Intelligence Driven Exercises and Solutions (IDEAS)

An uncomplicated approach to solving complicated problems using Tabletop Exercises

Theresa Fersch

February 2021

MITRE | **SOLVING PROBLEMS FOR A SAFER WORLD**™

What is IDEAS?

- Intelligence Driven Exercises and Solutions (IDEAS) is a tabletop exercise (TTX) methodology developed at MITRE.

- Our solutions are thoughtfully designed discussion-based events during which participants explore dynamic problem sets or threats in a unique way to challenge assumptions, methods, and strategies and bolster understanding.

- Over the last ten years, a diverse team of subject matter experts (SME) have leveraged lessons learned and best practices from exercises conducted by DOD, DHS and the IC, to create a standardized yet customizable method for building tabletop exercises that can be applied to any industry or problem set.

IDEAS Background

- Methodology leverages MITRE's culture of speed, adaptability, and collaboration to create iterative experiences that address a changing environment

- Leverages MITRE's breadth of expertise to prioritize a cross-pollination of thoughts to identify new challenges and opportunities through the application of divergent and convergent thinking

- Designed to be lightweight, rapid, and flexible

- Built to augment and enhance value of existing and future program efforts (e.g., could precede simulations or full-scale exercises)

- Creates a path for knowledge transfer from subject matter experts (SMEs) through targeted discussion and actionable recommendations

Applying Exercises to Complex Challenges

Problem:

As threats, technology, and organizations change at ever increasing speed, MITRE's sponsors must adapt to this dynamic environment through continuous validation and refinement of their assumptions, methods, and strategies

This environment necessitates:

- speed to provide answers on a relevant timeline

- a methodology that leverages divergent and convergent thinking to pro-actively consider new and emerging challenges and opportunities

- a low cost and scalable approach that is adaptable to the current need.

Applying Exercises to the Problem:

IDEAS events target key individuals (leaders, decision makers, users, etc.) within an ecosystem. Participants are then provided the opportunity to explore complex problems, threats, and capabilities in a realistic, controlled environment - leading to increased understanding of their domain as well as enhancing effective decision making.

Why Exercises?

- Augment existing or future sponsor efforts.

- Allow players to focus on specific aspects of a challenge without having to manage unnecessary variables that are otherwise overwhelming in real life.

- Continually evolve to reflect real-world threats and adversaries.

- Promote the consideration of diverse perspectives stemming from varying subject matter expertise.

- Pull players out of their daily routine and minimize distractions; this fosters innovation.

- Promote creative thinking because there are no wrong answers, players are free to explore "wild" ideas.

- Provide a safe, no-fault, non-attribution, environment.

MITRE

Impact

Final outputs of an IDEAS event identify gaps, reveal lessons learned, and offer actionable recommendations which result in updated plans, policies, and strategies

- Cybersecurity/Healthcare – Enabled the participating healthcare institution (20+ sites) to safely realize the impact of a cyber extortion event involving all aspects of the organization. The institution implemented lessons learned for response and recovery that were utilized during a downtime incident only a few months later

- Foreign Military – Enabled the organization to explore notional command and control (C2) concepts and select a best-of-breed approach to modernize its C2 structure and evolve toward 5th generation dominance and real joint operations

- Emergency Management – Enabled the safe exercising of a major trans-national boundary toxic industrial chemical train derailment resulting in catastrophic damage and loss of life. Involved over a dozen state, US, and foreign organizations and resulted in the establishment of critical information sharing relationships between participating agencies

MITRE

Explore the Problem Set

IDEAS exercises allow sponsors to sharpen their focus on a specific problem or threat and understand its most essential components.

PEOPLE	**People** – Identify roles and responsibilities, define decision-making parameters, establish relationships.
PROCESS	**Process** – Establish process used to address identified gaps or technical challenges, improve/refine analysis techniques, develop CONOPS and plans.
TECH	**Technology** – Explore technology effectiveness, define requirements.

Exercise Methodology

The IDEAS team works closely with the sponsor and (SMEs) to scope the problem, define objectives, design the exercise, build products, execute the event, and analyze output.

