[Department/Organization]

**[Campus]
Business Continuity Checklist
As of [Month xx, 20xx]**

The attached checklist is a ***tool*** designed to perform an internal audit assessment or a self-assessment of the state of business continuity (BC) and disaster recovery (DR) within a particular department or business unit. This checklist can be used as a resource to identify areas where security safeguards may be needed, or where existing security safeguards may need to be improved.

For simplicity, the checklist follows a structure of administrative, physical and technical safeguards, organizational requirements, and policies, procedures, and documentation requirements. The checklist is broken down into the following columns:

* Controls and Testing – required control along with a description and the testing procedure (if applicable).
* Assessment Date – actual date the control/testing was reviewed by the assessor.
* Assessment – four columns representing the actual date of assessment/testing and the opinion of the assessor on the completeness of the control/test.
	+ AD – control/test is viewed as adequate by the assessor.
	+ CP – control/test is viewed as compensating by the assessor.
	+ IA – control/test is viewed as inadequate by the assessor.
	+ N/A – used when this particular type of control/test does not apply to departmental systems or processes.
* References – source documentation pertaining to the control/test.
* Observations – comments by the assessor if the controls/tests could use improvement.

Definitions and Bibliography follow the Business Continuity & Disaster Recovery Checklist.

**Obtain a copy of the following documents:**

D1) Copy of IT Disaster Recovery Plan for areas/systems in scope of the review. *(A.2, A.4, A.6, A.8, A.24)*

D2) Copy of the Business Continuity Plan(s) for the key business areas that utilize the systems in the scope of the review. *(A.4, A.6, A.8)*

D3) Copy of the last Business Impact Analysis. *(A.7, A.21, A.22, B.9, B.14)*

D4) Inventory list and pertinent information for information technology components within the scope of the review to include but not limited to: *(B.4, B.11, B.13, B.14)*

1. Applications/systems (in-house or vendor purchased vendor name and hosting hardware)
2. Hardware and its physical location
3. Databases (type and hosting hardware)
4. Ancillary Hardware (printers, workstations, laptops smart phones, etc...)
5. Infrastructure systems (i.e. network, telecommunications, operating systems, web services vendor connectivity, operating systems, e-mail, etc...)
6. Support Software/Systems (i.e. federated access systems, federal government grant systems, etc…)
7. Interfaces and timing requirements.

D5) Vendor contact list and call tree. *(B.3, F.4)*

D6) Employee contact list and call tree. *(A.5, A.9, B.1, F.3)*

D7) Results/summary of last three IT Disaster Recovery Plan tests conducted including resulting action plans and current status of those plans. *(Section E)*

