IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

SUITE OF TOOLS FOR THE ANALYSIS OF RISK (STAR)

STAR is an innovative engine for forward-looking, functional risk assessment of critical infrastructure (CI) at the national scale. STAR facilitates data integration, model coupling, and decision-supporting visualization of high-priority CI.

WHY A FUNCTIONAL APPROACH TO RISK ANALYSIS?

- CISA and the National Risk Management Center's (NRMC) mission is to assess and reduce risk across all CI
- STAR's functional perspective breaks down silos by drawing out connections and analyzing related effects throughout the network of CI
- STAR provides a holistic view of risk on a national scale

> The functional perspective allows leadership to make risk-informed decisions that include cross-cutting or cross sector risks, emerging risks, and dependencies.

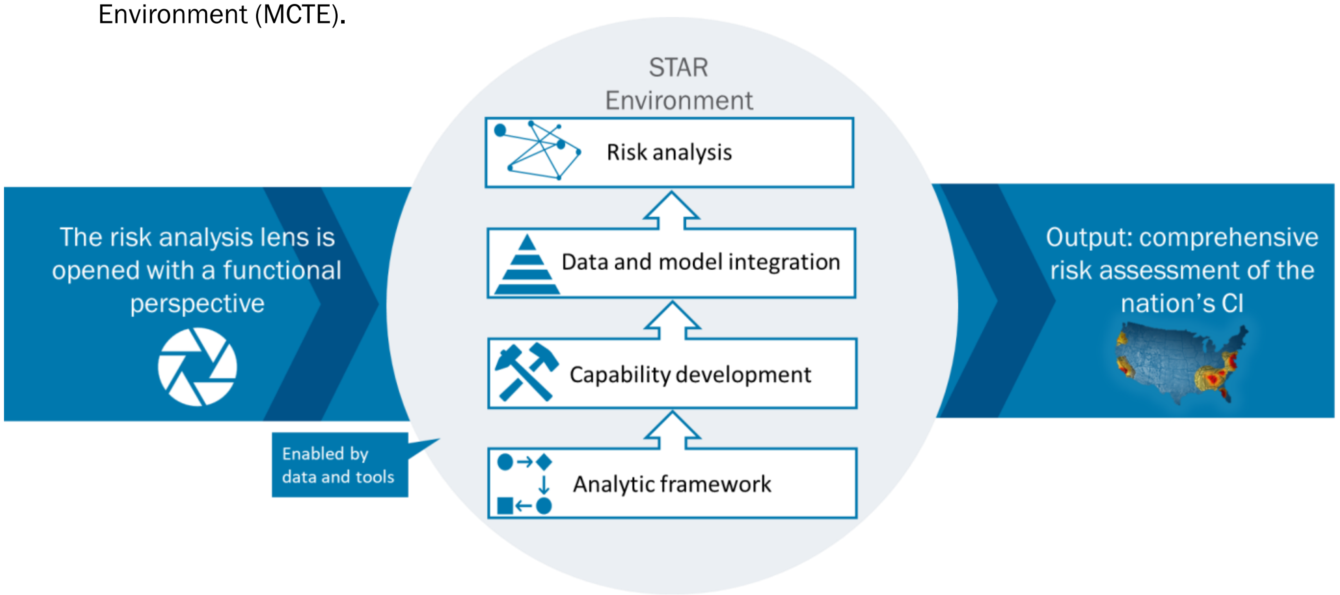
STAR connects functions to assets and answers the following questions:

What could break?
Assets

Who is responsible if it breaks?
Sectors/Entities

What would happen if the asset broke?
Functions

STAR is the engine of standard analytic tools and reproducible processes for CI risk assessment, ensuring that analysis is defensible, compatible, and enduring. STAR integrates the innovative National Critical Functions (NCF) dataset. This holistic functional view identifies connections between sectors by looking at all relationships within CI. STAR is hosted on CISA's Modeling Capability Transition Environment (MCTE).


