Audit Program for Data Centers

Audit Objectives

The objective of the exercise is to evaluate the adequacy, effectiveness and efficiency of controls in place to minimize the risk of unauthorized access to the data center, business disruptions, theft of information assets, safety, emergency and environmental hazards.

Areas of coverage

- Personnel procedures and responsibilities addressing employee termination, cross-functional and systems training.
- Backup procedures are adequate to minimize business interruption and protect against loss of data in the event of a disaster.
- Physical security controls are adequate to prevent unauthorized access to data center areas (server, power and communication rooms)
- Environmental controls are adequate to minimize hardware/software losses from fire or flood.
- Safety and emergency procedures are adequacy enough to ensure protection of equipment and human live from damage/jeopardy.
- Power system adequacy and redundancy (alternative power sources and uninterrupted power supply) – STS technology.

Audit Scope

The following areas of data center operations shall be covered: Access to the information processing facility or data center, visitors/vendor restriction, protection of assets, identification of the information processing facility, access to offsite storage facility, policies and procedures, personnel, incident management, safety and emergency procedures (fire and flooding hazard), environmental control (temperature & humidity) monitoring, power system adequacy and redundancy controls, etc. However, specific attention will be paid on the following areas:

- Data center operating policies and procedures.
- Physical security controls.
- Environmental controls.
- Incident handling and management.
- Infrastructure maintenance
- Cabling, racking and telecommunications management.
- Service monitoring and availability management.
- Business continuity management.

- Disaster recovery planning
- Power supply adequacy and redundancy
- Safety and emergency procedures
- Resilience

Data Centre Audit Checklist

S/N	Audit Area	Risk	Control	Test Procedures
1	**PEOPLE AND PROCESS**	Lack of separation of duties, ambiguity in business rules and inconsistency in processes and procedures.	Dept. organogram, Job descriptions, procedure manuals and product documentation.	Obtain the Data Centre organogram as it relates to the organizational structure as well as job descriptions.
				Confirm that each staff has documented job descriptions.
				Interview all the staff in the data center and ascertain the processes and procedures required for the performance of their job functions.

S/N	Audit Area	Risk	Control	Test Procedures
				Ascertain the risks associated with the processes and confirm the adequacy of controls (system and manual) to minimize the risk.
2	**ORGANIZATION AND ADMINISTRATION OF THE DATA CENTRE**	Inconsistent practices and substandard operation of the data center due to lack of standard operating manual.	Document a standard data center operating policy and manual.	Have data center operating policy and manual been documented and approved?
				Are they sufficiently descriptive to guide in the administration and operation of the data center?
				Are the data center operators aware of the existence of the operating manual as well as its provision?
				Is there a procedure in place for the periodic review of the operating manual to ensure that it reflect changes and improvement in the data center operations and ensure compliance to best practice?

S/N	Audit Area	Risk	Control	Test Procedures
		Risk of compromise by the Data Centre Operators due to lack of duty rotation and monitoring of operators' activities.	Maintain a duty roaster to ensure job rotation among the data center Operators.	Verify that data center Operators ensure job rotated? Request for data center duty roaster and confirm rotation of duties in a systematic manner.
				Confirm that the duty roasters are routinely reviewed by the Data Centre Manager.
			Maintain an operator logbook to capture significant events in the data center and corrective actions.	Confirm that operator logbook is maintained to record any significant events/incidents in the data center and corrective action taken by the operator. The log book could be in the form of incident management/reporting software or portal.
				Confirm that every duty shift in the data center writes a handover report on completion of their shift on activities carried out as well as significant issues during the shift to aid smooth takeover by the next shift.
				Confirm that the logbook or portal is reviewed frequently by management.

S/N	Audit Area	Risk	Control	Test Procedures
			Maintain record of End of Day (EOD) or End of month (EOM) activities and processes to prevent system breach, suppression of malicious acts or service failures (in the case of high processing data centre using high end ERP or banking software).	Confirm that all EOD activities and processes are captured in the EOD register or portal to prevent suppression of malicious acts as well as service failures.
				Confirm that EOD/EOM activities and processes are reviewed regularly by the Head of Data Centre to ensure that no service issues or malicious acts are suppressed by the Operators.
				Confirm that incidents recorded during EOD/EOM processing are promptly escalated to relevant persons in management for resolution. Take samples of such incidents for verification if need be.

