policies and standards	O.SP-5: MONITORING AND REVIEW O.CO-1: COMPLIANCE TO SECURITY POLICY AND PROCEDURES
A.15.2.2	Technical compliance checking	O.SA-5: TECHNICAL VULNERABILITY OF INFORMATION SYSTEM
A.15.3	**Information systems audit considerations**	
A.15.3.1	Information systems audit controls	O.SP-5: MONITORING AND REVIEW
A.15.3.2	Protection of information systems audit tools	I.AC-1: ACCESS CONTROL POLICY I.SI-1: SYSTEM INTEGRITY

7.0 References

[1] FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems

[2] NIST SP 800-53: Recommended Security Controls for Federal Information Systems

[3] ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements

[4] ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security management

8.0 Acknowledgements to the contributors

Contributed by members of the core group in STQC, DIT

Ms. Mitali Chatterjee, Senior Director (Convener)

Mr. Arvind Kumar, Director

Mr. N.E. Prasad, Director

Mr. B.K. Mondal, Director

Mr. Aloke Sain, Director

Mr. Subhendu Das, Director

Core Group acknowledges the contribution made by the Expert Committee of DIT through their reviews