Methodology in Three Steps:

Execution

Planning and Development

Analysis and Output
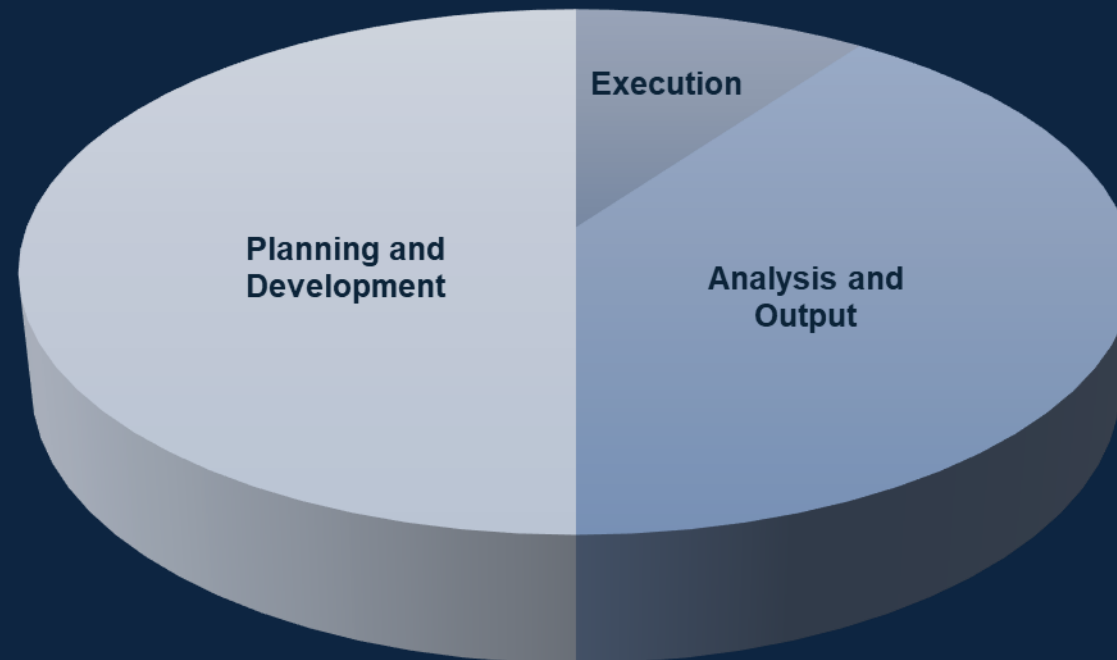
1. Exercise Planning and Development

- **Plan**
  - Scope problem and goals – identify specific threat/vulnerability to be explored (scaling a problem to a manageable level is one of the most difficult challenges IDEAS helps sponsors to address)
  - Define exercise objectives
  - Convene SMEs to develop threat space and adversarial actions (CONOPS)
- **Develop**
  - Develop realistic scenario(s) describing the problem – based on intelligence, facts, recent events, models, requirements, and SME analysis
  - Build injects, evaluation criteria, etc. – necessary details pertaining to the scenario that steer the exercise
  - Train facilitators and note takers
  - Conduct dry runs if necessary

MITRE

2. Exercise Play/Execution

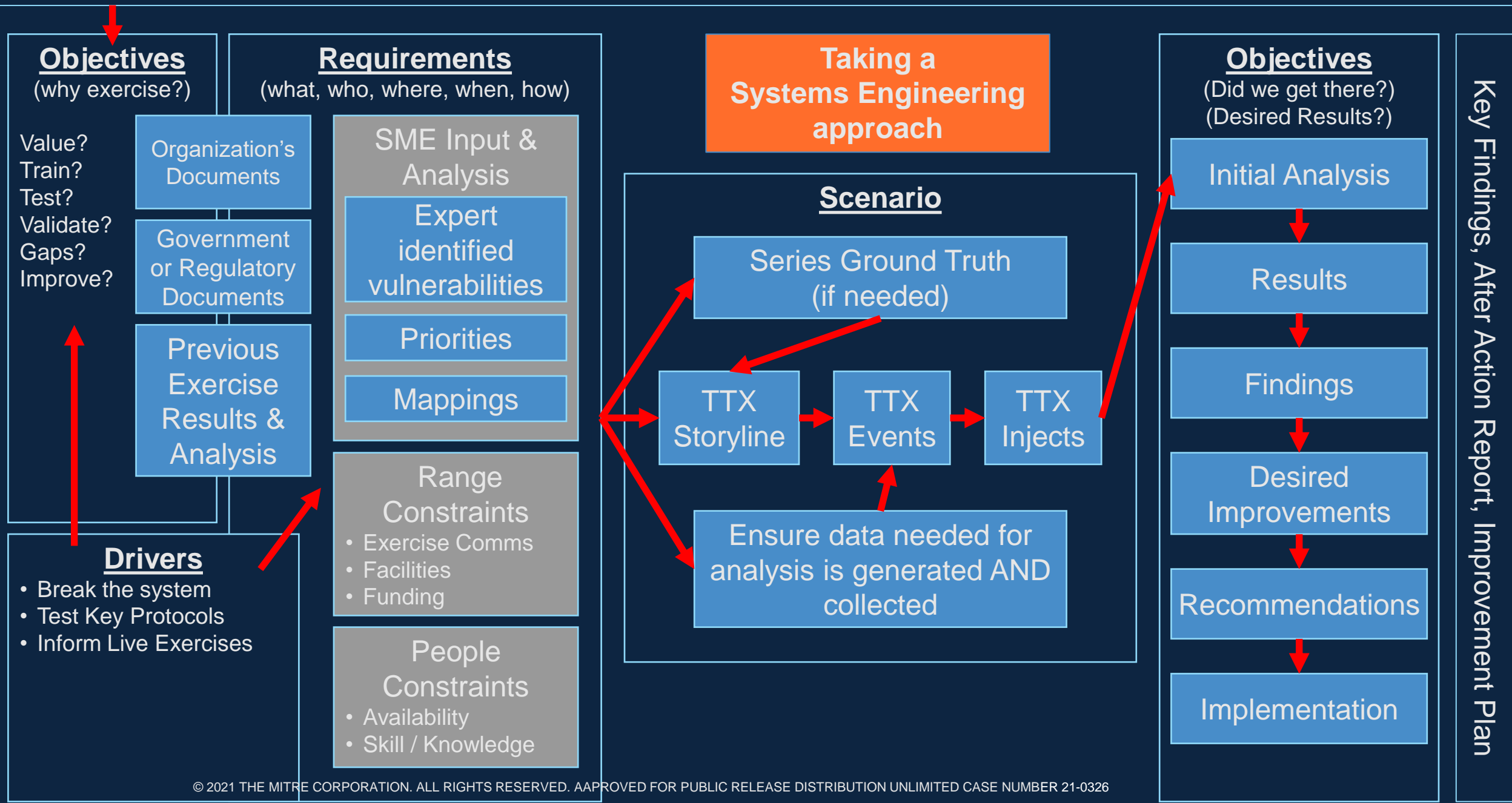- **White Team – controls the flow of the exercise**
  - Controllers/Facilitators – facilitate discussion, provide players with background, and answer questions
  - Analysts/Evaluators – collect/analyze data and track outcomes
- **Blue Team/Exercise Players – respond to injects, identify gaps, and refine TTPs iteratively during exercise**
- **IDEAS Team – provides any/all logistical/administrative/facilitation support**