| **Controls and Testing** | **Assessment** | **Criteria** | **Observations** |
| --- | --- | --- | --- |
| **Date** | **AD** | **CP** | **IA** | **N/A** | **Reference** | **Chapter** |
| **A. MANAGEMENT, PLANNING & MAINTENANCE** |
| 1. | Does senior management support the development of an IT DR plan? |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2 |  |
| ANSI | 4.6.1, 4.6.2, 4.3.1  |
| NIST 800-34 | 2.1, 3.1, 2.2.6 |
| 2. | Are the roles of senior management in the planning, development and execution of an IT DR plan clearly defined? (this may be part of an overall Business Continuity Planning Process)*Note: See documentation D2 from above.* |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2 |  |
| ANSI | 4.4.2, 4.4.1, 4.2.1, 4.2.2 |
| NIST 800-34 | 2.1, 3.1, 2.2.6 |
| 3. | Is there an IT senior management representative assigned to the overall Business Continuity decision making, command center, and public relations committee(s)? |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2 |  |
| ANSI | 4.4.1, 4.6.1, 4.2.1, 4.4.1 |
| NIST 800-34 | 2.2.1 |
| 4. | Has the IT Disaster Recovery Plan been approved by the university board or high level executive council and/or the executive in charge of the area in the scope of this review. The IT Disaster Recovery Plan approval may have been a part of the overall Business Continuity Plan that was approved.*Note: See documentation D1 and D2 from above.* |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2 |  |
| ANSI | 4.4.1, 4.2.1 |
| NIST 800-34 | 2.2, 2.2.6, 3.1, 3.2 |
| 5. | Have key personnel been identified as responsible for plan development and maintenance. Is this part of their overall job description and assigned functions?*Note: See documentation D6 from above.* |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.4.1, 4.4.3, 4.2.2  |
| NIST 800-34 | 2.2, 3.1, 3.2 |
| 6. | Has a standard medium and templates been selected for documenting the plan (e.g. DR planning system with a data base, word processing, etc..)*Note: See documentation D1 and D2 from above.* |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.1.1, 4.4.1 |
| NIST 800-34 | 2.1, 3.4 |
| 7. | Are assumptions made in the planning documented and aligned with the university’s key business functions and Business Impact Analysis results?*Note: See documentation D3 from above.* |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.1, 4.3.3 |
| NIST 800-34 | 3.2, 3.2.1, 3.2.2, 3.2.3 |
| 8. | Is the plan well organized and easy to follow?*Note: See documentation D1 and D2 from above.* |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3, 4.3.1 |
| NIST 800-34 | 3.5, 3.6 |
| 9. | Are employees familiar with their responsibilities for developing, maintaining and execution of the plan?*Note: See documentation D6 from above.* |  |  |  |  |  | OK IT | 5.1, 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.2.1, 4.4.1, 4.4.2 |
| NIST 800-34 | 3.5, 3.5.2 |
| 10. | Has a budget been approved for IT Disaster Recovery planning? |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.1.1, 4.3.1 |
| NIST 800-34 | 2.2, 2.2.6 |
| 11. | Did the threat analysis take into consideration various types of risks that could affect plan development: 1. natural disasters
2. willful damage
3. loss of critical employees
4. telecommunication failures
5. disgruntled employees
6. disgruntled students
7. other…
 |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.1.1, 4.2.1, 4.3.1 |
| NIST 800-34 | 2.1, 3.4, 5.3.1, 5.3.2 |
| 12. | Did the risk evaluation take into account the following key IT processes affecting a timely business system recovery?1. Performance monitoring
2. Capacity planning
3. Asset Management
4. Security
5. Incident response
6. Help desk
7. Virus protection
8. Patch application and tracking
 |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.1, 4.3.3, 4.1.1  |
| NIST 800-34 | 2.1, 2.2.7 |
| 13. | Were IT employee considerations assessed during the risk evaluation? Such considerations are to include:1. Employee turnover
2. Employee expertise
3. Employee availability
4. History of workplace violence
5. Compensation
6. Excessive reliance on key employees or contractors
 |  |  |  |  |  | OK IT  | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.1, 4.3.3, 4.4.2  |
| NIST 800-34 | 2.1, 2.2.7, 5.1 |
| 14. | Were the following voice and data communication infrastructure considerations addressed? Such considerations are:1. Single points of failure (local central office and inter-exchange carrier)
2. Voice communications path outside of demarcation point
3. Data communications path outside of demarcation point
4. PBX failure
5. Threat of inadvertent cable cuts
6. Performance and scalability degradation
7. Usage of network diagnostic and/or troubleshooting software.
 |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 3.4.6, 4.3.1, 4.3.3  |
| NIST 800-34 | 2.1, 5.1, 5.3 |
| 15. | Were all major communications methods addressed (e.g. radio, satellite, cellular, internet, phone, email, etc...)? |  |  |  |  |  | OK IT | 8.2, 8.3 |  |
| ANSI | 4.3.1, 4.3.3, 4.4.3 |
| NIST 800-34 | 2.1, 2.3, 2.2.3, 5.4 |
| 16. | How often is the plan updated? Are there key trigger points within the purchasing and change management procedures that trigger plan updates? |  |  |  |  |  | OK IT | 8.2, 8.3 |  |
| ANSI | 4.4.5, 4.6.1, 4.2.1, 4.4.7 |
| NIST 800-34 | 3.6 |
| 17. | Are all changes to personnel, services and processes utilizing automated services communicated to IT Disaster Recovery planning personnel? How are these changes communicated and are they effective? Have all changes that are communicated applied to the DR plan in a timely manner? |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3, 4.4.4, 4.4.6 |
| NIST 800-34 | 2.2.6, 3.6, 4.2 |
| 18. | Is a backup of the plan stored off-site (preferably at the backup site and/or command center)? |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.4.5, 4.6.1, 4.4.7 |
| NIST 800-34 | 2.1, 3.4.2, 3.4.3, 3.6, 5.1.2 |
| 19. | Do key personnel (IT triage team, IT senior decision maker, BC Command Center Chair) have a copy of strategic portions of the plan, know the location of the backup copy, and have access to backup copy? |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.4.5, 4.6.1 |
| NIST 800-34 | 2.1, 3.6, 5.1.2 |
| 20. | Is there a log of all maintenance performed on the plan? |  |  |  |  |  | OK IT  | 8.1, 8.2, 8.3 |  |
| NIST 800-34 | 2.1, 3.6, 4.4.3, 4.4.4 |
| NIST 800-92 | 3.2, 4.1, 4.2, 5.1.2 |
| 21. | Has a Business Impact Analysis been performed? * Did the analysis include the identification and documentation of IT recovery requirements such as RTO’s, RPO’s, and critical period timeframes for each business process?
	+ Data recovery points that are acceptable to meet Business Recovery Point Objectives (RPO’s). How much data can they afford to lose?
	+ Recovery time frames that are acceptable to meet business Recovery Time Objectives (RTO’s). How soon do they need the process fully recovered including the technology portions?
* Was a BIA conducted on all applications and system to determine the business processes impacted?

