sifma

COB Assessment for EXISTING Suppliers

Review of Plan/ Recovery Strategy/ Testing/ Regulatory

1. Have there been any changes to the location recovery strategy for your facilitites (technology and staff)
   If so, please explain

2. Have there been any major software or hardware changes to the systems servicing XXX in the past year?
   If so, please explain

   If changes were made, how are the changes managed and applied to the recovery environment

3. If you answered yes to #1 or 2, please explain how the approach to testing has changed over the previous year (e.g. types of tests, volumes tested, success measures, etc.)

4. What impact have the changes noted above had on your recovery plan? Have you updated the recovery plan to include changes made in #1 or 2 above?

5. Have any key employees responsible for recovery activities left the organization in the past 12 months?
   How have implications on recovery been addressed?

6. If you use subcontractors for disaster recovery of products / services / applications provided to XXX, have there been any changes in relationship (i.e. contract renewal, change of service) that would impact recovery and your ability to provide services to XXX?

7. Did you submit copies of business/technology continuity tests completed in the last year? If not:
   a) What were the test results?
   b) Were the recovery timeframes achieved?
   c) If not, were all issues remediated?
   d) What is outstanding to be remediated?

8. For failed tests, was the test rescheduled? What was the result?

9. Has this business process / application experienced an outage, incident, and/or invocation within the past year?
   a) What was the cause? Has it been fully remediated?
   b) Were the recovery timeframes achieved?

10. Have any regulatory agencies or other parties identified any issues that could hinder your ability to recover in the event of an incident? If so, what is/was the issue and has it been fully resolved?

COB Assessment for NEW Suppliers

Planning

1. Describe the recovery strategy, the capacity in which you operate (as a percentage of production capacity), and the duration you are able to sustain in each of the following scenarios:
   a) Loss of Workspace (DOA) ie: dedicated recovery seating for 100% of critical staff for x duration- to be defined
   b) Staff unavailability ie: Pandemic Planning
   c) Loss of technology (DOS) ie: full site outage, partial site outage, application outage (100% recovery capability for all tech)
   d) Cyber attack ie: wide scale accessibility impact across businesses and locations
2. How often are your recovery plans updated?
   a) Annually? b) Less Frequently c) More Frequently
3. What is the process to update recovery plans? Are emerging threats included in the planning process? If so, which threats are you addressing

Testing

4. What is your approach to testing to ensure that recovery timeframes and strategies (as specified in question #1) can be achieved (e.g. types of tests, volumes tested, success measures, etc.)?
5. When was the Business Continuity / Technology recovery plan last tested and what were the test results? Were the recovery timeframes achieved? If not, what were the issues and were they all remediated?
6. How frequently do you conduct testing of your Business / Technology plans? Is there a testing requirement that is tied to plan modifications? i.e: change to Business or Technology environment results in change to plan and testing
7. Describe how the network is tested and restored in DR. Is the same IP address schema used in production and DR?
8. How do you test recovery of core infrastructure & technology (e.g. power, cooling, network links, critical hardware and software)?
9. Describe your process and results for batch recovery testing (if applicable) How are jobs synchronized between production and DR?

Change Management- Storage and Recovery

10. Is there a change process in place to ensure that your production and back up environments (technology) remain in synch? If yes, please describe. If no, please describe how you manage change
11. Do you have equal capacity in both your production and recovery environments? If not, please describe your strategy to ensure full recovery capability
12. What is your process for restoring physical and virtual servers?
    a) Physical to Physical b) Physical to Virtual c) Full virtual d) Other (please describe)
13. How is production data stored and what is the process and frequency of replication? Ie: DASD, Local Disk / replicated daily, hot/hot

Sub-Contracting

14. Do you outsource any of your services and / or products to an alternate provider/ subcontractor? If so, please describe the services provided by each
15. What is the process to review and monitor the business continuity plan and recovery resources of your subcontractor(s)? How do you ensure that the subcontractor's business continuity plan(s) include or address recovery strategies for scenarios outlined in question #1?

Proximity

16. Where are the Primary and Recovery sites located?
17. Is the recovery site at a sufficient distance to avoid proximity risk (risk that an event could simultaneously affect both sites)
18. If multiple customers are affected by the same event, will the recovery timeframes in still be delivered to XXX? If yes, what processes and technology are in place to ensure this? If no, please describe the strategy to address XXX's Service Level Agreement requirements

Incident and Crisis Management

19. Has this business process / application experienced an outage, incident, and/or invocation within the past two years?
    a)What was the cause? Has it been fully remediated?
    b)Were the recovery timeframes achieved?
20. Please describe your Crisis Management Plan, including the following:
    a) Roles and Responsibilities, including contact information of key personnel
    b) Crisis Management procedures/protocols
    c) Location of primary and recovery command centers
    d) Frequency and procedure for review and update of the Crisis Management Plan

Regulatory

21. Have any regulatory agencies or other parties identified any issues that could hinder your ability to recover in the event of an incident? If so, what is/was the issue and has it been fully resolved?