NCDIT for NC Department of Transportation

Disaster Recovery Assessment (DRA) Process

**Standard Operating Procedure**

# Document Purpose:

This document specifies who what where when and why a disaster recovery assessment process exists. Roles and responsibilities are defined while using an order of precedence as typically experienced.

Instructions are given for use with the associated DRA process site which is found internally available to all IT on [this Share Point site](https://ncconnect.sharepoint.com/sites/NCDITTransportationBusinessContinuity/DR_BCP/Forms/By%20Event%20Type.aspx?isAscending=true&id=%2Fsites%2FNCDITTransportationBusinessContinuity%2FDR%5FBCP%2FProcess%2FDR%20Assessment&viewid=12f2790b%2D0ff0%2D415a%2Dbf8a%2D975708200867). Business teams are granted access as required.

This document’s value is complemented by process diagram flow provided here:

[DR Assessment\DRA Process Flowchart.vsd](https://ncconnect.sharepoint.com/sites/NCDITTransportationBusinessContinuity/DR_BCP/Forms/By%20Event%20Type.aspx?isAscending=true&id=%2Fsites%2FNCDITTransportationBusinessContinuity%2FDR%5FBCP%2FProcess%2FDR%20Assessment&viewid=12f2790b%2D0ff0%2D415a%2Dbf8a%2D975708200867)

Contents

[Document Purpose: 1](#_Toc106187918)

[High Level process information by functional role 3](#_Toc106187919)

[Business 3](#_Toc106187920)

[Procurement 3](#_Toc106187921)

[Project Team 4](#_Toc106187922)

[Engage the Team & Start the DRA process 4](#_Toc106187923)

[Project Lead & DR PM 4](#_Toc106187924)

[Produce Business DRA 5](#_Toc106187925)

[Project Lead 5](#_Toc106187926)

[ISO Continuity 5](#_Toc106187927)

[Produce Offeror DRA 6](#_Toc106187928)

[The offeror DRA Content 6](#_Toc106187929)

[Provide the Offeror DRA 8](#_Toc106187930)

[DRA Instructions to vendors 8](#_Toc106187931)

# High Level process information by functional role

## Business

1. Objectives & Scope is provided, part of which are the Business objectives stated in Disaster Recovery (DR) terminology. Introduce specifically 3 Key Metrics: Criticality, Maximum Tolerable Downtime (MTD) & Recovery Point Objective (RPO).
2. Terminology & Definitions is an assessment of the audience to gauge what level of training & awareness is required. Specifics to be covered are the above indicated terms plus an overview of value resiliency plays for the business.
3. Guidelines & Main components – Business Continuity (BC) & DR process information is shared, order of precedence for what happens 1st, 2nd, next etc.
* High Level Requirements may be known and could be provided by the owning business team at this early stage. If such, the 3 specific metrics required; Criticality Level, Maximum Tolerable Downtime (MTD) & Recovery Point Objective (RPO), which can be hardened using the Application Resiliency Signoff (ARS) sub process. DocuSign provides for confirming the desired business requirements, alongside which IT is required to provide current recoverability capabilities.

When a business team does not know precisely what the given requirements are to be, the DRA engages to produce them, using a training and awareness conversational questioning and discussion-based process. The above-mentioned ARS is required to document the business requirements as a foundational element.

## Procurement

1. Leads with a formal kick off for the team, sharing program terms & conditions, roles responsibilities, and the overall procurement process, setting expectations.
2. ISO informs that DRA Instructions for Procurement Specialists are required, which need to be understood before proceeding.

## Project Team

1. Begins to gather and produce customer, and or technical data and project documentation.
2. ISO informs that DRA Instructions for PMO specialists are required, which need to be understood.
3. ISO shares high level illustration of business and offeror DRA versions each serving a unique purpose within the DRA process.

# Engage the Team & Start the DRA process

## Project Lead & DR PM

Note 1: the project leader and ISO collaboratively drive this swim-lane.

Note 2: Where we say application, this may mean an application suite, a service or a function to be procured.

1. The team is built with assigned resources to provide various input to the DRA process, based on given discipline.
	1. At the earliest team meetings, scope confirmation is needed, whether one business application, a service, function, or a combination of or a suite of applications, etc. We also inform, the business owner representatives are required to participate in the DRA process. To begin that process, we ask the business to provide their essential function/s which are to be served by the given application.
2. ISO requests time be allocated for the DRA process, to include overview, awareness, and training as may be required. Dependent upon the experience level of the audience, this may be 2, 3, 4 or more hours in effort by the team. Architecture may participate, however at a minimum a business analyst, business owner representative, such as a process owner or key functional unit manager, project technical coordinator (if exists) must participate, led by ISO to facilitate Disaster Recovery requirements gathering.
3. ISO recommends DRA reading, in preparation for the business requirements gathering process. The collective illustration presents background in statute, policy, who, what and why of the DRA process, along with procedure.
4. Gather & collate preliminary information to move forward with producing the business requirements as stated in DR terminology

# Produce Business DRA

## Project Lead

1. Establish DRA meetings, ensuring the right combination of players will be in attendance. This includes Architecture may participate, however at a minimum a business analyst, business owner representative, such as a process owner or key functional unit manager or managers and the project lead must participate, led by ISO to facilitate Disaster Recovery requirements gathering.

1.1 Remind the business unit they’ll want to consider starting work on essential function testing, producing test cases if needed, create scripting, produce a business validation plan which will be required in the DRE. Assign end users, provide a planning contact for a DRE which is required to be executed post award & prior to production go live.

1. Ensure all have access to, found and reviewed the documentation provided as recommended reading on the internal DRA site.
2. Hand off lead to ISO Continuity.

