Business Continuity

Guidelines – general

CDO specific DR – by app and priority

Replication and Failover

Remote HA/DR

Local HA/DR

Planned maintenance

Unplanned maintenance

HA vs scalability

Scalability = flexibility and elasticity

Dependent on the number of users

“Gold/Silver/Bronze”

RTO/RPO

Application Dependencies and App-Specific Recovery Steps

SaaS

Backup targets (Azure BLOB, AWS S3, etc.)

Retention periods (compliance)

Scenarios

Recovery from User Error

Recovery from Data Corruption

SQL Server/RDBMS/Data Lake

VM vs. Physical

Smoking Crater

Inter-DataCenter connectivity/resiliency/portability

Data vs. Config (OS/App)

Incident Response

When to declare a disaster

Disaster Declaration document

Test schedule

Cost model

Business Impact Analysis and Prioritization

Definitions

Guidance for DR Readiness

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Section** | **Question** | **Guidance** | | |
| **General** | **Acceptable Answers** | **Comments** |
| General Information | Provide the name of the document that contains your disaster declaration process. | A disaster declaration is the formal identification of an event of such severity as to warrant the implementation of business continuity and DR Plans. A disaster declaration provides authorization to execute third party contingency contracts where applicable.  In order for an event to be declared a disaster, a disaster declaration must be made by authorized leadership through a recovery event management process. A recovery event management process is used when extraordinary efforts outside of standard incident management processes are required.   A disaster declaration document should include a recovery event management process and the steps that would be taken to assess and declare a disaster. The following should be included: - The process by which communication methods (e.g. bridge calls) are initiated - The name of the team that manages the communications/discussions (e.g. command center, IT operations group, Help Desk) - A list of leaders that would join discussions to determine if the incident should be a recovery event (this may or may not include all individuals with authority to declare a disaster) - The authorized individuals who can declare a disaster | If a disaster declaration process does not exist, one must be documented in order to complete the DR plan by the due date. | If a disaster declaration process is not documented, the plan requirement cannot be completed and a policy exception is required. |
| General Information | Are procedures documented for managing a disaster event from declaration to fully functional? (Y/N) | Documenting procedures to manage a disaster event from beginning to end will ensure all impacted resources are aware of their roles and responsibilities throughout the event and will assist in the quick and efficient recovery of applications. | Answer **Y** if procedures to manage a disaster event from beginning to end are documented.  If the answer is **N**, think about incorporating these procedures into the recovery management process. |  |
| General Information | Are communication procedures to notify Senior Leadership, employees, customers, suppliers, media and other stakeholders established and documented? (Y/N) | Documenting communication procedures will ensure pertinent stakeholders are notified of the disaster declaration and kept informed of the status of application recovery. | Answer **Y** if communication procedures are documented.   If the answer is **N**, think about incorporating these procedures into the disaster management process. | All media communications should go through Corporate Communications. This should be included in the communication procedures. |
| General Information | List the full address(es) of all datacenters. | Distinguish between Production datacenter(s) and Recovery datacenter(s). | Provide the full address(es) of the production and recovery datacenters, including suite numbers, if applicable. Location code is helpful, if available.  Enter TBD for next to Recovery if a recovery location is not identified.  If any applications have DR Active (Active/Active solutions across datacenters), list the datacenter address as both Production and Recovery.  If the data center is owned/managed by a third party, include the name of the vendor. |  |
| General Information | Will access to contact information for key support contacts be available in the event of a disaster in the production datacenter(s)? (Y/N) | If contact information is stored only in the production datacenter it may not be available after a disaster. Having contact information accessible in the event of a disaster will assist in the quick and efficient recovery of applications. | Answer **Y** if access to contact information will be available in the event of a disaster.  If the answer is **N**, think about incorporating this into the disaster management process. |  |
| General Information | Are controls in place to ensure access to DR Plans is limited to a need to know basis? (Y/N) | DR documentation is confidential and access should be granted only to those who need to know the details of the documentation. | Answer **Y** if access controls are in place.  If the answer is **N**, think about implementing access controls. | Having controls in place are not required to complete the DR plan requirement but not having controls may become an audit issue. |
| General Information | Are DR Plans stored in a secured repository for internal only access? (Y/N) | DR documentation is confidential and should be stored in secure locations. | Answer **Y** if DR documentation is stored in a secured repository.  If the answer is **N**, think about placing documentation in a secured repository. | Having DR documentation in a secured repository is not required to complete the DR plan requirement but not having DR documentation in a secured repository may become an audit issue. |
| General Information | Is the DR plan repository located in a geographically separated location from the production datacenter(s)? (Y/N) | If the DR plan repository is located in the production datacenter, it may not be available during a disaster event. | Answer **Y** if DR documentation is stored in a geographically separated location from the production datacenter.  If the answer is **N**, think about placing documentation in a geographically separated location from the production datacenter. |  |
| General Information | Is a process or program in place to train employees and contractors on disaster recovery responsibilities in the event of a disaster? (Y/N) | Knowing the roles and responsibilities during a DR event will assist in the quick and efficient recovery of applications. | Answer **Y** if a training process or program is in place.  If the answer is **N**, think about implementing a process. |  |
| General Information | Applications /core infrastructure may be functionally exercised this year. (ALL / Some / None) | **Option 1**: Demonstrate the ability to recover and validate all components (servers/devices) of the application using its recovery infrastructure.  Requirements: • Follow documented procedures to recover and validate all components (servers/devices) of the application in a geographically separated location from production. Note: If the application has multiple components (servers/devices) that provide the same functionality, at least one component must be included in the exercise. • Recover data and validate data consistency between production and what was recovered. • Validate basic application functionality. • Log and report issues encountered during the exercise. Track issues through remediation (during and post exercise). Closure is not required to get exercise credit.  **Option 2**: For applications spanned across two or more datacenters, demonstrate the application remains available when all components (servers/devices) in one datacenter are unavailable.  Requirements: • Provide evidence of the application remaining fully available in an alternate datacenter during a planned or unplanned outage. | Answer **ALL** if the expectation is to meet functional exercise requirements for all applications / infrastructure during the calendar year.  Answer **Some** if the expectation is to meet functional exercise requirements for some applications / infrastructure during the calendar year.  Answer **None** if there is no expectation to functionally exercise any applications / infrastructure during the calendar year. | If an application does not meet the functional exercise requirements, they must be reviewed in a Tabletop exercise.   The Enterprise DR Coordinator will provide additional details regarding DR exercises during the DR readiness documentation discussions. |
| Application Details DR Solution | List all application components, solutions and RTO/RPO. | Servers supporting the application may have different solutions, RTOs and RPOs. Use the DR Solutions definitions document under the comments field. | List components (server or functionality types). **Example** Web servers = DR Active; 8 hr RTO; 0 hr RPO App Servers; DB Server = DR Media Recovery; 72 hr RTO; 48 hr RPO App Server = DR Cold Recovery; 1344 hr RTO; 48 hr RPO DB Server = DR Standby; 8 hr RTO; 1 hr RPO | [DR Solutions Definitions for Self-Managed Applications](#'DR_Solutions_Definitions'!A1) |
| Application Details DR Solution | What is the current application disaster recovery solution? | The overall DR solution for the application is comprised of all solutions of the application components identified in the prior field. | List all solutions identified in the prior field. **Example** DR Active; Media Recovery; Cold Recovery; DR Standby |  |
| Application Details RTO/RPO | What is the current application RTO? | Recovery Time Objective (RTO) is the maximum length of time an application can be unavailable before the business is impacted. | Enter a number value of the RTO in hours. | If the servers supporting the application have different RTOs, list the longest RTO. Using the example above, the RTO = 1344 |
| Application Details RTO/RPO | What is the current application RPO? | Recovery Point Objective (RPO) is the maximum acceptable amount of data an application can lose, measured in time, before the business is impacted. | Enter a number value of the RPO in hours. | If the servers supporting the application have different RPOs, list the longest RPO. Using the example above, the RPO = 1 |
| Application Details Production Hardware | List address(s) of where the application production hardware resides. |  | Provide the full address of each datacenter, including suite numbers, if applicable. Location code is helpful, if available.   If the data center is owned/managed by a third party, include the name of the vendor. |  |
| Application Details Production Hardware | Is there a documented inventory of the application's current production hardware? (Y/N) | Not having an inventory of the current production hardware will hinder the ability to recover applications quickly and efficiently. | Answer **Y** if all inventory supporting the application is documented.  If the answer is **N**, the inventory must be documented in order to complete the DR plan requirement by the due date. | If the inventory is not documented, the DR plan requirement cannot be completed and a policy exception is required. |
| Application Details Production Hardware | Is the inventory documentation maintained in a geographically separate location from the production datacenter? (Y/N) | If your inventory is located in the production datacenter it may not be available after a disaster. | Answer **Y** if the inventory list is available outside of the production datacenter.  If the answer is **N**, the inventory list must be placed in a location outside of the production datacenter in order to complete the DR plan requirement by the due date. | If the inventory is not located outside of the production datacenter, the DR plan requirement cannot be completed and a policy exception is required. |
| Application Details Production Hardware | Is the documented inventory updated when changes are made to the production environment?  (Y/N) | Outdated or missing information inventory will hinder the ability to recover applications quickly and efficiently. | Answer **Y** if the inventory is updated whenever changes are made to the production environment.  If the answer is **N**, think about incorporating this into the change control process. |  |
