AUDIT PROGRAM FOR BUSINESS CONTINUITY MANAGEMENT AND DISASTER RECOVERY PLANNING

Audit Objectives

The objective of the exercise is to evaluate the adequacy, effectiveness and efficiency of controls in place to minimize the risk of business/service disruptions as a result system failure or disaster affecting an organization's IT infrastructure or operating environment.

Areas of coverage

- Ensure that adequate and effective contingency plans have been established to support prompt recovery of crucial enterprise functions and IT facilities in the event of major failure or disaster.
- Ensure that all mandated disaster recovery, business continuity, and security requirements have adequate compliance policies and procedures in place.
- Ensure that all the potential risks to the enterprise and its IT facilities are identified and assessed in preparation of the contingency plans.
- Ensure the optimum contingency arrangements are selected and cost effectively provided.
- Ensure that an authorized and documented disaster recovery / business continuity plan is created, maintained up-to-date, and securely stored.
- Ensure that the recovery plan is periodically tested for its relevance and effectiveness.
- Ensure that all internal and external parties to the recovery process are fully aware of their responsibilities and commitments.
- Ensure that appropriate liaison is maintained with external parties (i.e. insurers, emergency services, suppliers, etc.).
- Ensure that both the main and recovery sites are secure and that systems are securely operated in support of the enterprise.
- Ensure that systems and procedures are adequately and accurately documented to aid the recovery process.

S/NO	Audit area	Risk	Controls	Procedure
1.	**BUSINESS CONTINUITY READINESS**	**Inability to adequately respond to emergencies or disasters that have the potential to**	Business Continuity Plan (BCP).	Ascertain that the organization has a Business Continuity Management System in place as well as a BCP document that serve as a policy or procedure document.

S/NO	Audit area	Risk	Controls	Procedure
		disrupt critical services of the organization.		
				Ensure Executive management buy-in in the business continuity plan especially up to the organization's Board of Directors.
				Ensure that it is routinely being tested for workability.
				Ensure that responsibilities have been assigned to the various Emergency Response Teams created by the BCP and that the teams have been constituted and adequately trained on their roles and responsibilities during emergency.
				Is copy of the BCP document maintained in the main site as well as in the DR site?
				Ensure that drills and simulation of disaster situations, a test of the organization's readiness to respond to disaster are being routinely conducted.
				Ensure that a procedure for proper maintenance of all servers and equipment in the data centre as DR site in line with Service Level Agreements (SLAs) entered with their respect vendors.
				Ensure that business impact analysis (BIA) has been carried out and that all the critical information resources and assets are identified and scoped.
				Also, determine if comprehensive risk assessment of the areas and functions covered by the Business Continuity plan has been prepared and that it appears reasonable.
				Ensure that the BIA identifies the risks peculiar with the organization's operations, the likely frequency of their reoccurrence, ranking of the risk as low, medium and high risks. Confirm that they metric for measuring the impact of each risk is reasonable and feasible.
				Evaluate the effectiveness of the documented procedures for the initiation of the Disaster recovery

S/NO	Audit area	Risk	Controls	Procedure
				plan.
				Determine if all critical applications and IT infrastructure (ERP software, Windows servers, Domain controllers, AIX/UNIX servers, Storage systems, etc) have been identified.
				Review planned support available for critical applications & systems, including all core ERP systems.
				Determine if all applications have been reviewed for their level of tolerance and easy of recoverability in the event of a disaster.
				Review the list of business continuity response personnel, emergency hot site contacts, emergency vendor contacts, etc, for appropriateness and completeness.
				Call a sample of people in the list to verify that their phone numbers and addresses are correct as indicated and that they possess a current copy of the business continuity plan.
				Interview key personnel for an understanding of their assigned responsibilities as well as up-to-date detailed documentation describing their tasks in a disaster situation.
				Evaluate the coordination among the business continuity team and external vendors and suppliers.
				Verify if surprise test has been carried out to determine the level of preparedness of and effectiveness of personnel and the plan itself.
			Emergency guidelines and procedures	Evaluate the procedure for updating the Business Continuity plan/manual.
				Ensure that updates are applied and distributed in a timely manner.
				Ensure that responsibilities for maintenance of the manual are documented.

S/NO	Audit area	Risk	Controls	Procedure
				Evaluate the effectiveness of the documented procedures for the initiation of the business continuity plan.
				Evaluate all written emergency & recovery procedures for thoroughness, appropriateness, accuracy and currency.
				Determine if all recovery teams have written procedures to follow in the event of a disaster.
				Determine if a suitable procedure exists for updating the written emergency procedures.
				Determine if user recovery procedures are documented.
2.	**DISASTER RECOVERY SITE.**	Inability to recover from emergency situations or unplanned disruptions in a timely manner that will impact on the organization's ability to deliver services to its customers.	Disaster Recovery Plan (DRP).	Obtain and review a copy of the disaster recovery plan and the DR site agreement. Determine if they are complete and current, and if executive management has signed off on the plan.
				Determine who was responsible for developing the plan and if users and all facets of data processing were adequately involved in its development.
				Determine if executive management has approved the funding for the DR site and testing of the disaster recovery plan. Observe a test of the plan.
				Observe a test of the plan if possible within the audit period and review the results of the test of the disaster recovery plan (DRP). Determine if corrective action has been taken on any problems encountered during the test.
				Visit the DR site. Assess its suitability and compatibility with the main processing facility.

