PENN: Mission Continuity Program: Questions contained in review tool

Fall 2012

1. Are controls in place to ensure IT continuity plans address all key business functions and processes?

2. Is the IT continuity plan tested on a regular basis?

3. Does the testing consider the appropriate scope? (single applications to integrated testing scenarios to end-to-end testing, and integrated vendor testing)

4. Do all concerned parties receive IT continuity plan training?

5. Are controls in place to ensure all relevant parties receive the IT continuity plan training on a regular basis?

6. Are procedures in place to ensure the IT recovery times are understood by business management?

7. Do IT recovery action plans specify customer and stakeholder communications?

8. On successful resumption of the IT function, after a disaster has occurred, is there a review performed to assess the adequacy of the IT recovery plan?

9. After a review has been performed to assess the adequacy of the IT recovery plan, is it updated accordingly?

10. Are change control procedures followed to ensure the IT continuity plan continually reflects actual business requirements?

11. Do the change control procedures ensure clear and timely communication of changes in IT contingency procedures and responsibilities?

12. Are procedures in place to ensure there are recovery testing documentation and testing results?

13. How often is the continuity plan tested?

14. Does the test schedule for BCP indicate how and when each element of the plan should be tested?

15. Are individual elements of the business continuity plan tested frequently?

16. Do the business continuity plans include testing technical recovery?

17. Do the business continuity plans include testing recovery at an alternate site?

18. Do the business continuity plans include testing of supplier facilities and services?

19. Do the business continuity plans include the use of complete rehearsals?

20. Are controls in place to ensure the recovery plan been distributed to all appropriate personnel?

21. Are procedures in place to ensure the vendors' services will be available during an interruption to the company?

22. Does the DR plan include an inventory of assets needed for offsite recovery (example: backup tapes, operating system software, credit cards for travel expenses, etc.)?

23. Have the guidelines for the recovery/alternate work been defined (e.g., number of seats, number of computers, type of printer, etc)?

24. Are documented guidelines followed for offsite storage to ensure periodic test and restoration of archived data?

25. Are controls in place to ensure that back-up media are regularly tested to require they can be relied upon for emergency use?

26. Do you have at least five Action Plans, one for each element of the BETH3 model (Loss of Building, Loss of Equipment, Loss of Technology, Loss of Human Resources, Loss of Third-Party Partner/Vendor)?

27. Is each of your action plans organized in the Mission Continuity software tool according to the provided columns: Trigger, Action, Responsible Person(s), Procedures?

28. Do you have Roles defined and populated with specific people?

29. Do you use your pre-defined Roles to populate the Responsible Person(s) column in your plans?

30. Do you have Call Lists included under the Contacts section within the Mission Continuity software tool?

31. Do you have a copy of your plans stored or printed elsewhere besides in the Mission Continuity software tool, such as in hard copy and/or on a flash drive, and kept off-site?

32. Are your plans (and the copies that are kept off-site) updated on a regular basis, such as every quarter, every six months, or every year?

33. In addition to updating personnel changes, how often do you review your overall plans with your plan owner / leadership?

34. Have you performed tabletop tests to test your plans and revise them based upon experience?

35. Have you included an incident response plan in Shadow Planner?

36. Have you ever had to activate your plan?

37. Does your plan take into consideration any applicable compliance with regulatory requirements (e.g., HIPAA, PCI Compliance, etc.) and/or 3rd party vendor contracts that would affect your department?