*Note: See documentation D3 from above.* |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3. 1, 4.3.3 |
| NIST 800-34 | 3.2, 3.2.1, 3.2.2, 3.2.3, 5.1.1 |
| 22. | Is the Business Impact Analysis reviewed and updated regularly, with special attention to new technology, business changes, migration of applications to new solutions, etc...?*Note: See documentation D3 from above.* |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3. 1, 4.3.3, 4.6.1  |
| NIST 800-34 | 2.1, 3.2, 3.2.2, 3.2.3, 3.6, 5.1.1 |
| 23. | Do Backup plans include all critical data, programs, documentation and support items (critical resources) required to perform essential tasks during recovery period? |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.1. 1, 4.3.3, 4.4.5  |
| NIST 800-34 | 3.1, 5.1, 5.2, 5.3, 5.4 |
| 24. | Does the DR plan complement the organization-wide Business Continuity Plan in terms of recovering key systems in line with business process recovery objectives?*Note: See documentation D1 from above.* |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.1.1, 4.6.1 |
| NIST 800-34 | 2.1, 2.2.6, 3.1, 3.4 |
| **B. PLAN CONTENT – Does the plan include:** |
| 1. | A listing of required staff and alternates with their non-work contact numbers. (home, cell, neighbor, relative, email, Facebook, twitter, etc...) *Note: See documentation D6 from above.* |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3, 4.4.1 |
| NIST 800-34 | 2.1, 2.3, 4.2 |
| 2. | Are there any staffing alternatives, if needed staff is unavailable? Procedures for acquiring alternate system experts if needed (i.e. vendors, temporary agencies, etc...) |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3, 4.4.1, 4.4.2 |
| NIST 800-34 | 2.1, 2.3, 4.2 |
| 3. | A listing of vendor contacts to include (authorized contacts, business and alternate phone numbers, authorization codes, system names, etc...)*Note: See documentation D5 from above.* |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.1.1, 4.3.3 |
| NIST 800-34 | 2.1, 4.2 |
| 4. | A listing of required voice and data lines needed for recovery of both voice and data services along with respective phone numbers.*Note: See documentation D4 from above.* |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.1.1, 4.3.3 |
| NIST 800-34 | 2.1 |
| 5. | The location of alternate business office or service office sites and respective contact numbers (main offices, leasing offices, conference room numbers, etc...) |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.1.1, 4.3.3 |
| NIST 800-34 | 2.1 |
| 6. | Roles and responsibilities of all IT staff/teams? And the sequence and how they will be notified of decisions made that affect their ability to carry out their recovery responsibilities. (Disaster Organization Chart). Are there teams/responsibilities clear defined for:1. A management team to officially declare a disaster?
2. An offsite recovery team(s) to recover IT systems?
3. An onsite team to clean up the former IT environment?
4. A resumption team to focus on the permanent rebuild of the IT environment?
 |  |  |  |  |  | OK IT  | 8.1, 8.2, 8.3 |  |
| ANSI | 4.1.1, 4.4.2, 4.3.3 |
| NIST 800-34 | 2.1, 5.1, 5.2, 5.3 |
| 7. | Assumptions made in plan development? Is it very important if they affect recovery efforts? |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.1.1, 4.3.3 |
| NIST 800-34 | 3.1, 3.2, 3.5 |
| 8. | Conditions under which a disaster recovery site would be used? Decision responsibilities for use of the backup site? Procedures for notifying backup site if maintained by a vendor or another institution? Location of the backup site (hot or cold)?  |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.1.1, 4.3.3, 4.5.2 |
| NIST 800-34 | 3.1, 3.2, 3.5 |
| 9. | A copy of the Business Impact Analysis (BIA) or the processing priorities to be followed? If using a processing priorities list does this agree with the Business Continuity BIA? Are customer service levels clearly defined for all phases of BC (response to restoration)?*Note: See documentation D3 from above.* |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.1 |
| NIST 800-34 | 3.2 |
| 10. | Has the team identified and developed a method to track all IT costs associated with the outage. Are the cost tracking procedures clearly defined and include the tracking of: temporary personnel, alternate site costs, travel expenses, personal expenses, overtime, replacement equipment, construction costs, etc… |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.4.1 |
| NIST 800-34 | 2.1, 3.5 |
| 11. | The files, data, programs, documentation and supplies to be taken to the backup site and how they are to be transported (or inventory of what is at the backup site). Are there provisions for reserve supplies (forms, pencils, paper, tapes, etc…that may be needed during and after recovery at the backup site?*Note: See documentation D4 from above.* |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.4.1, 4.5.1 |
