**Risk Assessment Action 3 Worksheet: Critical Load Vulnerability**

Worksheet Last Updated By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Worksheet Last Updated On: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Identifying Critical Load Vulnerability

The Technical Resilience Navigator (TRN) Risk Assessment model allows vulnerability to be calculated in two manners: by answering a series of questions about the critical load or by choosing a vulnerability probability category. In general, the vulnerability questions will provide more granular insight, though a broader categorization is provided for those who desire it. For those working offline, for the purpose of the TRN Risk Assessment Excel model (**Tab 4**) you must choose one or the other (though you can change between the two options if desired).

Users should attempt to answer the vulnerability questions for all critical loads to receive richer insight in the Risk Assessment. Review the questions below and fill out the table with the applicable “No” or “Yes” response. Note that you must be able to answer “Yes” to all of the questions within the Reliability category for the critical load to mark “Yes”; otherwise, write “No.” For those working offline, if any redundant system supporting the critical load was listed as being vulnerable to a dual-impact hazard or threat in the worksheet from Action 2, leave “Design” blank, since this question needs to be answered on a hazard and threat-specific basis in **Tab 4** of the Risk Assessment Excel file**.** For those working online, the “Design” question will be automatically included or not included in the vulnerability assessment question as relevant.Otherwise, if there are no dual-impact hazards or threats to which the redundant systems serving the asset are vulnerable, then write “Yes” for Design. The information in the tables below helps users answer vulnerability questions in either the online tool or **Tab 4** of the TRN Risk Assessment Excel model.

For any critical loads that could not be characterized using the vulnerability questions, use professional judgement to assign a vulnerability category to the load. This gives a rough estimate of the probability of failure based on the expertise of relevant personnel.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **First Redundant System—Vulnerability Questions** | | | | | |
| **Critical Load** | **Redundancy** | **Design** | **Reliability** | **Start-Up Configuration** | |
| Is there a redundant system to the primary supply system? | Are all components of the redundant system designed to withstand the realized hazard or threat? (Hazard-specific) **AND**  Is the design for the realized hazard or threat documented? (Hazard-specific) | Is the equipment in the redundant system part of a preventative maintenance program? **AND**  Are written schedules and procedures in place and followed for the preventative maintenance and testing of the equipment? **AND**  Is there documentation of performance of preventative maintenance and testing, and documentation of observations associated with these activities? **AND**  Is there an onsite parts supply sufficient for realized hazard or threat conditions? | Is the redundant system configured to automatically start upon disruption of the primary service?  **OR**  If manual start-up of the redundant system is required, is it supported by written, up-to-date procedures relevant to the realized hazard or threat conditions, and are these procedures trained upon with documentation of completion of the training? | Is the redundant system configured to automatically start upon disruption of the primary supply system? |
| IT plug loads in Data Center X | Yes | No | Yes | Yes | No |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Second Redundant System—Vulnerability Questions** | | | | | |
| **Critical Load** | **Redundancy** | **Design** | **Reliability** | **Start-Up configuration** | |
| Is there a redundant system to the primary supply system? | Are all components of the redundant system designed to withstand the realized hazard or threat? (Hazard-specific) **AND**  Is the design for the realized hazard or threat documented? (Hazard-specific | Is the equipment in the redundant system part of a preventative maintenance program? **AND**  Are written schedules and procedures in place and followed for the preventative maintenance and testing of the equipment? **AND**  Is there documentation of performance of preventative maintenance and testing and documentation of observations associated with these activities? **AND**  Is there an onsite parts supply sufficient for realized hazard or threat conditions? | Is the redundant system configured to automatically start upon disruption of the primary service? **OR**  If manual start-up of the redundant system or service is required, is it supported by written, up-to-date procedures relevant to the realized hazard or threat  conditions, and are these procedures trained upon with documentation of completion of the training? | Is the redundant system configured to automatically start upon disruption of the primary supply system? |
| IT plug loads in Data Center X | Yes | No | Yes | Yes | No |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

For critical loads that will be using the vulnerability probability category, review the below reference chart and fill out the following table with the applicable category.

|  |  |
| --- | --- |
| **Vulnerability Probability Category** | **Category Description** |
| Very high vulnerability (100%) | Loss of the primary supply system resource would certainly or almost certainly result in outage of the critical load beyond its tolerable outage duration (TOD) (Probability > 95%) |
| High vulnerability (70%) | Loss of the primary supply system resource would likely result in outage of the critical load beyond its TOD (Probability = 40% - 95%) |
| Moderate vulnerability (25%) | Loss of the primary supply system resource would result in loss of the critical load beyond its TOD with moderate likelihood (Probability = 15% - 40%) |
| Low vulnerability (10%) | Loss of the primary supply system resource would not be likely to result in outage of the critical load beyond its TOD (Probability = 2% - 15%) |
| Very low vulnerability (1%) | Loss of the primary supply system resource would be very unlikely to result in outage of the critical load beyond its TOD (Probability < 2%) |

Based on the chart above, fill out the applicable vulnerability probability category for select critical loads.

|  |  |
| --- | --- |
| **Critical Load** | **Vulnerability Probability Category** |
| IT plug loads in Data Center X | Moderate |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Document your decision of whether you will be using the vulnerability questions or the probability category in the TRN risk screening tool in the table below.

|  |  |
| --- | --- |
| **Critical Load** | **Use vulnerability questions, or select vulnerability probability category?**  (Vulnerability Questions/Vulnerability Probability Category) |
| IT plug loads in Data Center X | Vulnerability Questions |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |