# RISK ASSESSMENT METHODOLOGIES

Risk assessment involves the evaluation of risks taking into consideration the potential direct and indirect **consequences** of an incident, known **vulnerabilities** to various potential threats or hazards, and general or specific **threat/hazard** information.

This resource document introduces various methodologies that can be utilized by communities to perform an infrastructure-focused assessment of risk as outlined in Step 3 of the IRPF. If your community has already completed a risk assessment as part of another planning process, such as FEMA hazard mitigation planning, the results of that assessment can be combined with and enhanced by conducting a critical infrastructure-specific risk assessment.

Whichever risk assessment methodology a community decides to utilize, the method should be documented, reproducible, and defensible to ensure transparency and practicality for stakeholders and decision-makers.

## Threat and Hazard Analysis Methods

### *Hazard Exposure Analysis*

Exposure analysis identifies the existing and future critical infrastructure systems and assets located in areas that susceptible to hazards. This approach often uses mapping tools such as Geographic Information systems (GIS) for analysis and visualization. Exposure analysis can quantify the number, type, and value of critical community infrastructure located within identified hazards areas, and show which systems and assets are exposed to multiple hazards. A number of tools are available to support hazard exposure, including:

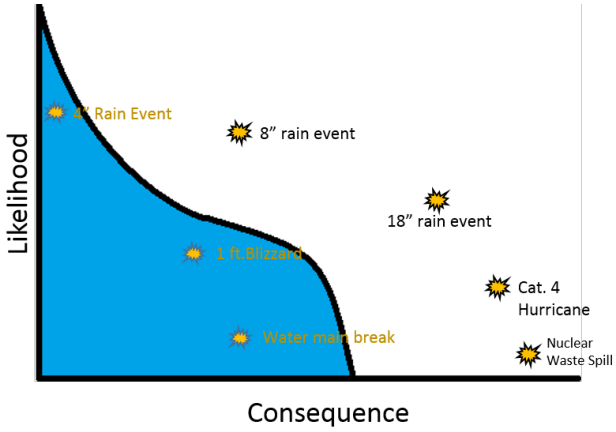
- **Seismic Hazards:** USGS Hazard Maps and Site-specific Data, http://earthquake.usgs.gov/hazards/hazmaps/
- **Sea Level Rise and Coastal Flooding:** Sea Level Rise and Coastal Flooding Impacts Viewer and Data Development, NOAA https://coast.noaa.gov/digitalcoast/tools/slr.html
- **Floods:** FEMA Flood Mapping Products, https://www.fema.gov/flood-mapping-products
- **Landslides:** Landslide Hazard Program, USGS http://landslides.usgs.gov

### *What-If Hazard Analysis*

What-if hazard analysis is a structured brainstorming method for developing threat and hazard scenarios and assessing their likelihood and consequences. This can be used to develop a strategy for managing risk from identified scenarios. More information about What-If Hazard Analysis can be found at:
http://web.mit.edu/course/10/10.27/www/1027CourseManual/1027CourseManual-AppVI.html

### *Threat and Hazard Scenario Analysis*

FEMA's *Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide Comprehensive Preparedness Guide (CPG) 201* provides guidance for conducting a THIRA, which includes a process for developing risk scenarios that can be used to execute a risk assessment. When developing scenarios, communities should select threats and hazards based on two factors: 1) the likelihood of a threat or hazard occurring and 2) the consequence of that event if it were to occur. A means of doing so is illustrated below.




***Scenarios should reflect high-consequence events that could affect your community***

As scenarios are being developed, planners should not consider just the threats and hazards a community usually faces and considers, but also those that are unusual, unlikely, or could potentially emerge coming years.