| NIST 800-34 | 2.1, 3.5 |
| 12. | The location of off-site storage tapes (disks, etc.) and procedures for who is authorized to access them and how to access them. Are there provisions for transporting this data to disaster recovery site if not one in the same? |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.4.1 |
| NIST 800-34 | 3.4, 3.5 |
| 13. | Is there a list of equipment and configuration options? Is there a hardware configuration diagram? (If hot site is being used should also have a configuration diagram hardware already installed).*Note: See documentation D4 from above.* |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3, 4.6.1 |
| NIST 800-34 | 3.5, 5.1, 5.2, 5.3, 5.4 |
| 14. | Is there a list of inventory of all software (applications, utilities, and systems) to be recovered, recovery priorities and key business decision contacts? This can be a part of an overall BIA.*Note: See documentation D3 and D4 from above.* |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3, 4.6.1 |
| NIST 800-34 | 3.5, 5.1, 5.2, 5.3, 5.4 |
| 15. | A method to replace the existing equipment on short notice?  |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.4.1, 4.4.5 |
| NIST 800-34 | 2.1 |
| 16. | A network configuration diagram? Or location of where the most current is stored along with backup information and how to find it? |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.4.1, 4.4.5 |
| NIST 800-34 | 3.5, 5.1, 5.2, 5.3, 5.4 |
| 17. | Have the alternative manual procedures to satisfy mission requirements during system down time been considered and documented? |  |  |  |  |  | OK IT  | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.4.1, 4.4.5 |
| NIST 800-34 | 3.5, 5.1, 5.2, 5.3, 5.4 |
| 18. | Are there procedures to restore network and connect to alternate business office or service office sites? |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.4.1, 4.4.5 |
| NIST 800-34 | 3.5, 5.1, 5.2, 5.3, 5.4 |
| 19. | Are there procedures to restore, install new hardware at the disaster recovery site, existing site, or alternate site? |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.4.1, 4.4.5 |
| NIST 800-34 | 3.5, 5.1, 5.2, 5.3, 5.4 |
| 20. | Are there documented procedures to restore the data and software backups? (For each system and application to include utility data). Data requirements (reload sequences, dependencies, backup locations, etc…) |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.4.1, 4.4.5 |
| NIST 800-34 | 3.5, 5.1, 5.2, 5.3, 5.4 |
| 21. | Does the plan include a formalized schedule for restoring critical systems? |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.4.1, 4.4.5 |
| NIST 800-34 | 3.5, 5.1, 5.2, 5.3, 5.4 |
| 22. | Are there documented procedures for validation of data recovery points and recovery of lost data? |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.5.1, 4.6.1 |
| NIST 800-34 | 3.5, 5.1, 5.2, 5.3, 5.4 |
| **C. PREVENTION** |
| 1. | Have data redundancy techniques been implemented reducing the reliance upon tape backup procedure, storage and recovery? |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3 |
| NIST 800-34 | 5.1, 5.2, 5.3, 5.4 |
| 2. | Is there the ability for a sister site server or a secondary/additional local server to assume processing for the main server if it goes down? Is there automated process to update the main processor with local transactions when recovery is complete? |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3 |
| NIST 800-34 | 5.1, 5.2, 5.3, 5.4 |
| 3. | Is there access to local databases or scaled down data bases for local processing in the event the main database server is down? |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3 |
| NIST 800-34 | 5.1, 5.2, 5.3, 5.4 |
| 4. | Are there provisions for synchronizing databases? |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3 |
| NIST 800-34 | 5.1, 5.2, 5.3, 5.4 |
| 5. | Do all critical systems and components have backup power supplies? |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3 |
| NIST 800-34 | 5.1, 5.2, 5.3, 5.4 |
| 6. | Do critical systems have duplicate:1. Disk drives?
2. Processors?
3. Controllers?
 |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3 |
| NIST 800-34 | 5.1, 5.2, 5.3, 5.4 |
| 7. | Are important files mirrored (on a separate disk) within the same server to protect against disk failure? Are mirrored disks connected to a separate controller? Is disk mirroring reviewed frequently to ensure all important files are mirrored? When the primary file fails, can the mirrored file be moved into production quickly and without losing data? Are move procedures practices and tested frequently? Are backups taken from the primary or the mirrored disk? |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3 |
