******

***BCP/DR Onsite Third Party Review Framework***

The purpose of this document is to allow a staff member who doesn’t have much experience in BCP/DR/Resilience but is doing a site visit to be able to ask questions on behalf of the BCP function within your firm and collect data for your review and assessment. The questions were designed to be asked by anyone however, we do recommend that a BCP professional go over the questions with the person(s) who’ll be doing the site visit so that they have an understanding of what you’re asking for and will be able to take better notes. As questions are asked, the focus should be to emphasize the relevance of the specific services provided by the third party to the reviewer's organization.

|  |  |  |
| --- | --- | --- |
| ***Assessment Areas*** | ***Required for BCP*** | ***Required for DR*** |
| ***Risk Assessments and Business Impact Analysis (BIA):*** |
| * How often are they conducted and/or refreshed?
 |  |  |
| * How do they do them?
 |  |  |
| * Are all facilities and departments taken into account?
 |  |  |
| * What are the recovery time objectives (RTOs) and recovery point objectives (RPOs)?
 |  |  |
| * Are the RPOs and RTOs provided the same or an improvement over the stated contractual and service level requirements?
 |  |  |
| * Do they do separate ones for business and technology functions?
 |  |  |
| ***BCP/DR Program:*** |
| * Published Program Exists
 |  |  |
| * Includes a maintenance/history log
 |  |  |
| * Notes who approved it and when
 |  |  |
| ***BCP/DR Plans:*** |
| * Maintenance Schedule (may be in the overall Program)
 |  |  |
| * Recovery Strategies Listed (may be in the overall Program)
 |  |  |
| * Critical Dependencies (e.g., applications, departments, vendors)
 |  |  |
| * Is there a secured repository for all recovery documentation?
 |  |  |
| ***Testing Program and Documentation:*** |
| * Published Testing Strategy (may be part of overall Program)
 |  |  |
| * Types of Testing Performed (may be part of overall Program)
 |  |  |
| * Do they include clients in their testing?
 |  |  |
| * Reporting process for test results (may be part of Program) – internal and external if they include clients
 |  |  |
| * Issue Tracking/Remediation Process (may be part of overall Program)
 |  |  |
| * If electronic information is stored or exchanged with the third party do DR exercises validate connectivity to the firm and a software-based recovery point data replication from the secondary (DR site) instance of the vendor's application systems
 |  |  |
| ***Pandemic Planning:*** |
| * Do they have a published program and plan in place?
 |  |  |
| * How often is it reviewed and exercised?
 |  |  |
| ***Incident Response:*** |
| * Is there a published program/process?
 |  |  |
| * Are there defined roles and responsibilities?
 |  |  |
| * Does the program include how communications are done and who performs them?
 |  |  |
| * Does the program include notification to clients?
 |  |  |
| * Are there formalized response teams in place?
 |  |  |
| * How often is this exercised?
 |  |  |
| ***Training and Awareness:*** |
| * Is there a published training program (may be part of overall Program)?
 |  |  |
| * What’s the training frequency?
 |  |  |
| * Who’s required to take the training and how often?
 |  |  |
| ***Plan Audit:*** |
| * Is there an internal audit performed on the program and if so, how often?
 |  |  |
| * Is there an external audit performed on the program and if so how often?
 |  |  |
| * Are the findings included in reports such as SSA16 or SOC II?
 |  |  |
| * Is this vendor subject to regulatory review and if so, which agency and how often?
 |  |  |
| ***Third Party/Vendor Due Diligence:*** |
| * Is there a program/process in place to perform risk reviews on Third Parties to determine their resilience?
 |  |  |
| * Are critical third parties subject to more stringent reviews?
 |  |  |
| * Is there review done to determine concentrations of risk with all vendors (all in the same geography, a large number of functions done by the same vendor, etc.)?
 |  |  |

***Physical Site Review:***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Area*** | ***Yes*** | ***No*** | ***N/A*** | ***Notes*** |
| Does the facility appear clean and orderly? |  |  |  |  |
| Does facility security appear to be equal to if not better than yours? |  |  |  |  |
| Are all entry points secured? |  |  |  |  |
| Would you feel comfortable in working there? |  |  |  |  |
| Is there onsite monitoring 24x7x365? |  |  |  |  |
| Do they have video surveillance systems? |  |  |  |  |
| Do they keep video logs of what happens and how long do they retain it? |  |  |  |  |
| Did they make you log in, wear a visitors badge of some sort? |  |  |  |  |
| Were you escorted at all times? |  |  |  |  |
| If you were given a tour, did the person giving you the tour appear to be knowledgeable and also have pride in the maintenance of the facility? |  |  |  |  |
| If you were taken to their data center(s), is there extra security compared to the other facilities you visited? |  |  |  |  |
| Does the data center appear to clean, orderly and in good condition? |  |  |  |  |
| Is there onsite monitoring of the data center 24x7x365? |  |  |  |  |
| Do they have video surveillance systems for the data center? |  |  |  |  |
| Do they keep video logs of what happens at the data center and how long do they retain it? |  |  |  |  |
| Did they make you log in, wear a data center visitors badge of some sort? |  |  |  |  |
| Were you escorted around the data center at all times? |  |  |  |  |
| If they show you their data center power plant, does it appear to be clean and orderly? |  |  |  |  |
| Did the person giving you the tour of the data center appear to be knowledgeable and also have pride in the maintenance of the facility? |  |  |  |  |
| ***Other Notes/Observations:*** |

Tips on how to do these:

* BCP – is focused on the people and process side of recovery
* DR – is focused on the technology and process side of recovery
* If this is a business process based contract – they’ve got people doing work on our behalf – focus on the BCP part
* If this is a technology based contract – providing data, processing trades, etc. – focus on the DR part
* Have them walk through the entire program which, in many cases, should go over most of these points.
* If possible, try and obtain copies of any documents – highly unlikely as most of this is very sensitive.
* Ask them if they’re willing to talk to BCP and DRP people about this.