## ISO Continuity

1. Lead team in producing the Business DRA.

4.1 The business unit performs some day-to-day function(s) using the given application. It’s this or these “essential function/s (EF)” which must be established.

* Each EF will have some level of criticality, meaning when impacted is the impact statewide, or something lesser, such as agency wide or perhaps a program within the agency, or it may not be critical at all. Of the 4 criticality levels, this begins the conversation.
* When a given EF is impacted what amount of time is an acceptable downtime? Each EF will have a Maximum Tolerable Downtime (MTD).
* In a series of questions staged across 3 categories; risk, function and data, EFs will result in providing the key metric areas needed to formulate Criticality, Maximum Tolerable Downtime (MTD) & Recovery Point Objective (RPO).
* This enables moving forward to ISO Continuity completing the business DRA and producing the Vendor version DRA outfitting procurement with an appropriate addendum to the outgoing package for offerors to consume.
* At this juncture, the business has set the expectation as per the essential function performed by the business in ongoing day to day operations. Results of these 3 criteria are the Agency Approved Desired Business Requirements. These are applied into an Application Resiliency Signoff (ARS) form.
* IT will be asked if 2 of the above criteria (MTD & RPO) can be currently met. Whether IT can or cannot meet the expectation is purely incidental. IT’s capability does not change the business’ stated objective.
* An offeror/ vendor may become the supporting IT entity, in which at the appropriate time an Offeror may be asked if they as IT support can meet such. In this case the offeror who becomes the accountable IT party would then need to accommodate the respective fields in the ARS.

#  Produce Offeror DRA

## The offeror DRA Content

* The DRA contains Offeror instructions, these are known as the Security Requirements Traceability Matrix (SRTM) Guidance. The SRTM serves to capture the state of the organizations’ security control implementation specifically for Contingency Planning (CP) of the application/ system or service in this solicitation, utilizing the excel based questionnaire.

This spreadsheet contains tabs which each includes criteria from an individual NIST control family. The structure of each control family tab is identical. Please fill out columns marked in yellow/pink (depending on monitor settings) H, J, K, L & M. As selections are made, beginning with column H, highlighting logic will change the color of corresponding cells. Completed cells will appear green, cells requiring no action will appear gray and

cells highlighted in red will represent missing required information. These sheets are locked preventing editing of structure or content with the exception of cells that need an input. On the Guidance tab you can see an example of how the spreadsheet should be filled out as well as an explanation of what each column addresses.

Throughout this assessment, all questions focus on your proposal, therefore responses must address a given proposed solution, as is intended in a live production environment supporting the given procurement.

*e.g.*

*CP2.1 asks "Are the organization's: DR plans detailed & specific in the IT recovery solution clearly articulating ’how’ to meet or exceeding provided business objectives for the following 4 distinct recovery elements; recovery time objective, recovery point objective, maximum tolerable downtime, and restoration priorities?"*

*In this example, your organizations DR plans are those which would support the submitted proposal.*

* If your solution is to be cloud based or on customer premise, where a question may appear not to apply, provide a justification statement in the appropriate field.
* Additionally, on the Requirements tab with your proposal submission, Offeror provides a concise statement relating if their solution is cloud hosted, on state owned premise, or another.

If you have any questions regarding how to complete this spreadsheet, please reach out to your point of contact.

* The Business Requirements tab contain offeror instruction and Business Requirements supporting the given essential function/s, stated in DR terminology as MTD and RPO, must be met or exceeded in your submission.
* These Business Requirements are stated in DR terminology as MTD and RPO, support the provided essential function(s), must be met or be exceeded by a solution being submitted. MTD & RPO definitions are found on the Key Metrics tab of the DRA excel form if needed.
* In the DRA, Disaster Recovery metrics **MTD & RPO** are provided on the 1st tab labeled “Specifications”. Offerors provide a concise statement relating if their proposed solution meets the MTD & RPO, to be placed in the Offeror statement box in the Specifications tab. NCDOT & or NCDIT may require offerors complete the remaining tabs contained in the DRA, subsequent to the proposal submission. See Guidance tab for further detail, for complete instructions.
* Offerors must complete the DRA as is, in its native Microsoft Excel format, and be returned in this same native format as an attachment with a bid submission.
* Guidance tab is a detailed level of instruction how to complete the questionnaire, including examples.
* Contingency Planning tabs are identified by policy criteria such as CP2, CP3, CP4, etc.
* Key Metrics Reference tab contains definitions.

# Provide the Offeror DRA

## DRA Instructions to vendors

* The Specifications tab contain the business essential function/s which has been assigned three (3) resiliency metrics, stated in DR terminology as Criticality level, Maximum Tolerable Downtime (MTD) and Recovery Point Objective (RPO).
* Requirements supporting the given essential function are owned by the divisional team named.
* Given Application/ System / Service is named.
* MTD & RPO must be met or exceeded by the solution and noted in your submission.
* Detailed Offeror instructions are found on the DRA Guidance tab row 2 as labeled; **Security Requirements Traceability Matrix (SRTM**) Guidance.
* Offeror statement field:

To comply, Offeror will address the 2 key metrics ***MTD*** *&* ***RPO*** as specified for given application/ system/ service within a procurement, whether their solution meets the obligation. These DR requirements MTD & RPO are found in the DRA on the requirements tab.

* Offeror provides a concise statement relating if their solution meets or exceeds the MTD & RPO.
* Offeror provides a concise statement relating if their solution is cloud hosted, on state owned premise, or another.
* NCDOT & or NCDIT may require offerors complete the DRA after the proposal submission.

