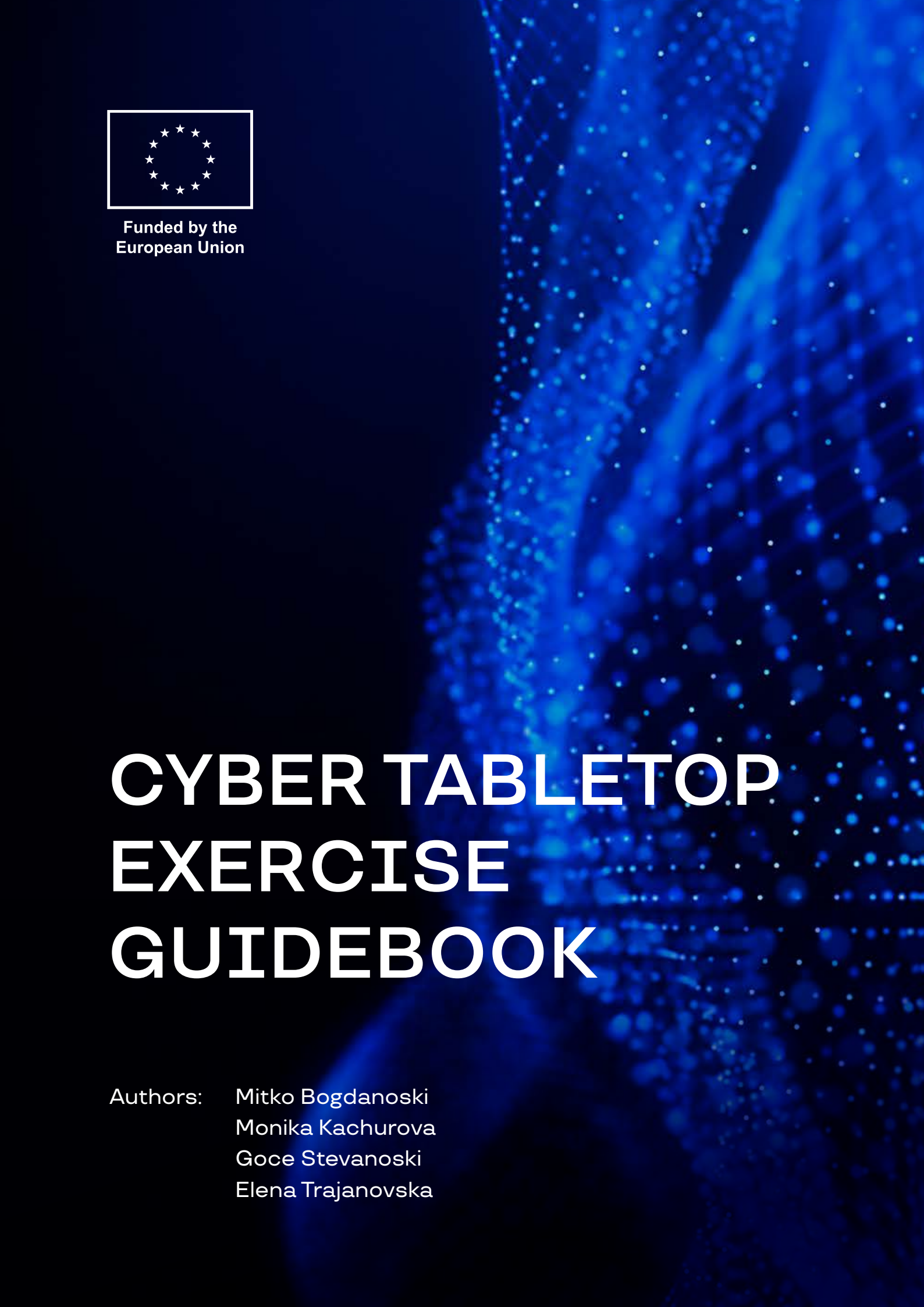


Funded by the
European Union

CYBER TABLETOP EXERCISE GUIDEBOOK

Authors: Mitko Bogdanoski
Monika Kachurova
Goce Stevanoski
Elena Trajanovska

Cyber Tabletop Exercise Guidebook

Funded by
the European Union

This guidebook was prepared under the **"Cyber Balkans"** project, funded by the European Union and implemented by the e-Governance Academy. The project enhances cyber resilience in the Western Balkans by strengthening prevention, preparedness, and response capacities in line with EU standards and best practices.

The content of this publication is the sole responsibility of the authors and does not necessarily reflect the views of the European Union.

Authors: Mitko Bogdanoski, Monika Kachurova, Goce Stevanoski, Elena Trajanovska
Design by OÜ Dada AD

Published by
e-Governance Academy
Ahtri 6, 10151, Tallinn, Estonia
ega.ee

The e-Governance Academy is an Estonian centre of excellence to increase the prosperity and openness of societies through digital transformation. In more than 20 years, we have cooperated with more than 300 organisations from 145 countries, supporting a more efficient use of information and communication technologies in governance and democratic processes. The core of our team consists of the architects and founders of the Estonian and Ukrainian digital state. Find out more information at ega.ee.

Contents

List of Abbreviations

Abbreviation	Full Form
AAR	After-Action Report
CFO	Chief Financial Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CTEP	CISA Tabletop Exercise Package
DDoS	Distributed Denial of Service
DPO	Data Protection Officer
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
HR	Human Resources
IRP	Incident Response Plan
IT	Information Technology
ISO/IEC 27001	International Organization for Standardization / International Electrotechnical Commission Standard 27001
MS Teams	Microsoft Teams
MSSP	Managed Security Service Provider
NIS2 Directive	EU Network and Information Security Directive 2
PDF	Portable Document Format
PR	Public Relations
SitMan	Situation Manual
SMART	Specific, Measurable, Achievable, Relevant, Time-bound
TTX	Tabletop Exercise
Zoom	Zoom Video Communications (platform)

1. Introduction

What Is a Cybersecurity Tabletop Exercise (TTX)?

A Cybersecurity Tabletop Exercise (TTX) is a **structured, discussion-based simulation** that tests how an organisation would respond to a hypothetical cyber incident. It brings together stakeholders from across departments—technical, legal, public relations, human resources, and leadership—to walk through a fictional scenario and evaluate decision-making, communication, and coordination in a no-risk setting.

Unlike red teaming or penetration testing, a TTX is **non-technical** in **execution**. Participants do not manipulate live systems or utilise cybersecurity tools in real-time. Instead, they simulate how they would respond to evolving events using existing policies, procedures, and experience. The facilitator presents a narrative scenario, and participants must react as they would during a real-world incident, discussing what actions they would take and why.

These exercises are often structured with a set of **injects**—updates or twists introduced during the scenario to simulate how incidents unfold in real time. Injects help prompt discussion and test the agility of response plans.

Why Are TTXs Important?

1. Test Incident Response Plans

TTXs provide a safe way to validate whether your **Incident Response Plan (IRP)** works in practice. Many organisations have IRPs on paper that are never exercised until a real attack hits. A TTX reveals gaps, outdated procedures, unclear responsibilities, or impractical escalation paths.

2. Strengthen Cross-Team Coordination

A cybersecurity incident affects more than just the IT department. It involves legal compliance, executive decision-making, PR messaging, and possibly HR actions. A TTX ensures that all stakeholders are aware of their roles and can **collaborate effectively under pressure**.

3. Improve Communication Workflows

Miscommunication or delay is one of the most common causes of failure during cyber incidents. TTXs help organisations test internal and external communication workflows, including how incidents are reported, who is notified, and what the messaging should be to customers, regulators, or the media.

4. Build Muscle Memory and Confidence

Much like fire drills, tabletop exercises build the **"muscle memory"** necessary for confident action in real incidents. Staff become familiar with procedures, escalation paths, and expected decisions. This confidence directly translates to better outcomes during actual crises.

5. Meet Regulatory and Legal Expectations

Cyber regulations, such as GDPR, HIPAA, the NIS2 Directive, and ISO/IEC 27001, often include requirements to test and review incident response capabilities. TTXs are a widely accepted and effective means of demonstrating **proactive compliance** and risk management.

When Should You Conduct a TTX?

