Blank Tabletop Plan

(the formatting is intentionally basic – bring your own formatting!)

Date: <content>

Author: <content>

Scenario: <content>

Audience: <content>

1. Purpose

Hint: make this specific and relevant to your audience.

Formulas:

- Audience, Behaviour, Condition, Degree

- Who, What, When, Where, Why, How

- Use tools like MITRE ATT&CK Groups to determine realistic threat agents for your organization.

The Key to your purpose: a decision point. What is the one key decision you want the audience to make? E.g.:

- Pay/not pay a ransom.

- Switch to a different service provider.

- Fire Jim.

Examples:

- "Executives will walk through the business impacts of a successful ransomware attack that cannot be recovered from via backups during a two-hour boardroom session."

- "The IT team will be tested on their knowledge of the incident response plan using a competitive and fun trivia event."

- "The Online Store Support Team will be tested on their ability to discover, analyze, contain, eradicate, and recover from an advanced persistent threat injected into their payment gateway."

2. Objectives

Hint: These statements support your purpose and become your "inputs".
Formulas:
- Specific, Measurable, Action-Oriented, Realistic, Time Bound
- Audience, Behaviour, Condition, Degree

The Key to your objectives: define questions to answer, or create discussion.

Examples:
- "The IT team are presented with a packet capture that indicates industrial process control signals have been sent from an unexpected host, they have five minutes to analyze the information to determine if an attacker is present."
- "The Executives are presented with evidence that confidential client information is available on the dark web for a purported ransom of $10M, they have ten minutes to discuss their obligations and capabilities to respond."
- For a knowledge check question: "The incident handling process from NIST 800-61.R2 is:"

2.1. Objective 1

<content>

2.2. Objective 2

<content>

2.3. Objective 3

<content>

3. Requirements

Hint: determine what you and the participants need to be successful

Examples:

- Physical spaces

- Technology (computers, internet access, conference/collaboration tools)

- Pre-reading materials

- Test devices or machines

- Comfort (snacks, drinks)

- Safety (physical safety / muster locations, psychological safety)

3.1. Technology Requirements

- <content>

3.2. Physical Requirements

- <content>

3.3. Safety Requirements

- <content>

3.4. Pre-Reading Materials

- <content>

4. Session Plan

Hint: Copy/Paste as much as you can

First pass: build your content top-down. Consider Mitre Attack Navigator to help you with realism.
Second pass: build your timing bottom-up
Third pass: add or remove complexity, add collateral items such as packet captures, screen shots.
Give participants something to work with!

4.1. Ground Rules

TIME: 00:00

- **The facilitator and participants will insist on an inclusive, positive, and safe environment for attendees:**
  - Any individual feeling uncomfortable with any aspect of the event is encouraged to communicate concerns to the facilitator or an appropriate leader, either publicly, or privately with confidence;
  - Any individual concerned about a potential safety concern can call "Freeze!" to stop the scenario for investigation of a safety violation.
- **Safety:**
  - Muster zones in case of evacuation;
  - Ensure hydration and nutrition needs of self and others;
  - Incident response activities, both real and simulated, can induce significant stress on individuals. Be aware of your personal wellbeing and needs, monitor your peers' wellbeing and deviation from baseline behaviors.
- **Schedule:**
  - Ground Rules
  - Scenario Time
  - Review Time
- **Purpose:** <content>
- **Are there any questions?**

4.2. Scenario Time

4.2.1. Objective 1

- **TIME:**
- **SLIDE #:**

<Objective 1 content>

4.2.2. Objective 2

- **TIME:**
- **SLIDE #:**

<Objective 2 content>

4.2.3. Objective 3

- **TIME:**
- **SLIDE #:**

<Objective 3 content>

TIME: XX:XX

SCENARIO WIND DOWN:

Repeat that it's ok for feelings of exhaustion, frustration, elation, sadness at the end of a tabletop scenario for all sorts of reasons, offer encouragement that we're through the hard part and heading into a respectful discussion.

15-minute break:

- Grab a drink of water, stand up and stretch your legs if you need to
- Deep breathing, release tension from your shoulders and neck

4.3. Post Scenario Review

- Review <PURPOSE>
- Review <OBJECTIVES / INPUTS>

Probing Questions (hint: open ended questions are best!):

- How do you think that went?
- Tell me some positive things that surprised you?
- What gaps did we uncover that we believe requires improvement?
- Did we discover any missing documentation, processes, or resources?
- Did we learn about any previously unknown or unexpected resources or talents?
- Knowing what you know now, if you were transported back in time, what would you do differently?

SESSION CLOSE:

Final words, Facilitator:

- Remind participants that this type of scenario is designed to make them stretch and anticipate; and that there is incredible value practicing your abilities to react in the face of an incoming threat, but also in the process of developing and maintaining those same abilities.
- Encourage participants to keep communicating, keep learning, keep correlating. Ask questions, get their hands dirty, explore new things in their environment as often as they can."

Final words, HOST:

- Invite the host to share final thoughts, and close the meeting for all participants.