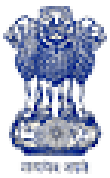
Document No: eSAFE-GD202

Version: 1.0

January, 2010

E Security Assurance Framework:

Baseline Security Controls for Medium Impact Information Systems eSAFE-GD202



Government of India
Department of Information Technology
Ministry of Communications and Information Technology
New Delhi – 110 003

Baseline Security Controls For Medium Impact Information Systems

GD 202

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

Introduction

The selection and employment of appropriate security controls for an information system are important tasks that can have major implications on the operations and assets of an organization. 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 security controls defined in this document are recommended for use in MEDIUM IMPACT (Categorized as per GD 100) information systems for eGovernance. These are the subset of the controls taken from the document GD200. These controls are the minimum set of controls required to secure MEDIUM IMPACT Information Systems and termed as Baseline Security Controls for the MEDIUM IMPACT Information Systems for eGovernance.

This Guidelines Document 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

Introduction 3
1.0 Scope 9
1.1 Objective 9
1.2 Description 9
2.0 Target Audience 9
3.0 Type of Document 9
4.0 Definitions and Acronyms 9
5.0 Security Control Organization and Structure 10
6.0 The Baseline Security Controls for MEDIUM IMPACT Information Systems 11
A: APPLICATION CLASS 11
A.IA: IDENTIFICATION AND AUTHENTICATION 11
A.IA-1: USER IDENTIFICATION AND AUTHENTICATION 11
A.IA-2: AUTHENTICATION HINT 11
A.IA-3: HANDLING OF AUTHENTICATION FAILURE 11
A.IA-4: ENFORCING USE OF QUALITY AUTHENTICATION SECRET 12
A.IA-5: GENERATING QUALITY AUTHENTICATION SECRET 12
A.AC: ACCESS CONTROL 12
A.AC-1: SYSTEM ACCESS NOTIFICATION 12
A.AC-2: ACCESS ENFORCEMENT 13
A.AC-3: NOTIFICATION OF PREVIOUS LOGON 13
A.AC-4: CONTROL OF CONCURRENT SESSIONS 13
A.AC-5: AUTHENTICITY of COMMUNICATION SESSIONS 13
A.AC-6: AUTOMATIC SESSION TERMINATION 14
A.AC-7: AUTHENTICATION OF CONNECTING EQUIPMENT 14
A.AC-8: ACCESS LOG 14
A.AC-9: ACCESS TIME RESTRICTION 14
A.AC-10: ENFORCING DATA INPUT BY HUMAN (CAPTCHA) 15
A.DH: DATA HANDLING AND PROTECTION 15
A.DH-1: INPUT DATA VALIDATION 15
A.DH-2: PROTECTION OF TRANSMITTED DATA 15

A.DH-3: APPLICATION PARTITIONING 15
A.DH-4: ERROR HANDLING 16
I: INFRASTRUCTURE CLASS 16
I.IA: IDENTIFICATION AND AUTHENTICATION 16
I.IA-1: USER IDENTIFICATION AND AUTHENTICATION 16
I.IA-2 NODE AUTHENTICATION FOR REMOTE ADMINISTRATION OF NETWORK DEVICES AND SERVERS 16
I.IA-3: MANAGEMENT OF IDENTIFIER 17
I.IA-4: SPECIFICATION OF AUTHENTICATOR 17
I.IA-5: MANAGEMENT OF AUTHENTICATOR 18
I.IA-6: AUTHENTICATION FOR EXTERNAL CONNECTION 19
I.IA-7: USER REGISTRATION AND DEREGISTRATION 19
I.AC: ACCESS CONTROL 20
I.AC-1: ACCESS CONTROL POLICY 20
I.AC-2: ACCOUNT MANAGEMENT 21
I.AC-3: ACCESS ENFORCEMENT 21
I.AC-4: SEGREGATION OF DUTIES 22
I.AC-5: NETWORK SEGMENTATION 22
I.AC-6: NETWORK ROUTING CONTROL 23
I.AC-7: NETWORK CONNECTION CONTROL 23
I.AC-8: SECURE LOG-ON PROCESS 23
I.AC-9: WIRELESS ACCESS CONTROL 24
I.AC-10: REVIEW OF ACCESS RIGHTS 25
I.AL: AUDIT AND LOGGING 25
I.AL-1: SELECTION OF AUDITABLE EVENT 25
I.AL-2: AUDIT RECORD MANGEMENT 26
I.AL-3: CAPACITY OF STORAGE FOR AUDIT LOGS 26
I.AL-4: PROTECTION OF AUDIT /LOG DATA 27
I.AL-5: TIME SYNCHRONIZATION OF INFORMATION SYSTEMS 27
I.AL-6: RETENTION OF AUDIT RECORDS 27
I.SC: SYSTEM & COMMUNICATION PROTECTION 28
I.SC-1: TRUSTED SERVICE 28