				Interview users and/or IT personnel in the DR site to determine if they have been trained in their responsibilities in the event of an emergency or disaster. Also determine if they are aware of manual procedures that are to be used when processing is delayed for an extended period of time.
				Ensure that all the procedures for Contingency/Recovery are documented e.g. Data Centre Operating Procedures.
				Has the maximum allowable outage and recovery time objectives been determined? Ascertain the adequacy of the recovery time for information resources in which business processing must be resumed before significant or unacceptable losses are suffered.
				Review the results of prior tests plan to determine whether actions requiring correction have been incorporated into the plan.
				Perform detailed inventory review of the offsite storage facility to ensure the presence, synchronization and currency of critical media and documentation including: Data files, applications software, applications documentation, systems software, systems documentation, operations documentation, necessary supplies, special forms and a copy of the business continuity plan.
				Evaluate the security at the offsite facility to ensure adequacy of proper physical and environmental access controls.
			Contingency plan for DR site (i.e. Recovering from recovery).	Ensure that the plan adequately addresses relocation/movement to a new information processing facility in the event that the original DR site cannot be restored.
				Determine if the plan adequately addresses recovering from recovery.
				Determine if terms necessary for the reconstruction of

				the Information processing facility are stored offsite which include: Blueprints, Hardware inventory, Wiring diagrams, etc.
			Storage of Data Backup media in offsite facility.	Ascertain that telecommunication backups are addressed in the plan.
				Ascertain that the plan address loading data is processed manually into an automated tape management system.
				Ensure that regular and systematic backups of files required for sensitive and/or crucial applications and data exist.
				Ascertain that offsite storage is used to maintain backups of critical information required for processing operations, either on- or offsite.
				Ensure that adequate documentation exists to perform a recovery in case of disaster or loss of data.
				Assess the vital records retrieval capacity.
			Insuring the DR site against collateral damage to prevent huge financial losses to the bank.	Verify if the organization's investment in the DR site and its infrastructures are covered by insurance to avert possible losses. Determine as a matter of policy that investment in the DR site are covered by an insurance company.
				Review insurance coverage for adequacy taking into consideration: i. Insurance premium (cost). ii. Coverage for media damage. iii. Business interruption. iv. Equipment replacement. v. Business continuity processing.

S/NO	Audit Area	Risk	Controls	Procedure
3.	**DISASTER RECOVERY SITE AS A DATA CENTRE.**	Unauthorized physical or logical access to the DR site data centre.	Adequate physical and logical protection to prevent unauthorized entry.	Ensure adequate entry control (biometric or smart card device) is used to control access within the DR site data centre.
				Ensure that there is a procedure in place for assigning and retrieval of access from personnel that work in the DR site data centre.
				Ensure that all personnel that work within DR site data centre area are authorized by their supervisors and have need to access the centre.
			Adequate audit trail users' activities within the DR site data centre.	Ensure that sufficient audit trail of users' access are being capture by the biometric or smart card device software.
				Ensure that the captured access logs are backed up externally for retention in the event of system crash or disaster affecting the main facility.
				Ensure that CCTV cameras were strategically installed in the DR site data centre and that specific entry areas were covered.
				Ensure that CCTV DVR recorder keep audit trail of activities within the data centre for reasonable period of time as specific in the policy as well as best practice.
		Impact of environmental and external conditions such as fire, flooding and other disasters in the DR site data centre.	Adequate protection from environmental conditions such as fire, interference, flooding, etc.	Ensure those FM 200 fire extinguishers were installed and routinely tested in the DR site data centre to forestall any incidence of fire outbreak.
				Ensure that smoke detectors were installed and routinely tested in the DR data centre for prompt detection of smoke or fire.

S/NO	Audit Area	Risk	Controls	Procedure
				Ensure that Environmental Monitoring & Control System (EMCS) was installed and routinely tested to detect change in environmental conditions (such as temperature and humidity) within the DR site data centre that went beyond acceptable thresholds while promptly alerting responsible personnel for their action.
				Ensure that the fire alarm system in the centre is in good working condition and are routinely tested.
				Ensure that are good security practices within the centre and that drills are routinely carried out to ensure adequacy of the emergency and evacuation procedure established for the DR site data centre.
				Ensure the adequacy of the power supply of the DR site data centre in delivering pure and uninterrupted power.
	Prepared By:	**Oxley Technologies Inc.**		