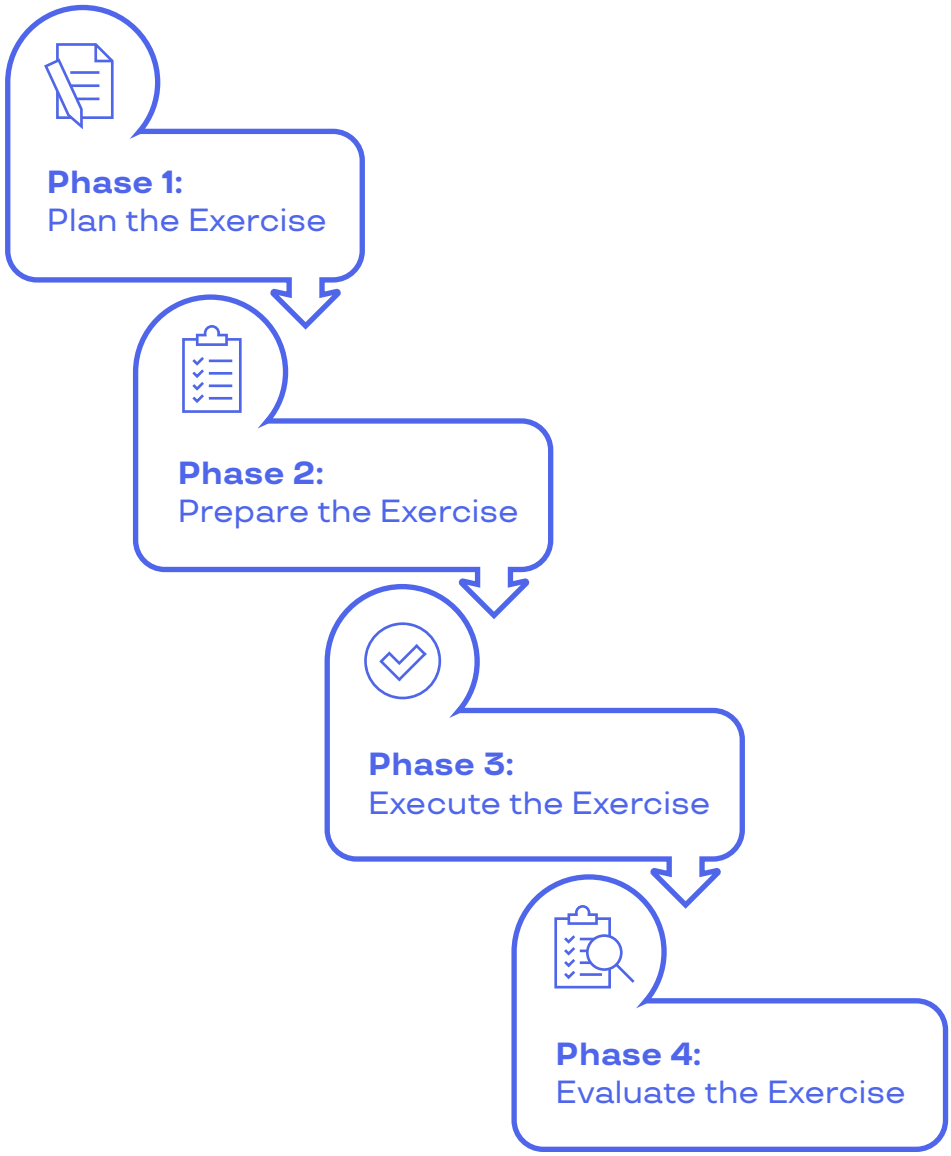
Organisations should run a TTX at least **annually**, or when:

- Significant changes are made to systems, networks, or vendors
- New threats or vulnerabilities emerge
- Leadership or key personnel change
- After a real-world incident (yours or another organisation's)
- Before audits or regulatory reviews

What This Guide Will Help You Do

This quick guidebook is designed to walk you step-by-step through:

- Planning a TTX based on real organisational needs
- Designing realistic scenarios
- Running the session professionally
- Evaluating performance and driving measurable improvement



2. Phase 1: Plan the Exercise

Planning is the foundation of any successful Tabletop Exercise (TTX).
It ensures the session is aligned with actual organisational needs, involves the right people, tests the right risks, and produces beneficial outcomes. Rushing this phase leads to wasted time, disengaged participants, and shallow results.

This section covers how to plan a TTX in five clear steps:

1. **Conduct a Needs Assessment**
2. **Define SMART Objectives**
3. **Determine Scope and Type**
4. **Select Participants and Assign Roles**
5. **Manage Logistics and Timeline**

2.1 Conduct a Needs Assessment

Before building a scenario or selecting participants, you need to understand *why* you're running the exercise.

Step 1: Identify the Core Purpose

Ask leadership:

- Are we testing our Incident Response Plan (IRP)?
- Are we focusing on a specific threat (e.g., ransomware, insider attack)?
- Is the exercise meant to train staff, validate procedures, or meet compliance?