I.SC-2: USE OF STRONG PROTOCOLS 28
I.SC-3: CONFIDENTIALITY OF STORED DATA 28
I.SI: SYSTEM & INFORMATION INTEGRITY PROTECTION 29
I.SI-1: SYSTEM INTEGRITY 29
I.SI-2: PROTECTION OF SYSTEM INTEGRITY 29
I.SI-3: RESTRICTION IN REMOTE ADMINISTRATION 29
I.SI-4: PATCHING OF OS AND APPLICATION SOFTWARE 30
I.SI-5: CONTROL OF MALICIOUS SOFTWARE 30
I.SI-6: INTEGRITY OF DATA 31
O: OPERATIONS AND MANAGEMENT CLASS 31
O.SP: SECUIRTY POLICY & PROCEDURE 31
O.SP-1: INFORMATION SECURITY POLICY 31
O.SP-2: OPERATIONAL PROCEDURE 31
O.SP-5 : MONITORING AND REVIEW 32
O.SO: SECURITY ORGANISATION 33
O.SO-1: SECURITY FRAMEWORK 33
O.SO-2: AUTHORIZATION OF INFORMATION SYSTEM 33
O.PS: PERSONNEL SECURITY 33
O.PS-1: PERSONNEL SECUIRTY PROCEDURES 33
O.PS-2: SCREENING 34
O.PS-3: TERMS AND CONDITIONS OF THE EMPLOYMENT 34
O.PS-5: INFORMATION SECURITIES, AWARENESS, EDUCATION & TRAINING 35
O.PS-6: DISCIPLINARY PROCESS 35
O.PS-7: TERMINATION PROCESS 35
O.PE: PHYSICAL & ENVIRONMENTAL SECURITY 36
O.PE-1: PHYSICAL & ENVIRONMENTAL PROTECTION POLICY & PROCEDURE 36
O.PE-2: PHYSICAL ACCESS PERIMETER 36
O.PE-3: AUTHORIZATION OF PHYSICAL ACCESS 36
O.PE-4: PHYSICAL ACCESS CONTROL 37
O.PE-5: ACCESS CONTROL FOR DISPLAY MEDIUM 37
O.PE-6: MONITORING PHYSICAL ACCESS 37
O.PE-7: CONTROL OF VISITOR 38

O.PE-8: PROTECTION AGAINST FIRE 38
O.PE-11: WORKING IN SECURE AREAS 39
O.PE-12: SUPPORTING UTILITIES 39
O.PE-13: CABLING SECURITY 39
O.PE-14: EQUIPMENT MAINTENANCE 40
O.PE-15: WORKING OFFSITE 40
O.PE-16: SECURE DISPOSAL OR RE-USE OF DEVICES 40
O.PE-17: DELIVERY AND REMOVAL 40
O.MS: MEDIA SECURITY 41
O.MS-1: MEDIA HANDLING PROCEDURE 41
O.CM: CONFIGURATION MANAGEMENT 42
O.CM-1: CONFIGURATION MANAGEMENT PROCEDURE 42
O.CM-2: CONFIGURATION BASELINING 42
O.CM-3: CONFIGURATION CHANGE CONTROL 42
O.CM-4: MONITORING CONFIGURATION CHANGES 43
O.CM-5: OPTIMUM CONFIGURATION 43
O.IM: INCIDENT MANAGEMENT 44
O.IM-1: INCIDENT MANAGEMENT PROCEDURES 44
O.IM-2 TRAINING ON INCIDENT RESPONSE 44
O.IM-3: INCIDENT REPORTING 44
O.IM-4: INCIDENT RESPONSE 45
O.IM-5: INCIDENT MONITORING 45
O.SA: SYSTEM & SERVICE ACQUISITION & MAINTENANCE 45
O.SA-1: SYSTEM & SERVICE ACQUISITION & MAINTENANCE POLICY 45
O.SA-2: ACQUISITION & MAINTENANCE PROCESS 46
O.SA-3: CONFIGURATION MANAGEMENT OF INFORMATION SYSTEM 46
O.SA-4: SECURITY TESTING OF INFROMATION SYSTEM 46
O.SA-5: TECHNICAL VULNERABILITY OF INFORMATION SYSTEM 47
O.SA-6: ADDRESSING SECUIRTIES IN 3RD PARTY AGREEMENT 47
O.SA-7: MANAGEMENT OF 3RD PARTY SECUIRTY & DELIVERY SERVICE 47
O.BC: BUSINESS CONTINUITY MANAGEMENT 48
O.BC-1: BUSINESS CONTINUITY POLICY AND PROCEDURES 48

O.BC-2: BUSINESS CONTINUITY PLAN 48
O.BC-3: BUSINESS CONTINUITY TRAINING 48
O.BC-4: BUSINESS CONTINUITY PLAN TESTING AND EXERCISES 49
O.BC-5: BUSINESS CONTINUITY PLAN UPDATE 49
O.BC-6: ALTERNATE STRORAGE SITES 49
O.BC-7: ALTERNATE PROCESSING SITES 50
O.BC-8: INFORMATION SYTEM BACKUP & RECOVERY 50
O.CO: COMPLIANCE 51
O.CO-1: COMPLIANCE TO SECURITY POLICIES AND PROCEDURES 51
O.CO-2: LEGAL COMPLIANCE 51
7.0 References 52
8.0 Acknowledgements to the contributors 52

1.0 Scope

1.1 Objective

The purpose of this document is to provide guidelines for specifying security controls for medium impact 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

The guidelines have been developed to help achieve more secure information systems within the government by:

- Facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems;
- Providing a recommendation for minimum or baseline security controls for MEDIUM IMPACT information systems categorized in accordance with GD 100, *Guidelines for Security Categorization of Information Systems*;
- Providing a stable, yet flexible catalog of security controls for information systems to meet current organizational protection needs and the demands of future protection needs based on changing requirements and technologies; and
- Creating a foundation for the development of assessment methods and procedures for determining security control effectiveness.

2.0 Target Audience

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

NIL

5.0 Security Control Organization and Structure

Security controls in this security control catalog have a well-defined organization and structure. The security controls are organized into *classes* and *families* for ease of use in the control selection and specification process. There are three general classes of security controls (i.e., Application, Infrastructure, and Operations & Management) and 18 e security control families. Each family contains security controls related to the security functionality of the family. A three-character identifier is assigned to uniquely identify each control family. Table 1 summarizes the classes and families in the security control catalog and the associated family identifiers.