| Application Details Recovery Hardware | List address(s) of the location where the application will be recovered. |  | Answer **TBD** if a recovery location is not identified. |  |
| Application Details Recovery Hardware | Is there a documented inventory of the application's current recovery hardware? (Y/N/NA) | If there is identified hardware in a recovery location, having an inventory will assist in the quick and efficient recovery of applications. | Answer **NA** if a recovery location is not identified.  Answer **Y** if all recovery inventory supporting the application is identified and documented.  Answer **N** if the inventory is not documented. | If there is identified recovery hardware, documentation should include mapping each production server to the corresponding recovery server where that functionality will be recovered. |
| Application Details Critical External Contacts | Are critical external contacts for the application documented? (Y/N/None) | Identifying critical contacts will assist in the quick and efficient recovery of applications.  Critical External Contacts include application and IT external entities, vendors, clients or 3rd parties that send or receive data. | Answer **None** if there are no critical external contacts.  Answer **Y** if critical external contacts are documented.  Answer **N** if critical external contacts are not documented. | All Critical External Contacts required in the event of a disaster should be documented, regardless of the VRO (Vendor Relationship Owner). |
| Application Details Critical Required Skills | Is the list of roles/skillsets that would be required to recover the application documented? (Y/N) | In the event of a disaster, current technical resources may be unavailable. In order to properly augment staff, the skillset required should be documented. | Answer **Y** if the roles/skills are documented.  If the answer is N, think about documenting the critical skills required to recover and validate the application. | Documentation should include description of skill set required, role, level/years of experience and number of resources needed. |
| Application Details Recovery and Validation | If one or more application components require backups to restore data, are those backups stored in a geographically separate location from the production datacenter? (Y/N/NA) | If the application requires restoring from backups located in the production datacenter, the application cannot be restored during a disaster event. | Answer **NA** If none of the application components require backups to restore data..  Answer **Y** if one or more application components require backups to restore data AND the backups are stored in a geographically separate location from the production datacenter.  Answer **N** if one or more application components require backups to restore data AND the backups are NOT stored in a geographically separate location from the production datacenter. | Backups must be stored in a different geographic location from the production datacenter in order to complete the DR plan requirement by the due date. If they cannot be stored in a different geographic location from the production datacenter a policy exception is required. |
| Application Details Recovery and Validation | If the application depends on other applications OR other critical applications depend on this application, are those dependencies documented? (Y/N/No Dependencies) | Dependency information will assist in establishing priorities for application restoration by: - identifying applications that each application (in the Application Details tab) relies on to be fully functional (Predecessor). - identifying applications that rely on the applications (in the Application Details tab) before they can be fully functional (Successor).  Only applications that have a direct connection to the applications listed in the Application Details tab of this document need to be included. | Answer **No Dependencies** if this application does not require any other applications to be available to support business processes OR if no other critical applications are dependent on this application.   Answer **Y** if critical predecessor or successor applications (including data feeds) are documented.  If the answer is **N**, the critical predecessor or successor applications (including data feeds) must be documented in order to complete the DR plan requirement by the due date. | If there are critical dependencies but are not documented, the DR plan requirement cannot be completed and a policy exception is required. |
| Application Details Recovery and Validation | [Are application recovery procedures documented? (Y/N/None Required)](#'Application_Details'!Q5) | Procedures to complete recovery of an application will vary depending on the DR solutions of the components (servers/devices) that support the application. The steps required to recover/validate the infrastructure of the servers should be documented.  After the servers are recovered, if additional application specific steps (i.e. steps for starting services or configuration changes) may be required and should be documented.  Reach out to the Enterprise DR Coordinator with questions or additional guidance. | Answer **None required** only if the DR solution for all application components (servers/devices) are DR Active.  Answer **Y** if recovery procedures are documented.  If the answer is **N**, recovery procedures must be documented in order to complete the DR plan requirement by the due date. | If application recovery steps are required but are not documented, the DR plan requirement cannot be completed and a policy exception is required. |
| Application Details Recovery and Validation | Are procedures documented to validate the application works as expected? (Y/N) | Detailed validation steps will ensure application functionality has been recovered properly. | Answer **Y** if detailed validation steps are documented.  If the answer is **N**, validation steps must be documented in order to complete the DR plan requirement by the due date. | If the validation steps are not documented, the DR plan requirement cannot be completed and a policy exception is required. |