You must have an apparent reason for the TTX. Without it, you'll run an activity that feels generic and produces vague outcomes.

Step 2: Evaluate Your Cybersecurity Context

Gather the following:

- Summary of past incidents (internal or industry-wide)
- Recent audit or compliance findings
- Results from phishing simulations, endpoint monitoring, or threat hunting
- Business priorities (e.g., moving to the cloud, acquiring a company)

Step 3: Align With Organisational Risk Profile

Different organisations face different threats:

- A hospital may need to test data confidentiality under pressure from ransomware.
- A law firm might simulate a breach of sensitive client files.
- A retailer may focus on payment card theft or DDoS attacks.

Use this step to **tailor the exercise** to your organisation's real risks and vulnerabilities.

2.2 Define SMART Objectives

Every effective TTX is guided by **SMART goals**:

- **Specific:** What exactly are you testing or validating?
- **Measurable:** How will you determine if it was successful?
- **Achievable:** Is the objective realistic in the timeframe?
- **Relevant:** Does it address real organisational risks?
- **Time-bound:** Is the exercise scope appropriate to finish within 2–3 hours?

Examples of Good SMART Objectives:

"Test the escalation protocol and decision-making process during a ransomware attack targeting the finance department."

"Evaluate the ability of Legal and PR to coordinate external messaging during a data breach involving customer records."

Examples of Poor Objectives:

"Practice a cyberattack response."
(Too vague — what kind of attack? What response?)

"Ensure everyone knows what to do."
(Unmeasurable and unrealistic in one session.)

2.3 Determine the Scope and Type of the Exercise

Your goals define the scope (who is involved) and type (strategic vs. technical).

Strategic-Level TTX:

- **Audience:** Executives, legal, communications, crisis managers
- **Focus:** Decision-making, business continuity, media response, regulatory impact
- **Scenario:** High-level incidents (e.g., extortion threat, nation-state espionage, third-party compromise)
- **Outcome:** Coordination under pressure, messaging, and liability management

Technical-Level TTX:

- **Audience:** IT, security operations, sysadmins, service desk
- **Focus:** Detection, containment, recovery, escalation, forensics
- **Scenario:** Network breach, phishing entry point, credential compromise
- **Outcome:** Speed, clarity, and accuracy of technical response

Combined or Tandem TTX:

If resources allow, consider a split TTX:

- **Part 1:** Technical team responds to the breach
- **Part 2:** The Executive team is briefed and must make decisions based on the technical outcome

This mirrors real life and creates a richer exercise, but requires careful coordination.

2.4 Select Participants and Assign Roles

Who Should Be Involved?

A comprehensive TTX encompasses all functions impacted by a cyber incident. At minimum:

- IT / Security Operations
- Legal and Compliance
- Public Relations / Communications
- Human Resources
- Executive Sponsor / Crisis Leader

Other possible roles:

- Data Protection Officer (DPO)
- Risk or Audit lead
- External vendor or Managed Security Service Provider (MSSP)
- Insurance representative
- Government or law enforcement liaison

Roles During the TTX

Role	Description
Facilitator	Guides the exercise, presents scenario, asks questions
Players	Actively role-play their real job during the incident
Observers	Watch, take notes, and provide evaluation afterward
Trusted Agents	(Optional) Help plan but do not participate
Note-Takers	Capture key decisions, delays, and observations

Pro tip: Aim for **10–15 total participants**. Fewer than five leads to shallow discussions. More than 15 becomes hard to manage.

Common Pitfalls When Choosing Participants

- Inviting only IT/security > too technical, misses the bigger picture
- Inviting too many executives > they dominate the discussion
- Inviting everyone > no one participates fully

Instead, choose only those whose roles are **essential** for the chosen scenario.

2.5 Manage Logistics and Timeline

Choose a Time and Duration

- **Duration:** 2 to 3 hours is ideal
- **Avoid:** Mondays, Fridays, end of the quarter, or major project deadlines
- **Remote Teams:** Schedule for best overlap of time zones

Venue Options

- **Onsite Conference Room:** More engagement, better energy
- **Virtual (Zoom, MS Teams):** Flexible but less natural interaction
- **Hybrid:** More complex, risks disengagement from remote players

Prepare the Essentials:

- Whiteboard or shared notes (physical or online)
- Projector or screen for slides
- Printed or digital SitMan (Scenario Booklet)
- Backup internet or power if onsite
- Recording tools (if you will document insights)

Notify Participants Early

- Send invitations 2–3 weeks in advance
- Clearly state:
  - This is a simulation, not a test
  - It's a learning opportunity, not a performance review
  - Confidentiality is expected — don't pre-read the scenario

Pro tip: You may also want to run a short **pre-briefing** call 1–2 days before, to answer questions and calm nerves.