Ultimately, the planning team should identify scenarios that are plausible and represent a range of threat and hazards that could affect a community. Importantly, a good set of scenarios will cover three levels of likelihood:

- *Routine: Once every 5 years type of event.* At this level critical infrastructure systems should remain functional and not experience any significant damage or disruption[1]
- *Design: Once every 50 years type of event.* At this level, infrastructure systems should experience minimal damage or disruption as defined by designed performance levels.[2]
- *Extreme: Once every 200+ years type of event.* At this level, major damage or disruption can be expected but critical infrastructure should be able to operate at some minimal level.[3]

Once a set of risk scenarios have been developed, each scenario should be described and given context. This means specifying factors such as time, place, and conditions for the hazard. For the purposes of risk assessment, providing details about these aspects will help determine the implications of the hazard for critical infrastructure systems.

[1] NIST, 74
[2] Ibid, 74
[3] Ibid, 74

| Scenario | Context description |
|---|---|
| ***Category 4 Hurricane*** | A hurricane with sustained 135-mile per hour wind speeds and gusts up to 160 mph makes landfall four miles east of City Center, causing 15-ft of storm surge along coastal areas, and dropping 12 inches of precipitation over the majority of the region in a 24-hour period. |

Once developed, these scenarios can be used for other risk assessment applications such as vulnerability assessments and consequence analysis.

## Vulnerability Analysis Methods

### *Sector-Specific Plans Vulnerability Assessment Methodologies*

Many of the Sector-Specific Plans (SSPs) describe vulnerability assessment methodologies used in the specific critical infrastructure sectors. The SSPs also provide information about executing vulnerability assessments. The SSPs can be found at: https://www.cisa.gov/critical-infrastructure-sectors

### *Infrastructure Survey Tool (IST)*

The IST is a voluntary, Web-based vulnerability survey conducted by the Cybersecurity and Infrastructure Security Agency (CISA) to identify and document the overall security and resilience of a facility. The survey data, composed of weighted scores on a variety of factors for specific critical infrastructure, is graphically displayed in the IST Dashboard that compares the data against similar facilities and informs protective measures, resilience planning, and resource allocation. The IST is not currently available as a self-assessment tool. Critical infrastructure owners and operators should contact the local area CISA Protective Security Advisor (PSA) to schedule a visit to conduct an IST assessment. More information about the IST can be found at: https://www.dhs.gov/sites/default/files/publications/ecip-ist-fact-sheet-508.pdf

### *Integrated Rapid Visual Screen (IRVS)*

The IRVS was developed by the DHS Science and Technology Directorate to provide a facility-level risk assessment against a range of threats and hazards. The vulnerability assessment portion of IRVS includes analysis of the site, architecture, building envelope, structural components, mechanical systems and security to assess risk. Additional information about the IRVS and a downloadable version of the tool are available at: https://www.dhs.gov/bips-04-integrated-rapid-visual-screening-series-irvs-buildings

## Consequence Analysis Method

### *HAZUS-MH*

HAZUS is a nationally applicable standardized methodology that contains models for estimating potential losses from earthquakes, floods, and hurricanes. HAZUS uses GIS technology to estimate physical, economic, and social impacts of disasters. It graphically illustrates the limits of identified high-risk locations due to earthquake, hurricane, and flood. Users can then visualize the spatial relationships between populations and other more permanently fixed geographic assets or resources for the specific hazard being modeled. Additional information about HAZUS can be found at: http://www.fema.gov/hazus

## Performance Evaluation Method for Identifying Risk

The NIST Community Resilience Planning Guide (CRPG) approach can be used to evaluate the operational capabilities of critical infrastructure systems and assets against established performance goals under various threat/hazard scenarios. The CRPG emphasizes understanding how long a community can continue to operate if various services and infrastructure systems are compromised. Depending on the disaster event, a community should have an expected timeline of operational capabilities based on short-term (hours), intermediate (weeks) and long-term (months) goals.