Test Schedule

|  |  |  |  |
| --- | --- | --- | --- |
| **ASK ID** | **Application/Infrastructure Name** | **Planned / Actual Test Date**  (If exact date is unknown, provide target month. Only enter December if that is the accurate month.) | **Planned / Actual Test Type**  (Functional or Tabletop) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Disaster Declaration Document

1. An incident is reported to, or detected by the service desk or other operational team. The impacted services manager or other affected manager pages out to a technical bridge as part of the normal war room process.
2. The IT operational team or manager assesses the situation to determine if the issue cannot be resolved within a short time frame.
3. The IT Senior Leadership team will use our standard P1 process to implement a conference bridge.
4. The IT Senior Leadership team performs a situational assessment and impact to operations. Engage other leadership resources as appropriate to assess impact. Reprioritize resources as appropriate.
5. If a recovery Event is declared, continue – otherwise continue to utilize standard incident management procedures. Re-assess if impact changes.
6. Evaluate the Event to determine if a disaster declaration is warranted. Those with authority to declare a disaster include <names>. If a disaster is declared, the DR plan(s) will be invoked, and will be facilitated by the service manager with support of the senior IT leadership team. The service manager or an appropriate IT manager will provide status throughout recovery activities to IT Senior Leadership team.

**Recovery Event Management Team**

|  |  |  |
| --- | --- | --- |
| **Primary** | **1st Alternate** | **2nd Alternate** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Definitions:**

IT Senior Leadership Team – <names> are currently the primary members of this team.