Table 1: Security Control Classes, Families and Identifiers

Identifier	Class	Family
A.IA	Application	Application Identification and Authentication
A.AC	Application	Application Access Control
A.DH	Application	Data Handling & Protection
I.IA	Infrastructure	Identification & authentication
I.AC	Infrastructure	Access Control
I.AL	Infrastructure	Audit & Logging
I.SC	Infrastructure	System & Communications Protection
I.SI	Infrastructure	System & Information Integrity Protection
O.SP	Operations & Management	Security Policy & Procedure
O.SO	Operations & Management	Security Organization
O.PS	Operations & Management	Personnel Security
O.PE	Operations & Management	Physical & Environmental security
O.MS	Operations & Management	Media Security
O.CM	Operations & Management	Configuration Management
O.IM	Operations & Management	Incident Management
O.SA	Operations & Management	System & Service Acquisition
O.BC	Operations & Management	Business Continuity Management
O.CO	Operations & Management	Compliance

To uniquely identify each control, a numeric identifier is appended to the family identifier to indicate the number of the control within the control family. For example, A.IA-1 is the first control in the Identification & Authentication family of the Application class.

The security control structure consists of three key components: (i) a control section; (ii) a Explanation section; and (iii) a control Improvements section.

6.0 The Baseline Security Controls for MEDIUM IMPACT Information Systems

The controls and control improvements in faded color are not considered to be baseline controls for MEDIUM IMPACT Information Systems.

A: APPLICATION CLASS

A.IA: IDENTIFICATION AND AUTHENTICATION

A.IA-1: USER IDENTIFICATION AND AUTHENTICATION

Control: The application uniquely identifies and authenticates users or processes.

Explanation: Users are uniquely identified and authenticated for all accesses as per the access control policy at the application level. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof.

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.)

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.

Explanation: The feedback from the application does not provide any hint or information that would allow an unauthorized user to compromise the authentication mechanism. Display of asterisks, when a user types in a password, is an example of obscuring feedback of authentication information.

Control Improvements: None.

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.

Explanation: Due to the potential for denial of service, automatic lockouts initiated by the application are usually temporary and automatically release after a predetermined time period established by the organization.

Control Improvements:

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

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.

Explanation: This enforces users to use quality authentication secrets e.g. passwords as per the organization policy. Thus, an organization can restrict use of blank passwords, dictionary words, etc. It can enforce minimum length of password, alpha-numeric password etc.

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.

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.

Explanation: This enforces users to use quality authentication secrets generated by the application for some functions or transactions e.g. generating session tokens of adequate length, random in nature, having limited lifespan and cannot be reused after the session termination by the user or the application.

Control Improvements: None

A.AC: ACCESS 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.

Explanation: Privacy and security policies are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the application. For publicly accessible systems: (i) the system use information is available and when appropriate, is displayed before granting access; (ii) any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and (iii) the notice given to public users of the application includes a description of the authorized uses of the system.

Control Improvements: None

A.AC-2: ACCESS ENFORCEMENT

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

Explanation: 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.

Control Improvements:

(i) Cryptography based access control 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.

Explanation: None

Control Improvements: None

A.AC-4: CONTROL OF CONCURRENT SESSIONS

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

Explanation: None

Control Improvements: None

A.AC-5: AUTHENTICITY of COMMUNICATION SESSIONS

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

Explanation: This control focuses on protection of communications. The intent of this control is to implement session-level protection where needed (e.g., in service-oriented architectures providing web-based services). The application system can employ cryptographic mechanisms such as SSL, TLS etc. to achieve this.

Control Improvements: None

A.AC-6: AUTOMATIC SESSION TERMINATION

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

Explanation: A remote session is initiated whenever an application is accessed by a user (or an information system) communicating through an external, non-organization-controlled or untrusted network (e.g., the Internet).

Control Improvements:

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

A.AC-7: AUTHENTICATION OF CONNECTING EQUIPMENT

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

Explanation: Equipment/node identification can be used to ensure that communication can take place only from specific locations/nodes/equipment through some identifier attached to the node/equipment e.g. IP address, MAC address, telephone no. etc.

Control Improvements: None

A.AC-8: ACCESS LOG

Control: The application logs all access events.

Explanation: Examples of access events include successful/unsuccessful login attempts, creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message etc.

Control Improvements: None

A.AC-9: ACCESS TIME RESTRICTION

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

Explanation: Connection time controls should be considered for sensitive computer applications, especially from high risk locations, e.g. public or external areas. Examples of such restrictions are, using predetermined time slots for batch file transmissions, restricting connection times to normal office hours etc.

Control Improvements: None

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'.

Explanation: A CAPTCHA is a program that can generate and grade tests that humans can pass but current computer programs (bots) cannot. For example, humans can read distorted text but the 'bots' can't. Use of CAPTCHA in data input pages/user interfaces e.g login form, registration form, or any other form where user has to input data to authenticate, to write data into database or to query database, prevents various attacks like brute force/dictionary attack on password, denial of service attack on application etc.

Control Improvements: None

A.DH: DATA HANDLING AND PROTECTION

A.DH-1: INPUT DATA VALIDATION

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

Explanation: Checks for validity of input data are accomplished as close to the point of origin as possible. Rules for checking the validity of information system inputs (e.g., character set, length, range, type, format acceptable values etc.) are in place to verify that inputs match specified definitions for format and content.