The risk analysis lens is opened with a functional perspective
Enabled by data and tools
STAR Environment
Risk analysis
Data and model integration
Capability development
Analytic framework
Output: comprehensive risk assessment of the nation's CI

STAR 1

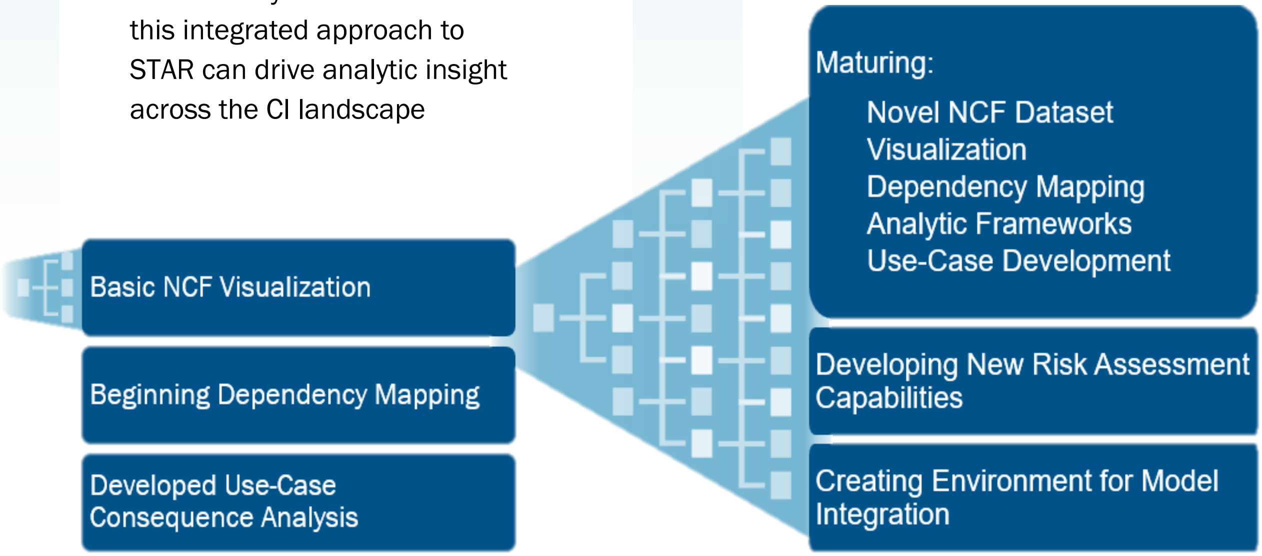
Laid the **foundation for advanced analytics** by developing core STAR capabilities:

- STAR v1 is the first visualization of cascading consequence and failure analysis of CI from functions to assets
- Successfully demonstrated that this integrated approach to STAR can drive analytic insight across the CI landscape

STAR 2

Builds on the foundational STAR v1 by **adding analytical and technical capabilities**:

- Will demonstrate component vulnerability analysis, continued data maturation, technical scalability through a test environment, and maturing analytic frameworks



Basic NCF Visualization

Beginning Dependency Mapping

Developed Use-Case Consequence Analysis

Maturing:

Novel NCF Dataset
Visualization
Dependency Mapping
Analytic Frameworks
Use-Case Development

Developing New Risk Assessment Capabilities

Creating Environment for Model Integration

As STAR matures, capability development through targeted analytic modeling efforts will provide NRMC, CISA, and the federal enterprise an engine for risk analysis that shifts from *reactive* to *prospective*. STAR's use-cases will focus on notional examples where STAR develops, analyzes, and communicates risk analysis related to systems surrounding cyber disruption scenarios to align with the NRMC's Risk Register development. Examples of scenario driven prompts and questions analysts can answer using STAR are below. These questions can be adapted to analyze any of the 55 NCFs.

STAR v1 Scenario

Given a cyber-attack resulting in the disruption on a major US Pipeline, you can answer the following questions:

1. How are materials transported by pipeline?
2. If pipelines are disabled, what **other functions** could be impacted?
3. What **needs to be functioning** so pipelines can function?
4. What compromised assets could **directly** cause pipelines to stop functioning?
5. What compromised assets could **indirectly** cause pipelines to stop functioning?
6. Where are the key assets **located**?

STAR v2 Scenario

Given a cyber-attack on the water system, you can answer all the questions from STAR V1, but also answer these new questions:

1. Which assets are **vulnerable**?
2. Given compromised assets, which **underlying subfunctions** are impacted?
3. How **many people** are affected by the disruption?
4. What are the **potential health** and **economic impacts**?
5. How does the attack **cascade across** specific sectors and subfunctions?