| NIST 800-34 | 5.1, 5.2, 5.3, 5.4 |
| 8. | Are “hot” servers used for systems that cannot tolerate an outage (High Availability)? Is the “hot” server remote? Are databases/files on “hot” servers synchronized? If the primary server goes down, can the “hot” server take over immediately? Are the takeover of the “hot” server practices and practiced and tested frequently? Are backups taken from the primary or “hot” server? |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3 |
| NIST 800-34 | 5.1, 5.2, 5.3, 5.4 |
| 9. | Can the phone company switch inbound call to the IT recovery sites quickly? Has this process been tested? (Specifically important for IT Help Desk functionality).  |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3, 4.5.2 |
| NIST 800-34 | 3.5, 5.1, 5.2, 5.3, 5.4 |
| 10. | Is the computer facility in a low access area/building? |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3 |
| NIST 800-34 | 5.1, 5.2, 5.3, 5.4 |
| 11. | Are computer facilities protected by appropriate physical security controls and are these monitored for appropriate access on a regular basis? |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3, 4.4.7 |
| NIST 800-34 | 5.1, 5.2, 5.3, 5.4 |
| 12. | Is the area surrounding the computer equipment and data storage devices free from obstacles and hazards? |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3, 4.4.7 |
| NIST 800-34 | 5.1, 5.2, 5.3, 5.4 |
| 13. | Are there multiple grids for electricity and central exchanges in use? |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3, 4.4.7 |
| NIST 800-34 | 2.1, 5.1, 5.2, 5.3, 5.4 |
| 14. | Are there multiple transformers for larger data processing areas? |  |  |  |  |  | OK IT  | 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3, 4.4.7 |
| NIST 800-34 | 2.1, 5.1, 5.2, 5.3, 5.4 |
| 15. | Are there backup generators? Are backup generators automatically activated through a UPS in case of a power outage? |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3 |
| NIST 800-34 | 2.1, 5.1, 5.2, 5.3, 5.4 |
| 16. | Have alternate paths been built into data and telecommunications networks?  |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3, 4.4.7 |
| NIST 800-34 | 2.1, 5.1, 5.2, 5.3, 5.4 |
| 17. | Have data de-duplication efforts been initiated to reduce the amount of data to be stored and recovered.  |  |  |  |  |  | OK IT  | 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3, 4.4.7 |
| NIST 800-34 | 2.1, 5.1, 5.2, 5.3, 5.4 |
| 18. | Do all automated system software and service contracts clearly define:1. Responsibilities of all parties involved in the event of a disaster (e.g. client, software vendor, hardware vendor, hosting vendor, etc...)?
2. Problem reporting, response, and resolution time frames?
3. On-site support in a reasonable time frame if needed?
4. Billing amounts and process for support during a major outage? Are the billing amounts reasonable?
5. Confidentiality statements and safeguards during an outage and usage of alternate processing sites?
6. Usage of software on alternate hardware during all phases of recovery?
 |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3, 4.4.1, 4.4.5, 4.4.7 |
| NIST 800-34 | 3.1, 3.2, 5.1, 5.2, 5.3, 5.4 |
| 19. | Has a business interruption insurance policy been purchased and does the policy clearly define:1. Responsibilities of insurer and the insured?
2. Contain words “due diligence” and the agreed upon definition?
3. The deductible? Is it reasonable? Does it apply to a lump sum actual total or is it separated into categories?
4. Maximum payoff limits? Are these adequate to cover complete restoration of the business?
5. Clear reporting requirements and time frames?
 |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3, 4.4.1, 4.4.5, 4.4.7 |
| NIST 800-34 | 3.1, 5.1, 5.2, 5.3, 5.4 |
| 20. | Have the following IT General Controls audits been performed to identify weaknesses that may impact the ability to recover crucial infrastructure, processes and data: 1. Backups (data & systems/applications)?
2. Off-site storage?
3. DC review of backup site?
4. DC review of all primary sites?
5. Service provider contracts (software, hosting, cloud, etc...)?
6. Review of service provider third party audit results?
7. Others…?
 |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.1, 4.3.3, 4.4.1 4.4.5, 4.4.7  |
| NIST 800-34 | 3.1, 3.2, 5.1, 5.2, 5.3, 5.4 |
| 21. | Do the appropriate user representatives have an active role in creating and reviewing control reliability and backup provisions relevant to their applications? |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.4.2, 4.4.7, 4.5.1 |
