Audit Program – Business Continuity

Objective - Provide management with an independent assessment of the effectiveness of the business continuity plan and its alignment with subordinate continuity plans, evaluate the enterprise's preparedness in the event of a major business disruption and identify issues that may limit interim business processing and restoration.

The scope of this audit included:

- Ascertain the existence and effectiveness of the current hospital business continuity plan and its alignment with the enterprise business continuity plan, policies and procedures.
- Evaluate IS function's preparedness in the event of a process disruption.
- Evaluate Business Unit (hospital) function's preparedness in the event of a process disruption.
- Determine compliance with applicable federal laws and regulations.

Controls are not in place to ensure that a Business Continuity Plan exist and is properly documented			*Review policies and procedures for Business Continuity plan.*
	P&P	1	Determine if there is a documented BCP (obtain copy)
		2	Has senior management signed off on the plan? How often is it reviewed and approved by senior executives
		3	Is there documentary evidence of all reviews/approvals
		4	Has the plan been communicated / distributed to all stakeholders?
		5	Ascertain identity of the BCP business officer (contact information)
		6	Ascertain identity of the BCP planner (contact information)
		7	Does the plan list recovery strategies?
		8	What is the process for keeping the plan up to date?
		9	Determine if a copy of the contingency plan is stored offsite. (at the hot site)
		10	Is an off-site data processing facility (HOT SITE) in contract for a disaster? (obtain contract)
		11	Inquire and obtain evidence that funding has been allocated for BCP efforts
		12	Are there subsidiaries that must be notified in the event of a disaster? If so are the subsidiaries names and contact numbers included in the plan.
Incident response responsibilities are clearly defined and routinely executed.			*Obtain and review the Incident Response policies and procedures.*
	Incident Response	1	Obtain incident response policies and procedures
		2	Incident drills are scheduled.
BIA methodology is not defined and implemented			*Obtain and review the Business Impact Analysis*
	BIA	1	Determine if a comprehensive BIA is the basis for business continuity decisions

	2	BIA Methodology used; Obtain BIA forms used
	3	Does BIA identify business continuity teams comprised of key operations and system management and their emergency contact numbers.
	4	Includes teams roles and responsibilities
	5	Determine that the organization has determined RTOs (Recovery Time Objectives) and RPOs (Recovery Point Objectives) for each critical application
	6	Assess that the RTOs and RPOs are practical and reasonable for each application and line of business or function.
	7	Includes vendor contact information (Iron Mountain, Telecom, etc.) and their related products
	8	Tape backup recall procedures current and up-to-date
	9	Clearly defines responsibilities for designated teams or staff members.
	10	Explains actions to be taken in specific emergency situations.
	11	Lists (for each dept.) primary and secondary levels of staffing, material and headcount required to resume operations.
	12	Identifies and documents each businesses recovery objectives and critical recovery time frames.
	13	Documents the current processing environment inclusive of all systems, applications, networks, and data, supporting business functions on a normal operating day.
	14	Ensure that all personnel information listed in the BCP is current (review personnel files / active employee list)
	15	Includes maps or directions to the alternate site
	16	Does BCP list the actions necessary for each business area to take in event of a disaster?
	17	Details of alternate office space
	18	Contains a plan for reconnecting to the network
Business Continuity is not an integral component of Enterprise Risk Management Program.		*Obtain, if available the ERM performed for Business Continuity*
Risk Management	1	Was a risk assessment performed? (under ERM)
	2	Obtain management meeting minutes
	3	Obtain risk management documents
Controls are not in place to ensure that the Business Recovery plan exists.		*Obtain and review the results of the business continuity recovery plan.*
Recovery Plan	1	Does a recovery plan exist? If so, obtain a copy of the plan.

		2	Determine if a business continuity recovery plan has been kept current and reflects relevant changes to business processes
Controls are not in place to ensure that the BC plan is tested.			*Obtain and review the results of the business continuity plan test.*
	Plan Test	1	Does a testing cycle exist to ensure that the plan is tested on a regular basis?
		2	Determine if a business continuity plan been tested regularly
		3	Does testing policies exists?
		4	Determine if testing included both walkthroughs and full scale drills of the interim process and recovery plans.
		5	Determine if test results were documented and necessary updates/corrections made to the plan? Obtain copy.
		6	When was the plan last tested?
		7	Has senior management been informed of testing and results?