Control Improvements: None

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.

Explanation:

The organization can employ cryptographic mechanisms such as SSL, TLS etc. to recognize changes or to prevent unauthorized disclosure to data or information during transmission.

Control Improvements:

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

A.DH-3: APPLICATION PARTITIONING

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

Explanation: The application 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.

Control Improvements: None

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.

Explanation: Error messages generated by the application provide information without revealing any sensitive or potentially harmful information that could be used by malicious users to compromise the system. Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) are not listed in error logs or associated administrative messages.

Control Improvements: None

I: INFRASTRUCTURE CLASS

I.IA: IDENTIFICATION AND AUTHENTICATION

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 user.

Explanation: Users shall be uniquely identified and authenticated prior to getting access to the information systems. The access may be either through local interface or over network. This identification and authentication shall be treated as bare minimum requirement for getting access to the system through which the user actually accesses the eGovernance application. Usually separate identification and authentication mechanisms are employed at the application level. Unique identification of the user at system level helps the enforcement of other control like 'audit and logging'. Authentication of user identities is accomplished through the use of passwords, access tokens, biometrics, and in the case of multifactor authentication, some combination thereof.

Control improvements:

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

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

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.

Explanation: Remote access to the system, especially for system administration, brings additional risk of unauthorized access. Hence, it is necessary to restrict remote access only from specified machines. Enforcement of this control should ensure that the communication for system administration have been initiated from known locations or equipments. An identifier (say MAC address or IP address) in or attached to the equipment can be used to indicate whether this equipment is permitted to connect to the network. These identifiers should clearly indicate to which network the equipment is permitted to connect. It may be necessary to consider physical protection of the equipment to maintain the security of the list of equipment identifiers.

Control improvements: None

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

Explanation: 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. However generic names like 'guest', 'everyone' etc. shall be avoided as a first line of protection of such accounts from unauthorized use.

Control improvements: None

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 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.

Explanation: Information system authenticators include, for example, passwords, tokens, PKI certificates, biometrics, and key cards. Depending on the requirement a particular type of authenticator should be used. For sensitive information system where any unauthorized access may create sufficient impact on its Confidentiality, Integrity and Availability, a combination of more than one authenticator should be used. The authenticator shall not be based on anything easily guessable like person related information, e.g. names, telephone numbers, dates of birth etc

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 can not be ensured through other means

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

Explanation: Information system authenticators include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. Users will take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not sharing authenticators with others. They are required to report immediately to a competent authority in case of loss or damage or suspected compromise of it. The authenticators are required to be protected from unauthorized disclosure by adopting mechanism like encoding (where impact of disclosure in not that high) or encryption. The protect mechanism is necessary not only when the authenticators are stored but also when in transmission.

The information system is also required to enforce such a mechanism that prohibits passwords from being displayed when entered.

If PKI-based authentication is used, it is necessary to validate certificates through authorized certification path to Certification Authority.

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

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.

Explanation: Examples of remote access methods include dial-up, broadband, and wireless. Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. The organizations are required to restrict remote access from public domain in general. However, if it is absolutely necessary the same will be achieved through secure protocol which uses cryptographic technique to protect data for unauthorized disclosure during transmission. Additional authentication mechanism for remote users should be enforced to minimize the risk of unauthorized access by simply guessing the authenticator.

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

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.

Explanation: The procedure for user registration and de-registration is required to be in place and the same will be approved by the competent authority. The procedure will address the requirement for verification of user identity and authorization from the information system owner. The information system may not be flat in architecture; in such cases the access authorization must address the level of access, so that the same appropriate to the business purpose and /or in accordance with the security clearance of the user. Unless otherwise needed by the organization, the access rights of the user will be removed or blocked as soon as their roles are changed or they are separated from the organization. The

records generated out of this registration and de-registration will be treated as formal record of the organization.

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

I.AC: ACCESS CONTROL

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.

Explanation: Access control policy is nothing but the rules and rights for each user or group of users which the organization is intended to follow. The policy usually takes into account the following issues like:

- Policies for information dissemination and authorization (e.g. the need to know principle and security levels and classification of information)
- Scope of the access control policy, including the areas where mandatory access control is necessary to be enforced
- Permitted access methods for different users or group of users
- General authorization process
- Specific authorization process, depending upon the security requirements of individual information system
- Standard user access profiles for common job roles in the organization
- Authority for removal of access rights

Control improvements:

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

Explanation: Account management shall include the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization shall identify the authorized users for each information system and specify respective access rights/privileges. The organization shall grant access to the information system based on a valid need-to-know/need-to-share faces that is determined by assigned official duties and satisfying all personnel security criteria.

The organization shall look for proper identification for requests to establish information system accounts and approve all such requests, before creation. The organization shall specifically authorize and monitor the use of accounts having generic name (having no traceability with individual) and shall remove, disable or otherwise secure unnecessary accounts.

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

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.

Explanation: 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. 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.

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

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.

Explanation: The organization shall establish appropriate divisions of responsibility and should separate duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. Care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered in designing the controls. Whenever it is difficult to segregate, especially for small organization, other controls such as monitoring of activities, audit trails and management supervision should be considered. It is important that security audit remains independent.

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

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).

Explanation: Security of a large network should be controlled by dividing it into separate logical sub - networks, each protected by a defined security perimeter. A graduated set of controls can be applied in different logical networks to further segregate the network security environments, e.g. publicly accessible systems, internal networks and critical assets. The sub-networks should be defined based on a risk assessment and the different security requirements within each of the network segments, as governed by the access control policy. The relative cost and performance impact on the information flow across the controlling devices should also be taken into consideration while segregating the network into sub-networks.