| NIST 800-34 | 3.5, 4.2 |
| **D. DISASTER RECOVERY SITE (BACKUP SITE)** |
| 1. | Can the backup site process required volume? Does the backup site capabilities support all hardware and telecommunications requirements (mainframes, server types, voice and data lines, switches, etc..) required to support business or services offices (current or alternate locations)? |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.5.1, 4.5.2 |
| NIST 800-34 | 2.1, 3.5 |
| 2. | Can backup site provide sufficient processing time for as long as necessary?  |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.5.1, 4.5.2 |
| NIST 800-34 | 2.1, 3.5 |
| 3. | Is backup site geographically located a sufficient distance away from existing location as to meet human safety, BC, and legal requirements? |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.5.1, 4.5.2 |
| NIST 800-34 | 2.1, 3.5 |
| 4. | If the backup site is vendor-owned and operated, does the contract include: 1. The basis of costs and additional charges for special requests?
2. Confidentiality statements?
3. Maintenance of adequate insurance in the event of data losses through error and/or omissions?
4. Price changes?
5. Cost and method of cancelling the contract, including adequate time allowance?
6. Processing priorities between clients?
7. Notification of all changes that would affect contract (i.e. hardware eliminated or added)?
8. Adequate protection and established limit of liability for BOTH the servicer and the client?
9. Bonding of personnel?
10. Testing times and costs?
 |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.5.1, 4.5.2, 4.6.1  |
| NIST 800-34 | 2.1, 3.5, 5.1 |
| **E. TESTING** *Note: See documentation D7 from above.* |
| 1. | Is the plan tested on a regular basis (industry best practice still focuses on annual testing)? |  |  |  |  |  | OK IT | 8.1, 8.2 |  |
| ANSI | 4.5.1, 4.5.2 |
| NIST 800-34 | 3.5, 4.2 |
| 2. | Has an exercise schedule with realistic time scales been developed and approved by senior management? Does it include:1. Testing objectives?
2. Testing scopes?
3. Testing frequency?
4. Testing scenarios relevant to the environment/business and in line with threat/risk analysis (i.e. created that approximate the types of incidents the organization is likely to experience and the problems associated with these incidents)?
5. Exercise evaluation criteria?
6. Collection, storage and reporting of key exercise documentation and results?
 |  |  |  |  |  | OK IT | 8.1, 8.2 |  |
| ANSI | 4.5.1, 4.5.2, 4.6.1 |
| NIST 800-34 | 2.1, 3.5, 3.6 |
| 3. | Are all key applications and systems included in the testing? |  |  |  |  |  | OK IT | 8.1, 8.2 |  |
| ANSI | 4.5.1, 4.5.2 |
| NIST 800-34 | 3.5 |
| 4. | Are all key business function areas included in testing? |  |  |  |  |  | OK IT | 8.1, 8.2 |  |
| ANSI | 4.3.1, 4.5.1, 4.5.2 |
| NIST 800-34 | 3.5 |
| 5. | Are all portions of the plan tested (manual and automated)? |  |  |  |  |  | OK IT | 8.1, 8.2 |  |
| ANSI | 4.3.1, 4.5.1, 4.5.2  |
| NIST 800-34 | 3.5, 4.2 |
| 6. | Are test results documented and maintained for historical reference? |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.1, 4.5.1, 4.5.2 |
| NIST 800-34 | 3.5 |
| 7. | Are all test discrepancies followed through to proper correction? |  |  |  |  |  | OK IT | 8.1, 8.2 |  |
| ANSI | 4.3.1, 4.5.1, 4.5.2 |
| NIST 800-34 | 3.5 |
| 8. | Are all components of the network, operating systems, utilities, and logical security included in the testing? |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.1, 4.5.1, 4.5.2 |
| NIST 800-34 | 3.5 |
| 9. | Has the plan/backup site been tested under a full application/system load? |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2 |  |
| ANSI | 4.3.1, 4.5.1, 4.5.2 |
| NIST 800-34 | 3.5 |
| 10. | Have all network segments been tested? |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.1, 4.5.1, 4.5.2 |
| NIST 800-34 | 3.5 |
| 11. | Have voice (phone switch procedures) been included in the testing? |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.1, 4.5.1, 4.5.2 |
| NIST 800-34 | 3.5 |
| 12. | Are training sessions conducted for all relevant personnel on backup, recovery, and contingency operating procedures? |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.1, 4.4.2, 4.5.1, 4.5.2 |
| NIST 800-34 | 3.5 |
| 13. | Do appropriate user representatives participate in the testing? |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.1, 4.5.1, 4.5.2 |
| NIST 800-34 | 3.5 |
| 14. | Have testing success indicators been established? Do they include:1. Total time for execution of recovery tasks?
2. Balance to control totals?
3. Testing of remote office connectivity?
4. User and automated functionality testing of restored software (i.e. test scripts, automated load testing tools, etc...)?