3. Analysis and Output

- **Analyze Exercise Outputs (notes, surveys, etc.)**
  - Review lessons learned
  - Identify key gaps in information, analysis, processes, etc.
  - Recognize areas for improvement
  - Track unknown threats, domain vulnerabilities, and outcomes
  - Identify indicators and warnings (I&W)

- **Document Outcomes**
  - Document findings in an After-Action Report (AAR)
  - Update mission or operational plans and CONOPS
  - Document changes to requirements
  - Offer actionable recommendations

- **Communicate Results to Key Stakeholders**
  - Executive leadership
  - Operators/users
  - Decision Makers

Goal: Develop data to inform future exercises, identify areas for potential update and improve effectiveness of return to safe operations

Objectives
(why exercise?)

Value?
Train?
Test?
Validate?
Gaps?
Improve?

Organization's Documents

Government or Regulatory Documents

Previous Exercise Results & Analysis

Requirements
(what, who, where, when, how)

SME Input & Analysis

Expert identified vulnerabilities

Priorities

Mappings

Range Constraints
• Exercise Comms
• Facilities
• Funding

People Constraints
• Availability
• Skill / Knowledge

Drivers
• Break the system
• Test Key Protocols
• Inform Live Exercises

Taking a Systems Engineering approach

Scenario

Series Ground Truth (if needed)

TTX Storyline

TTX Events

TTX Injects

Ensure data needed for analysis is generated AND collected

Objectives
(Did we get there?)
(Desired Results?)

Initial Analysis

Results

Findings

Desired Improvements

Recommendations

Implementation

Key Findings, After Action Report, Improvement Plan

Examples of IDEAS Impact

Exercise results have helped sponsors achieve critical mission objectives:

- **DoD –** Led to establishment of an international Community of Interest among participants, which resulted in continued collaboration beyond the exercise itself

- **Intelligence Community –** Directly influenced federal policies on homeland security

- **Emergency Management –** Resulted in trusted partnership between participating federal agencies and national infrastructure organizations

- **Cybersecurity/Healthcare –** Enabled the participating healthcare institution to implement lessons learned from the exercise for improved response and recovery when it experienced a similar real-life incident months after the exercise.

- **Foreign DoD –** Resulted in the adoption of a formal Multi Domain Command and Control (MDC2) concept currently being used with sponsor's next-gen technology.

- **Transportation –** Resulted in changes to the sponsor's disaster recovery plan that will minimize downtime in the event of a system outage.

MITRE

MITRE

"I have heard so many positive comments from across the organization and many requests to conduct similar exercises in the future….We experienced a brief systemwide downtime and the role of the exercise in preparing teams for that event has been mentioned in every debriefing."

**Mass General Brigham
(formerly Partners Healthcare)**