Control improvements:

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

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.

Explanation: Information flow control should be regulated through suitable network routing where the information is allowed to travel within an information system and between information systems.

Flow control should be based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement should be implemented in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers).

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

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

Explanation: The connection capability of users can be restricted through network gateways that filter traffic by means of pre-defined tables or rules. Examples of applications to which restrictions should be applied are:

(a) messaging, e.g. electronic mail
(b) file transfer
(c) interactive access
(d) Application access

Control improvements:

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

I.AC-8: SECURE LOG-ON PROCESS

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

Explanation: The procedure for logging into an operating system should be designed in such a way that minimizes the opportunity for unauthorized access. The log-on procedure should therefore disclose the minimum of information about the system.

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

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 and following the security implementation guidance as given below.

Explanation:

(i) 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

(ii) 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

(iii) Disabling DHCP service from WLAN access point, instead if required, the parent DHCP service (from wired LAN) shall be used

(iv) Using a network firewall to secure a wireless network

(v) Use of WEP, WPA etc. as bare minimum security for authentication and protection of information on a wireless local area network (WLAN)

(vi) For WEP minimum key length should be 128 bit

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

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

Explanation:

Access rights are the formal authorization extended to the users on IT resources. "Need to know access policy" is the very first principle of information security and the same can be implemented if the access rights are kept under control. 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 quite common. Most of the cases these security weaknesses are remain unnoticed. 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.

Control improvements:

(i) 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

I.AL: AUDIT AND LOGGING

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*].

Explanation: The purpose of this control is to identify important events which need to be audited, as significant and relevant to security, of the information system. The organization should specify which information system components carry out auditing activities. Auditing activity can affect information

system performance. Therefore, the organization should decide, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems.

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

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.

Explanation: Audit records or log records are important data to investigate the security incidents, if any. Further these data gives confidence to the security manager or the administrator of the information system regarding the intended behavior of it. It is necessary to the system administrator or security manager to identify the issues on which they intend to enable the audit data. However, each of the audit record or log should contain the minimum information like 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

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

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.

Explanation: The organization provides sufficient audit storage capacity, taking into account the auditing to be performed and the online audit processing requirements

Control improvements:

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

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

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

Explanation: This control should aim to protect against unauthorized changes and operational problems with the auditing/ Logging facility which includes:

- Alterations to the message types that are recorded
- Audit data/Log files being edited or deleted
- Storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.

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.

System logs often contain a large volume of information, much of which is extraneous to security monitoring. To help identify significant events for security monitoring purposes, the copying of appropriate message types automatically to a second log, and/or the use of suitable system utilities or audit tools to perform file interrogation and rationalization should be considered.

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

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.

Explanation: The correct interpretation of the date/time format is important to ensure that the timestamp reflects the real date/time. The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. A network time protocol can be used to keep all of the servers in synchronization with the master clock.

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

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.

Explanation: The organization should retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes.
Control improvements: None

I.SC: SYSTEM & COMMUNICATION PROTECTION

I.SC-1: TRUSTED SERVICE

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

Explanation: Physical signature is used as traditional means for authenticity of any document. In electronic form the information are usually disseminated through web pages which may be faked by malicious intent. Authenticity of information in electronic form can be ensured through digital certificate obtained through PKI.

Control improvements: None

I.SC-2: USE OF STRONG PROTOCOLS

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

Explanation: The protocols like TELNET, FTP, and HTTP have inherent security weakness as they transmit data in clear text; the confidential data like account password can be sniffed (by attacker sitting inside LAN) and may be misused for unauthorized access to the information system. The risk of use of such protocol increases with vulnerability commonly associated with the users, that the same password is used for accessing different 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 should be protected through use of strong protocols.

Control improvements: None

I.SC-3: CONFIDENTIALITY OF STORED DATA

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

Explanation: Different information system uses security mechanism to avoid storage of confidential data like account password in clear text. By default most operating systems stores the account passwords in the form of cryptographic hashes.
In other cases, where the organization has an option to adopt suitable security mechanism to protect the confidential data, encryption with minimum key length of 128 bit, with reportedly strong and internationally accepted algorithm should be employed.

Control improvements: None

I.SI: SYSTEM & INFORMATION INTEGRITY PROTECTION

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.

Explanation: The security of individual servers & workstations is a critical factor in the defense of any environment, especially when remote access is allowed. 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. Further within an organization, the configuration of different components of similar type may vary according to their deployment in the network and the services, they are intended to provide. The standards can be drawn from International best practices like www.cisecurty.org .

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

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.

Explanation: As a security best practice, administrators should use their individual accounts, having suitably high privilege, for day to day system administration activities. 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.

Control improvements: none

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.

Explanation: Remote administration activities are conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet). The use of remote administration tools 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. The following other techniques controls should be considered for improving the security of remote administration:

(i) encryption and decryption of communications
(ii) strong identification and authentication techniques
(iii) 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.

Control improvements:

(i) 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

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.

Explanation: The security flaws acknowledged and corresponding release of the security patches by the respective vendors should be brought under closed observation. The necessary security patches, hot fixes etc should be reviewed and applied at the earliest.

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

I.SI-5: CONTROL OF MALICIOUS SOFTWARE

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

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. 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 signature of the malicious software shall be updated time to time through a managed process.

Control improvements:

(i) Content filtering & download restriction

(ii) Restriction in use of removable media
(iii) Control of mobile codes

I.SI-6: INTEGRITY OF DATA

Control: The organization should adopt security mechanism to detect the loss of integrity of information.