5. Other..?
 |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.1, 4.5.1, 4.5.2 |
| NIST 800-34 | 3.5 |
| 15. | Is there a formal process to certify the success of testing by management and independent observer? |  |  |  |  |  | OK IT | 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.1, 4.5.1, 4.5.2 |
| NIST 800-34 | 3.5 |
| **F. BUSINESS CONTINUITY INTEGRATION** |
| 1. | Have specific IT emergency evacuation procedures been posted in data center / processing sites? (i.e. hitting the power off button as you leave the building/room; is there a specific timeframe in which you have to evacuate between alarm sounding and the release of fire suppression gases?) |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3, 4.4.5, 4.6.1 |
| NIST 800-34 | 3.4, 4.2 |
| 2. | Has an IT response /triage team been identified? Does the overall Business Continuity Emergency Management team understand and respect the IT triage team’s responsibilities. Do they know and understand when to engage this team in IT triage duties? |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3, 4.4.5, 4.6.1 |
| NIST 800-34 | 3.4, 4.2 |
| 3. | Is the IT personnel included in overall BC personnel call tree or contact tree? Does the process exist/contain current up-to-date contact information? Are there alternates identified for all key personnel?*Note: See documentation D6 from above.* |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3, 4.4.1, 4.4.3, 4.4.5 |
| NIST 800-34 | 3.4, 4.2, 5.1 |
| 4. | Are IT vendors included in the overall BC vendor call tree or contact process and does it contain current up-to-date contact information? Is there alternate contact numbers and/or after hours contact information? *Note: See documentation D5 from above.* |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3, 4.4.1, 4.4.3, 4.4.5 |
| NIST 800-34 | 3.4, 4.2, 5.1 |
| 5. | Are there clearly documented time frames for escalation from a processing interruption to an IT disaster situation? Is there a definition for IT disaster? |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3, 4.4.1, 4.4.3, 4.4.5, 4.5.1 |
| NIST 800-34 | 3.4, 4.2, 5.1 |
| 6. | Does the IT response/triage team understand human safety and emergency response processes are to be the first priority? |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3, 4.4.1, 4.4.3, 4.4.5, 4.5.2 |
| NIST 800-34 | 2.1, 3.4, 4.2, 5.1 |
| 7. | Do IT emergency personnel understand where to meet and how to communicate with Business Continuity and IT DR decisions making authorities (i.e. command center)? Is the location of the alternate processing site(s), location of backups, known by key decision making personnel and IT response/triage team?  |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3, 4.4.1, 4.4.3, 4.4.5, 4.5.2 |
| NIST 800-34 | 2.1, 3.4, 3.5, 4.2, 5.1 |
| 8. | Has it been clearly documented and established who and how information systems and data will be protected during all phases of disaster recovery? Specifically, during the early crisis management phases (Response, Resumption & Recovery)? |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3, 4.4.1, 4.4.3, 4.4.5, 4.4.7 |
| NIST 800-34 | 2.1, 3.4, 3.5, 4.2, 5.1 |
| 9. | Are there different emergency response plans for internal disasters vs. external (community) or national disasters? Are the steps for protecting the IT resources addressed in all of these different scenarios? |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3, 4.4.1, 4.4.3 4.4.5, 4.4.7 |
| NIST 800-34 | 2.1, 3.4, 3.5, 4.2, 5.1 |
| 10. | Have manual processing procedures been documented for key business and service areas that may have to run without or with limited IT support? Do these processes address collection of data in format that allows for entry into automated systems once they are recovered? |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.1, 4.4.1, 4.4.5, 4.4.7 |
| NIST 800-34 | 2.1, 3.4, 3.5, 4.2, 5.1 |
| 11. | Are there clear lines of communications between BC decisions makers and IT recovery personnel and business recovery personnel? Are the communication channels the same to ensure that the same message is being delivered to both areas? Is there a predetermined method for documenting and communicating IT recovery efforts back to decision makers and to business/service recovery personnel? (Communications flow diagrams for each phase of BC does this include IT)?  |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.3, 4.4.1, 4.4.5, 4.6.1 |
| NIST 800-34 | 2.1, 3.4, 3.5, 4.2, 5.1, 5.2, 5.3, 5.4 |
| 12. | Is there a clear assignment of duties for reconstructions and off-site/recovery phase processing?  |  |  |  |  |  | OK IT | 8.0, 8.1, 8.2, 8.3 |  |
| ANSI | 4.3.1, 4.4.1, 4.4.5 |
| NIST 800-34 | 2.1, 3.4, 3.5, 4.2, 5.1 |