Service Manager – manager responsible to the business for service delivery, currently <name>

Services Manager – line manager responsible for a specific service such as desktop, network or an application

Disaster – an issue such that there is no defined path or schedule to recovery

Definitions

|  |  |  |
| --- | --- | --- |
| **Solution** | **RTO / RPO** | **Definition** |
| **DR Active** | RTO ≤ 8 hours RPO ~ 0 | - Production infrastructure components are located in at least two geographically separate datacenters. - All infrastructure components are in production status. - Each datacenter contains enough infrastructure to fully support the production load requirements of the application. - In the event of the loss of a single datacenter, the application continues to function with no intervention required. |
| **DR Standby** | RTO ≤ 8 hours RPO ≤ 1 hour | - Production infrastructure components are located in two (or more) geographically separate datacenters: At least one active site and one standby site. - All Infrastructure components are in production support status. - Each datacenter contains enough infrastructure to fully support the production load requirements of the application. - Production infrastructure in at least one datacenter (Active site) is actively servicing transactions/users of the application.  - Production infrastructure in Standby site(s) contains an exact copy of the production application. - In the case of a database, a replication tool (such as Oracle Data Guard) is used to replicate data from the active site to the Standby site(s). - In the event of the loss of the Active site datacenter, manual intervention is required before the application is returned to service. |
| **DR Site Specific** | RTO ≤ 8 hours RPO ~ 0 | - Production infrastructure components are located in at least two geographically separate datacenters. - All infrastructure components are in production status. - In the event of the loss of a single datacenter, the application continues to function in an alternate datacenter with no intervention required. The application must be validated to ensure full functionality is available. - If this application is a platform, DR applications running on the platform must design, build and deploy a DR Solution in an alternate datacenter and develop a DR Plan. - Under normal operation, there is no replication or other dependency between datacenter instances of the application. |
| **DR Storage Replication-Other** | RTO and RPO must be provided by the self-managed infrastructure team. | - Production and recovery Infrastructure components are located in two geographically separate datacenters. - Each datacenter contains enough Infrastructure to fully support the Production load requirements of the application. - Data available on server. Storage is available but not connected. - Data is replicated between systems or storage arrays in the alternate datacenter. - In the event of the loss of the production site datacenter, manual intervention is required to return to service. |
| **DR Media Recovery** | RTO and RPO must be provided by the self-managed infrastructure team. | - Production and recovery infrastructure components are located in two geographically separate datacenters - Each datacenter contains enough Infrastructure to fully support the Production load requirements of the application. - Production system image and data are backed up via backup restoration technology and stored at a secondary location. - In the event of the loss of the Production site datacenter, manual intervention is required to restore the system via backup restoration technology onto the recovery components before the application is returned to service. |
| **Solution** | **RTO / RPO** | **Definition** |
| **DR External Recovery** | RTO and RPO must be provided by the self-managed infrastructure team and must include lead time required per vendor contract. | - Contracted recovery at a service provider such as IBM or SunGard - Contract specifies equivalent infrastructure sized to fully support the Production load requirements of the application  - In the event of the loss of the Production site datacenter, manual intervention is required before the application is returned to service. |
| **DR Cold Recovery** | RTO and RPO must be provided by the self-managed infrastructure team. | - Production Infrastructure is located in one datacenter. - Production system image and data are stored on backup media and stored at a secondary location. - Alternate datacenter space with racks, network and backup restoration technology will be used for recovery. No recovery systems exist. - In the event of the loss of the Production datacenter, extended manual intervention is required to restore. System components are procured and installed. Systems are restored via backup restoration technology onto the procured components before the application is returned to service. *Integration Note: Optum Technology does not build new applications with this solution.* |
| **DR Best Effort Recovery** | RTO = 99999 RPO = 99999  99999 is a code to signify best effort. It does not represent actual hours. | - Production Infrastructure is located in one datacenter - Production system image and data are stored on backup media and stored at a secondary location - A recovery location has not been identified or other challenges may prolong the recovery. - In the event of the loss of the Production site datacenter, extended manual intervention is required to restore. System components are procured and installed. Systems are restored via backup media onto the procured components before the application is returned to service *Integration Note: Optum Technology does not build new applications with this solution.* |
| **DR No Recovery** | RTO = 555555 RPO = 555555  555555 is a code to signify No Recovery. It does not represent actual hours. | - A Disaster Recovery Solution has not been configured for the devices. |