Explanation: There are occasions where integrity of information is of prime issue and there is threat for compromise of the same. To mitigate this risk, the organization should adopt suitable security controls like hash/message digest and maintain snapshot of hashes of the target information. Any changes in the hash value will indicate the loss of integrity of the corresponding information.

Control improvements: None

O: OPERATIONS AND MANAGEMENT CLASS

O.SP: SECUIRTY POLICY & PROCEDURE

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.

Explanation: The security policy state management commitment and set out organization's approach to manage information security. The corporate security policy refers to individual policies and guidelines that exist to govern the secure and appropriate use of technology and processes with the organization. The area covers policy to address users, system, data etc. and the policy is appropriately communicated to employees and users, suppliers etc.

Control Improvements: None

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.

Explanation: The relevant procedures shall be identified for various activities associated with the information system, which are required for correct and secure operation. These procedures shall be documented, maintained and available to the concerned users. The examples of such procedures are backup, start-up and close-down procedure of servers, desktop, equipment maintenance, change management procedure, media handling etc.

Control Improvements: None

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.

Explanation: The principle of segregation of responsibility should be kept in mind in order to reduce the risk of accidental or deliberate misuse of security policies. While defining the operating procedures, care should be taken that no single person can access, use or modify information system without authorization.

Control Improvements: None

O.SP-4: ACCEPTABLE USAGE POLICY

Control: The usage policy of assets and services associated with the information system shall be defined and implemented.

Explanation: All employees, contractors, and third party users should follow the usage policy as identified for the assets and services associated with the information system. The various assets and services associated with the information system may include electronic mail, internet and mobile device and usage policy for such assets and services should be identified and implemented.

Control Improvements: None

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

Explanation: Monitoring and review of policies, procedures and controls provide the input to the management on effectiveness of the controls implemented and any corrective/preventive action to be taken. The monitoring and review also help to evaluate and identify the area of the improvement required in the information system. The monitoring and review should be carried out at defined frequency and in response to any changes to the organizational environment, business circumstances, legal, statutory and regulatory conditions or technical environment.

Control Improvements: None

O.SO: SECURITY ORGANISATION

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

Explanation: There should be security organizational structure that is responsible to plan, implement and independently review all security activities and to ensure the security objectives for the information system are met. The security organizational structure should also be responsible to provide adequate resources for security activities and to define and approve the roles and responsibilities at various level including authorization and review.

Control Improvements:

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

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.

Explanation: The introduction of new information system or upgrades of the existing system (including migration) or usage of information system facilities where the information system resides, may lead to increase in security risk and hence, these shall be controlled and authorized by appropriate level of the security organization to ensure the relevant security policies and controls are met and compatible with the existing information system. The authorization process can be integrated with the change management process as defined in Configuration Management (O.CM-3).

Control Improvements: None

O.PS: PERSONNEL SECURITY

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.

Explanation: The personnel security policy and associated procedures shall be consistent with applicable laws, government orders, directives, policies, regulations, standards etc. and risk associated with the information system. The personnel security policy can be included as part of the general information security policy and security roles and responsibilities of the employees, contractors and third party users shall be defined and documented in accordance with information security policy. Personnel security procedures can be developed to implement monitor and improve the applicable controls.

Control Improvements: None

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.

Explanation: Screening/ background verification on individual users including employees, contractor and third party users shall be carried out in accordance with relevant laws, regulation, and ethics

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

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.

Explanation: The terms and conditions of the employment in the form of code of conduct or an agreement can be used to cover the employee's, contractor's or third party user's responsibilities regarding confidentiality, data protection ethic, appropriate use of information and information system, as well as reputable practice expected by the management.

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

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).

Explanation: Based on the security requirements of the information system, the confidentiality or non-disclosure agreement containing various elements like scope, responsibilities of the users, reporting etc. should be signed by each user.

Control improvements:

(i) The requirements for confidentiality and non-disclosure agreements shall be reviewed periodically and when changes occurs that influence the requirements

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

Explanation: All the users (normal and privilege) are required to be trained and made aware of how security applies to their daily job activities so that they do not inadvertently expose their organization to a greater risk. Special security training shall be imparted to the officials responsible for implementation security mechanisms and management of Information security .The relevant records on training shall be maintained.

Control Improvements:

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

O.PS-6: DISCIPLINARY PROCESS

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

Explanation: The disciplinary process shall be consistent with applicable laws, government orders, directives, policies, regulations, Standards. The disciplinary process can be included as a part of the general personnel policies and procedures.

Control Improvements: None

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.

Explanation: As a part of termination process and / or change in employment, all employees, contractors and third party users should return all previously issued software, documents relating to information system, mobile computing device, access card, information stored in electronic media etc. Their access right to information and information system should be reviewed and appropriate decision either to remove or change in the access right should be taken 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

O.PE: PHYSICAL & ENVIRONMENTAL SECURITY

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.

Explanation: The physical and environmental protection policy and procedures shall be consistent with applicable laws, government orders, directives, policies, regulations, standards. The physical and environmental protection policy can be included as part of the general information security policy. Physical and environmental protection procedures can be developed to implement, monitor and improve the applicable controls.

Control Improvements: None

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.

Explanation: The security perimeters i.e. barriers such as walls, card controlled entry or manned reception desk shall be used to physically protect the information system. The use of multiple barriers around the information system gives the additional protection while the failure of the single barrier does not mean the security is comprised.

Control Improvements: None

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.