S/N	Audit Area	Risk	Control	Test Procedures
		Risk of business disruption due to lack of capacity management, monitoring as well as performance measurement of business systems.	Implement capacity management and planning measures.	Ensure that resource monitoring software (like AppManger or ManageEngine) are installed to monitor capacity utilization of resources on all servers of interest especially critical systems and applications.
				Request and examine system resource utilization reports; determine the times of peak resource demand within the processing day. Determine how Data Center management reacts to equipment utilization information.
				Confirm that IT management (IT Steering Committee) receives feedback on system capacity utilization reports, which they may need in planning towards acquisition of servers or applications in the future as part of its strategic functions.
				Determine whether capacity planning (processor, memory, channels, disk, etc.) performed, are consistent with, and integrated into strategic long-term plans.
			Implement performance measurement	

S/N	Audit Area	Risk	Control	Test Procedures
			and monitoring systems.	
				Determine whether performance measurement process services and infrastructure (systems) are in place.
				Determine whether system downtime is recorded or tracked.
				Confirm that alerts/notifications are set to monitor agreed resource thresholds for systems to trigger/alert the Operators when such thresholds are breach or exceed. This is to prevent over utilization of system resources in a manner that will cause damage to the infrastructure. For example, set alert on disk space utilization of the server disk drive, Netapp storage, Dell EMC storage, memory utilization, CPU utilization, etc.
				Confirm that system downtime or outage is effectively monitored to prevent service failure. For example, monitor service UPTIME on AIX/UNIX server.

S/N	Audit Area	Risk	Control	Test Procedures
		Compromise, theft and unauthorized access to backup media and offsite storage facility.	Implement adequate controls to ensure accountability and protection of backup media produced at the main facility as well as their transfer and retrieval to and from the offsite storage facility.	Confirm that all tapes that are sent to the offsite storage facility are properly documented and authorized before their transfer.
				Confirm that the method of transfer of the tapes (by either till box or safe) to the offsite storage facility is secured and adequately protected from theft or compromise. Inspect the box or safe as well as the process of tape transfer to ensure their security.
				Verify whether the tapes and other media are encrypted to prevent them from being accessed or compromised in the event of theft or loss.
				Confirm that the default OEM (Original Equipment Manufacturer) encryption code are changed and not used for encrypting the tape drives during backup. Symantec NetBackup solution as well as other solutions give room for the administrator to create its own encryption codes for use during back up.

S/N	Audit Area	Risk	Control	Test Procedures
				Are all visitors to the off-site facility required to sign a logbook or register their presence indicating their name, reason for visiting, time and date?
				Are the processes of retrieval of storage media (tape and hard drives) documented and adequately controlled to ensure that the right tapes are retrieved and there are proper authorizations?
				Are the storage media (tapes and hard drives) properly index and labeled to facilitate easy storage and retrieval?
3	**ENVIRONMENTAL CONTROL & MONITORING SYSTEMS.**	Risk of inadequate response in the event of fire outbreak and other emergencies.	Ensure that data center operators and other personnel in the main processing facility are adequately trained on how to respond in the event of fire outbreak.	Have the data center operators been adequately trained on what to do when the different types of fire emergencies or security violation occur?
				Do the other personnel in the main processing facility been adequately sensitized on what to do when fire emergencies occur?
				Confirm that fire marshals have been appointed to man key areas of the main processing facility and verify

S/N	Audit Area	Risk	Control	Test Procedures
				that they have been adequately equipped with basic tools to enable them coordinate emergency evacuation activities.
				Ensure that fire drills are frequently conducted in the main processing facility for all occupants to create necessary awareness on how to adequately respond to emergency or fire outbreaks.
			Install fire equipment and other emergency controls and ensure that they are adequately maintained and tested to respond to any fire outbreak.	Are the fire alarm pull boxes and emergency power switches clearly visible, marked and unobstructed?
				Are clear and adequate fire instructions posted in all locations within and around the data center?
				Confirm that emergency phone/ switch numbers of fire service authorities are conspicuously displayed in specific locations around the main processing facility for easy access and use in the event of fire. For example, dial 911 or 123, etc. as applicable.