**Definitions**

**Business Continuity** **Planning** (BCP) is the activity performed by an organization to ensure that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions. These activities include many daily chores such as project management, system backups, change control, and help desk. Business continuity is not something implemented at the time of a disaster; Business Continuity refers to those activities performed daily to maintain service, consistency, and recoverability.

A **Business Impact Analysis** (BIA) predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies. Potential loss scenarios should be identified during a [risk assessment](http://www.ready.gov/risk-assessment). Operations may also be interrupted by the failure of a supplier of goods or services or delayed deliveries. Impact analysis should determine/identify how the loss or damage will manifest itself, the process for potential escalation of damage or loss with time following an incident, minimum services and resources needed to continue operating at a minimum acceptable business level, and the timeframe within which activities, functions and services of the organization should be recovered.

A **Contingency Plan** provides the documented organizational plan to mitigate risks of business interruption and minimize the impact of any disruption of service. It must maintain instructions for achieving a full or minimally acceptable set of business objectives in the absence of assets, through cost-effective strategies to provide replacements for assets as they become unavailable. The Plan must involve advance planning and preparations to respond to external circumstances as determined by a risk assessment and continue to provide a pre-determined acceptable level of business functionality. The Plan should contain the roles, responsibilities and procedures for restoring a system or facility following a major disruption.

**Disaster Recovery** (DR)is the process consisting of policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a [natural](http://en.wikipedia.org/wiki/Natural_disaster) or [human-induced](http://en.wikipedia.org/wiki/Man-made_hazards) [disaster](http://en.wikipedia.org/wiki/Disaster). Disaster recovery is a subset of [**business continuity**](http://en.wikipedia.org/wiki/Business_continuity). While [business continuity](http://en.wikipedia.org/wiki/Business_continuity) involves planning for keeping all aspects of a business functioning in the midst of disruptive events, disaster recovery, among other functions, focuses on the IT or technology systems that support business functions.

**Recovery Time Objectives** is the duration of time and a service level within which a [business process](http://en.wikipedia.org/wiki/Business_process) must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in [**business continuity**](http://en.wikipedia.org/wiki/Business_continuity). It can include the time for trying to fix the problem without a recovery, the recovery itself, testing, and the communication to the users.

**Recovery Point Objective** is the maximum tolerable period in which [data](http://en.wikipedia.org/wiki/Data) might be lost from an IT service due to a major incident.

**Bibliography**

American National Standards Institute. “Organizational Resiliency: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use,” ASIS SPC.1 – 2009.

<http://webstore.ansi.org/RecordDetail.aspx?sku=ASIS+SPC.1-2009>

National Institute of Standards and Technology

* “Contingency Planning Guide for Federal Information Systems,” Special Publication 800-34 Rev.1, May 2010.
	+ <http://www.nist.gov/manuscript-publication-search.cfm?pub_id=905266>
* “Guide to Computer Security Log Management,” Special Publication 800-92, September 2006
	+ <http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf>

Office of State Finance. “State of Oklahoma Information Security Policies, Procedures, Guidelines V 1.5,” Revised March 1, 2011.
<http://www.ok.gov/OSF/documents/StateOfOklahomaInfoSecPPG_osf_12012008.pdf>

|  |  |
| --- | --- |
| **Subject:** Business Continuity & Disaster Recovery Checklist | **Version:** 2.0 |
| **Created:** 8/24/2012 | **Revised/Reviewed:** 11/6/13 |
| **Author:** Yevgen Pashchenko | **Author: Rachel Lacatus (**Cindy Hall) |