Explanation: The relevant information of all users with their authorized access details and authorization credentials should be maintained. Appropriate authorization credentials include, for example badges, identification cards, smart cards etc. The access which is no longer required needs to remove promptly from the access list personnel.

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

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 commensurated with criticality of the facility and shall be determined through Risk Assessment.

Explanation: The physical access devices (e.g. keys, locks, card reader) and/or guards to control entry to the facilities containing information system

Control Improvements:

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

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.

Explanation: Placement of the display medium of the information system should be such that unauthorized individual should not get an opportunity to see the display output.

Control Improvements: None

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.

Explanation: The physical access logs shall be periodically reviewed and investigated the apparent security violations or suspicious access activities. Response to detected physical security incidents is a part of incident management.

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

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.

Explanation: The designated contractor and others with permanent authorization credential are not usually considered visitors.

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

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.

Explanation: Security threat against fire hazards should be minimized and thus proper preventive and corrective action should be taken.

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

Control Improvements: None

O.PE-9 : PROTECTION AGAINST ELECERICAL HAZARDS

Control: Protection against damage from electrical hazards shall be designed and applied.

Explanation: Poor and inappropriate cabling, electrical switches and device and its inadequate maintenance may lead to electrical hazards and hence these should appropriately be maintained. To minimize such threat, the information system should be securely placed.

Control Improvements: None

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.

Explanation: Consideration shall be given to any security threats presented by various external and environmental threats. Where possible, the consideration shall also been given for selection of the location or site of the facility with regard to the physical and environmental hazards.

Control Improvements: None

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.

Explanation: The arrangement for working in areas where information system reside, shall include controls for the employees, contractors an third party users working in e.g. server room , as well as other third party activities talking place there.

Control Improvements: None

O.PE-12: SUPPORTING UTILITIES

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

Explanation: All supporting utilities such as electricity, water supply, air conditioning etc. shall be adequate for the information system. The uninterrupted power supply (UPS) shall be considered to support orderly close down or continuous running while back-up generator is used to continue processing in case of a prolonged power failure.

Control Improvements: None

O.PE-13: CABLING SECURITY

Control: Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

Explanation: Availability of the network services is critically dependent on the quality of interconnection between the hosts through structured cabling including termination and marking. All cable runs should be physically protected from damage via tie-downs or where appropriate in conduit. Appropriate demarcation and test points should be maintained for shielded cabling (T1/T3s).

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

O.PE-14: EQUIPMENT MAINTENANCE

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

Explanation: The maintenance of information system in accordance with supplier's recommended service interval and specification by trained or authorized maintenance personnel ensure its correct functioning.

Control Improvements: None

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

Explanation: Regardless of ownership, the use of any information system outside the organization's premises including home working shall be authorized by the management and consideration shall be given to protect information and information system appropriately through implementing applicable controls.

Control Improvements: None

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.

Explanation: Information stored in the media can be comprised through careless disposal or re-use of component of information system.

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

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.

Explanation: Any component of information system entering or exiting the controlled area (where the information system exists) should be authorized to isolate and to prevent leakage of information. The access points particularly the delivery and loading area and other points where the unauthorized person may enter the controlled area, should preferably be separated. The records of such entry or exit should be documented.

Control Improvements: None

O.MS: MEDIA SECURITY

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.

Explanation: The moveable media like HDD, CD, flash drive, hard copy information etc. shall be appropriately protected during its access, storage, transmission and disposal to prevent unauthorized disclosure, modification, removal or destruction of information contained in it.

Control Improvements: None

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.

Explanation: The classification of information is essential to ensure appropriate level of protection and should be done base on the legal impact, degree on confidentiality and availability. Once the information contained in the media is classified, the same should be appropriately labeled in order to handle them in accordance with the defined policy.

Control Improvement: None

O.MS-3: SECURE MEDIA STORAGE

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

Explanation: The media may be damaged if the same is not stored in proper environment as specified by the manufacturer and information contained in the media may be lost.

Control Improvement:

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

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.

Explanation: The media containing information should be disposed of in accordance with the defined procedure when it is no longer required. This would minimize the risk of sensitive information leakage to unauthorized persons.

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

O.CM: CONFIGURATION MANAGEMENT

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.

Explanation: The configuration management procedure is consistent with applicable directives, policies, regulations, standards, and guidance. The configuration management policy can be included as part of the general information security policy. Configuration management procedures can be developed to implement, monitor and improve the applicable controls.

Control Improvements: None

O.CM-2: CONFIGURATION BASELINING

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

Explanation: The baseline configuration provides information about the build of a particular component in the information system (e.g., the standard software loaded for desktop or laptop computer including updated patch Information) and the component's logical relationship with other components within the information system. The baseline configuration also states a well-defined and documented specification to which the information system is built.

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

O.CM-3: CONFIGURATION CHANGE CONTROL

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

Explanation: Formal change control procedure shall be documented and implemented starting from systematic proposal for change, justification, authorization, test/evaluation implementation, , review and closure with recording of changes to information system.

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

O.CM-4: MONITORING CONFIGURATION CHANGES

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

Explanation: The configuration verification and audit process, both physical and functional shall be scheduled and a check is performed to ensure that configuration information is accurate, controlled and visible.

Control Improvements: None

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.

Explanation: The information systems are capable for providing a wide range of functions and services. Some of the functions/ services provided by default may not be necessary to support essential operation.

Control Improvements:

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

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.

Explanation: The appropriate level of granularity for the information system components included in the inventory is determined to ensure adequate management control for tracking and reporting.

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

O.IM: INCIDENT MANAGEMENT

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.

Explanation: The incident response procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The incident management policy can be included as part of the general information security policy. Incident response procedures can be developed for the security program in general, and for a particular information system, when required.

Control Improvements: None

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

Explanation: The training on incident response can be a part of the general training program

Control Improvements:

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

O.IM-3: INCIDENT REPORTING

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

Explanation: A formal reporting channel for incident, event and weakness of the information system shall be established defined as a part of incident reporting policy and procedure as defined in O.IR-1.

Control Improvements:

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

O.IM-4: INCIDENT RESPONSE

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

Explanation: Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The lessons learned can also be incorporated from ongoing incident handling activities.

Control Improvements:

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

O.IM-5: INCIDENT MONITORING

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

Explanation: A database on all incidents is made available to designated personnel who are responsible to track and review the corrective action taken to prevent the re-occurrence of these incidents.

Control Improvements:

(i) The automatic mechanism / tools shall be deployed to support tracking and reviewing all incidents associated with information system in a specified time

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

Explanation: when a legal action (criminal or civil) against a person or organization is required to be taken following an incident, the evidence collected should conform to basic rule of the evidence i.e admissibility of evidence (whether or not the evidence can be used in the court) and weight of evidence (quality and completeness of evidence established through strong trail) and thus the integrity of the evidence should be maintained throughout its life cycle.

Control Improvements: None

O.SA: SYSTEM & SERVICE ACQUISITION & MAINTENANCE

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

Controls: 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.

Explanation: The security requirements of information system which includes business application, off-the self software application, user developed application, operating system, infra-structure etc. shall be identified prior to its development (may be during requirement phase) and these requirements and controls shall be implemented and maintained during its life cycle.

Control Improvements: None

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.

Explanation: The detailing and granularity of the various phases of the acquisition and maintenance process depends on the classification of the system (based on Risk Assessment) to be acquired. The standard system development life cycle as defined in International Standard may be adopted. These phases can be implemented either by those who makes acquisition or third party suppliers or outsourced partners.

Control Improvements: None

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)

Explanation: During acquisition and maintenance of information system, either new information system can be developed or upgrading of existing system takes place. Configuration management process as defined in "Configuration Management" (O.CM) controls the changes to the system during development / upgrades, tracks the security flaws, integrate the authorization process and facilitate the relevant documentation.

Control Improvements: None

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.

Explanation: The security testing of the information system under development should be carried out to verify the correct functioning of the security requirement and provides the confidence that the system will work satisfactorily during normal operation

Control Improvements: None

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.

Explanation: Technical vulnerability testing and evaluation on the information system in use shall be periodically (at least once in year or as and when new vulnerability is reported) done based on the published technical vulnerabilities and appropriate measures shall be taken if the risk resulting from exploitation of such vulnerabilities to the information system is considerably high.

Control Improvements: None

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.

Explanation: Usually the operation of any information system is highly dependent on the service of the suppliers. Hence, it is necessary to identify through risk assessment the areas that require special attention through formal contract/ agreement to ensure that the security of information system and information processing facilities is not reduced by the introduction of external party

Control Improvements: None

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.

Explanation: The third party agreement usually contains the security requirements (based on perceived risk from the third party), the service definition (e.g. the various types of services provided by third party) and the level of service (e.g. 99% availability of network service)

The implementation as per the agreement by the third party shall be monitored periodically and any decision on change in third party services (service definition & its level) and security requirements and/or third party, if required, is taken.

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

O.BC: BUSINESS CONTINUITY MANAGEMENT

O.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.

Explanation: The key elements of the business continuity management process are: Business impact analysis, Risk assessment, business continuity strategy, Implement standby arrangement, develop recovery plans, implement risk reduction measures, develop business continuity plan, testing and updating the plans and training.

Control Improvements: None

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.

Explanation: None

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.

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)

Explanation: The personnel shall be trained on specific activities of the business continuity plan as per the role and responsibility assigned to them in disaster scenario

Control Improvements:

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

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

Explanation: The various techniques are used to test / exercise the business continuity plan staring from table top testing to complete rehearsal. The extent of testing increases with the impact level of the information system.

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 test s / exercises of the business continuity plan shall also be executed at alternate processing site

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.

Explanation: Few important changes that trigger the revision of the business continuity plans are changes in personnel, address or telephone numbers, business strategy, location, facilities, and resources, legislation, contractors, suppliers, and key customers, processes, risk etc.

Control Improvements: None

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]

Explanation: The location of the storage site is a strategic decision and also depends on the requirement of the “alternate processing site “. The frequency and transfer rate of back-up information are consistent of the business requirements 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

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.

Explanation: The IT infra-structure and information system at alternate processing sites are made available within specified time frame when services from primary site are not available. The time frame to resume information system operation is consistent with recovery time objectives [RTO].

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

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.

Explanation: The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) are consistent with the recovery time objectives (RTO) and recovery point objectives (RPO). While integrity and availability are the primary concerns for system backup information, protecting backup information from unauthorized disclosure is also an important consideration depending on the type of information residing on the backup media

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

O.CO: COMPLIANCE

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

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

Explanation: A process shall be established to independently to verify the compliance of IT security policy & implementation of counter measures as applicable and identified in various class and family.

Control Improvements:

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

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.

Explanation: A process shall be established to independently check that all the legal / Statutory/ regulatory and contractual requirements of the land e.g. privacy laws, IT Act, Copyrights (including licensing issue of software), IPR issues etc are complied.

Control Improvements:

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

7.0 References

[1] eSAFE GD 100: Guidelines for Security Categorization of Information Systems

[2] eSAFE GD 200: Catalog of Security Controls

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

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

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

[6] 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