The figure below shows a sample operational capability recovery time frame. For each critical infrastructure asset or system, the planners should identify appropriate performance benchmarks following an event. Communities should determine how quickly each identified asset or system must be restored to ensure rapid response and recovery and avoid long-term economic or social damage to a community. Some assets or systems may be so critical, that any diminishment of capacity could cause long-term harm, while other assets only need to maintain a small portion of their operational capacity in the immediate aftermath of an incident.

| **Priority Infrastructure** | **Support Needed** | **Phase 1** Short Term (Hours) | | | **Phase 2** Intermediate (Weeks) | | | **Phase 3** Long Term (Months) | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 0 -24 | 24-48 | 48-72 | 1-4 | 4-8 | 8-12 | 3+ | 4-24 | 24+ |
| Infrastructure System/Asset 1 | R, S, MS C | 90% | | | | | | | | |
| Infrastructure System/Asset 2 | R | 30% | 90% | | | | | | | |
| Infrastructure System/Asset 3 | MS | | | 30% | 60% | | 90% | | | |
| Infrastructure System/Asset 4 | C | | 30% | | | 60% | | 90% | | |
| Infrastructure System/Asset 5 | | 60% | 90% | | | | | | | |

The following definitions for performance targets are adapted from the NIST CRPG. Planners can use these definitions for setting performance targets or create its own that are more tailored to their needs.

- 30% represents the operational capacity of the asset or portion of infrastructure system that need to be functional to initiate response and recovery activities
- 60% represents operational capacity of the asset or portion of infrastructure system needed for usual (i.e., daily) operations to resume at a reduced scale

- 90% represents the fraction needed to declare asset or infrastructure system at normal operating capacity.

In addition to performance targets, communities can determine what external support systems (such as mutual aid) are needed to meet planned benchmarks. They are typically:

- *(R) Regional: Neighboring communities, county government*
- *(S) State: State authorities*
- *(MS) Multi-State: Council of governments/governors, interstate support*
- *(C) Corporate/Community Organizations: e.g. Red Cross, major industries in community or region*

With established performance targets, planners can use the risk scenarios generated through the THIRA process (or any other scenario development method) to establish anticipated performance levels. For each scenario, planners should reassess performance goals and evaluate anticipated performance. This should include review and analysis of:

- **Information about past incidents,** which will demonstrate how similar threats and hazards have impacted critical infrastructure systems in the past and project how it would handle risk scenarios
- **Expertise resident in the planning participants—**especially from critical infrastructure owners and operators and those with knowledge of asset and system vulnerability to specific threats and hazards**—**will be particularly germane to determining anticipated performance
- **Past analyses** done in the community or by neighboring communities can provide estimates for anticipated performance.

Using the performance goal table, indicate the anticipated performance level for infrastructure assets and systems, as shown in the figure below. This work will help identify key gaps between performance goals and anticipated performance levels that represent risks to your community and should inform resilience planning. Those risks should be documented and used as a basis for the identification of resilience solutions.

**Anticipated Performance: Category 4 Hurricane**

| Priority Infrastructure | Support Needed | Phase 1 Short Term (Hours) | | | Phase 2 Intermediate (Weeks) | | | Phase 3 Long Term (Months) | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 0 -24 | 24-48 | 48-72 | 4-Jan | 4-8 | 8-12 | 3+ | 4-24 | 24+ |
| Priority Infrastructure 1 | R, S, MS C | 90%<br>30% | 60% | | 90% | | | | | |
| Priority Infrastructure 2 | R | 30% | 90%<br>30% | | 60% | 90% | | | | |
| Priority Infrastructure 3 | MS | | | 30%<br>30% | 60%<br>60% | | 90%<br>90% | | | |
| Priority Infrastructure 4 | C | | 30%<br>30% | | | 60%<br>60% | | 90%<br>90% | | |
| Priority Infrastructure 5 | | 60% | 90%<br>30% | | 60% | 90% | | | | |

In this table, anticipated performance levels are included. Areas where anticipated performance fails to meet the performance goal are marked in red; areas where the performance goals are met are marked in green.