S/N	Audit Area	Risk	Control	Test Procedures
				Are smoke/heat detectors periodically tested to ascertain their working conditions and ability to detect existence of fire or smoke when the need arises?
				Are smoke detectors strategically installed under the raised floors and on the ceiling of the data center such that will easily detect smoke or fire?
				Are there enough fire alarm pull boxes in and around the data center?
				Are the Operators assigned individual responsibilities in the event of fire outbreaks?
				Are the operators trained periodically in firefighting?
				How frequently are fire drills held?
				Are FM200 fire extinguishers installed in the data center for the purpose of firefighting?
				Are the FM200 fire fighters promptly maintained and serviced in line with the OEM service lifecycle?
				Are the firefighting equipment periodically tested to ascertain its working condition and ability to respond to disaster in the event of emergency?
				Are combustible materials found within and around the data center area? Combustible materials must

S/N	Audit Area	Risk	Control	Test Procedures
				not be kept in around the data center as they are fire fuelers and could aid spread of fire.
			Implement controls that will adequately prevent flooding and other disasters from affecting the data center.	Are the data center installed above raised floor?
				Are the materials used for the raised floor or base of the data center those that are not combustible or aid the spread of fire?
				Are there water lines/pipes or collectors that are through or close to the data center area to avoid flooding?
				Are environmental monitoring and control system (EMCS) installed in the data center and periodically tested to ensure that temperature and humidity conditions within the data center are controlled and monitored.
				Are the EMCS configurations adequate to ensure that triggers/alerts are sent to concerned persons when the temperature and humidity conditions within the data center drops or increases

S/N	Audit Area	Risk	Control	Test Procedures
				above the acceptable limits or threshold?
		Risk of service disruption arising from physical destruction of power and data cables or interception of signals.	Implement a trunked electrical wiring and cabling system in and around the data center to prevent physical damage.	Check to ensure that electrical power cables and wiring in around the data center are well arranged in trunks to prevent physical damage.
				Ensure that there were no exposed power cables to prevent electrocution of personnel.
			Safeguard signal/data cables in PVC trunks to prevent signal interception or tapping for malicious purpose.	Inspect all signal/data cables on servers and network devices to ensure that they are not exposed to interference or tapping.
4	**PHYSICAL AND LOGICAL ACCESS CONTROL TO THE DATA CENTRE**	Risk of unauthorized physical or logical access to the data center.	Implement biometric or smart card entry control device to restrict access to the data center.	Confirm that there is a procedure for granting access to users who have need to access the data center and establish the authorization process.
				Are all personnel entering the data center made to enter through an entry point controlled by either a biometric or smartcard access control device,

S/N	Audit Area	Risk	Control	Test Procedures
				which is monitored by the Data Center Manager?
				Ensure that there is a procedure for the review of the biometric or smartcard activity logs. Confirm that the review is done by the Data Centre Manager.
				Do biometric or smartcard devices restrict and grant access based on the individual's unique access credential, or restrict access to a door(s) for users or at a given time of the day.
				Do the means of gaining access, i.e. biometric or smartcard difficult to duplicate or compromise?
				Are there procedures in place for deactivating user access on the biometric or smartcard devices in the event that they are disengaged from the organization (either voluntarily or terminated by the company or if an employee smartcard is lost or stolen?
				Do the means of gaining access, i.e. biometric/smartcard automatically produce a silent or audible alarm if illegal entry is attempted?

S/N	Audit Area	Risk	Control	Test Procedures
				Do the biometric/smartcard devices automatically log and report successful access and unsuccessful attempts to the data center?
				Is the issuing, accounting for, and retrieving the smartcard/biometric an administrative process that is carefully controlled? Request for smartcards of users that have exited from the organization.
				Can all active smartcards be accounted for?
				Confirm that the access logs of the biometric or smartcard devices are captured and retained for a reasonable period. Verify that the logs are backed up on external media (tapes or HDD) for retention for purpose of investigation when the need arise.
				Are there video cameras located at strategic points in the information processing facility (data center) that are monitored by security personnel? Is the video surveillance recorded for possible future playback?
				Is there an alarm system in place that is linked to inactive entry points to the information processing facility or data center?

S/N	Audit Area	Risk	Control	Test Procedures
				Are employees and visiting technicians required to wear photo IDs or identification badges?
			Monitor and restrict visitors' access to the data center.	Are all visitors required to sign a visitor's log indicating their name, company represented, reason for visiting, and person to see before accessing the data center?
				Before gaining access, are visitors required to provide some method of verification of identification, i.e. Company ID, business card, vendor identification tag?
				Are visitors required to wear identification badges that are a different color from employee badges for easy identification?
				Are visitors required to be escorted by a responsible employee? Such visitors include friends, repairmen, computer vendors, consultants (unless long term, in which case special guest access is provided), maintenance personnel and external auditors.
				Are special service contract personnel, such as cleaning staff and off-site storage services, bonded and monitored during the discharge of their duties to limit the financial exposure

S/N	Audit Area	Risk	Control	Test Procedures
				of the organization or disruption of service?