End of Phase 1 – Planning Outcome:

By completing these steps, you will have a:

- Clear, measurable purpose
- Scenario mapped to real risks
- Balanced participant group
- Agreed on the scope and schedule
- Confident foundation to move to scenario design

3. Phase 2: Prepare the Exercise

Preparation is where the tabletop exercise comes to life. Once your goals, scope, and participants are defined, you proceed to build the actual scenario, structure the flow of the exercise, and ensure everything is ready for seamless execution.

A successful tabletop exercise is not improvised — it's scripted, structured, and supported by the right materials and mindset.

3.1 Design the Scenario

The scenario is the **core narrative** of the TTX. It drives all participant interaction and determines how realistic and valuable the exercise will be.

Key Elements of a Good Scenario:

1. **Plausible and realistic** – Must reflect actual threats or vulnerabilities.
2. **Relevant** – Aligned with your organisation's sector, size, systems, and processes.
3. **Progressive** – Should evolve with new information ("injects") to simulate pressure and decision-making.
4. **Neutral tone** – Avoid blaming any person or team in the narrative.

Scenario Types:

Scenario Type	Description	Example
Phishing to Ransomware	Starts with a phishing email that leads to system encryption	"An employee opens an attachment marked 'Updated Salary Info'"
Third-Party Breach	Incident originates from a vendor or partner system	"Your payroll provider notifies you of a compromise affecting your employee data"
Data Exfiltration	Internal or external actor exfiltrates sensitive files	"Suspicious FTP traffic is detected to an offshore server"
Insider Threat	Disgruntled or negligent employee causes the incident	"An HR admin exports a database before their last day"
Business Disruption/ DDoS	Your web services are knocked offline	"Your customer portal is unresponsive — suspected DDoS attack underway"

Step-by-Step Scenario Structure:

1. **Opening Situation (Initial Event):**
   Brief participants on the situation at hand — not too much detail, just enough to start the conversation.

Example: "It's Monday morning. Your IT team detects a spike in outbound traffic from the finance department server."

2. **First Inject – Escalation:**
   Present new developments or indicators.

"Several users report being locked out. Ransom note appears on screen demanding Bitcoin."

3. **Second Inject – External Involvement:**
   Introduce regulators, media, clients, or partners.

"Local media calls to ask if you're aware of rumours of a cyber breach affecting customers."

4. **Third Inject – Operational Impact:**
   Increase urgency with business continuity pressure.

"Payroll system is offline; employees will not be paid on time."

5. **Optional Final Inject – Legal/Regulatory Trigger:**
   Trigger privacy notification requirements.

"Forensics confirms that 5,000 customer records were exfiltrated before encryption."

Tips:

- Use time compression: say, "It's now two hours later" to simulate real-time escalation.
- Make events open-ended: let teams decide actions and policies to apply.
- Avoid "gotchas" or trying to trap participants — this is a learning exercise, not a quiz.

3.2 Build Supporting Materials

You don't need to create dozens of documents, but a few well-prepared materials will make your TTX feel structured, serious, and professional.

Required Documents:

Material	Description
Situation Manual (SitMan)	The scenario handout for participants. 1–3 pages max. No spoilers. Includes: background, setting, rules, timeline
Facilitator Guide	The behind-the-scenes playbook: inject schedule, expected questions, time limits, escalation path
Inject Sheet	A timeline of when each new event will be introduced during the session
Participant Roles Sheet	Who is playing what role — and optional brief on their function
Evaluation Form	Simple feedback sheet to collect reactions, insights, improvement areas

Optional Visuals:

- PowerPoint to display the injects and scenario
- A network map or org chart to help visualise
- Timeline tracker on a whiteboard

3.3 Assign Roles: Facilitators, Players, Observers

Facilitator(s):

- Guides the flow of the exercise
- Presents the scenario and injects
- Asks prompting questions (e.g., "What do you do now?", "Who do you notify?", "What policy applies here?")
- Maintains focus, pace, and neutrality

A skilled facilitator is often the **difference between a valuable TTX and a chaotic discussion**.

Pro tip: Avoid having the facilitator also be a participant. It compromises neutrality and flow.

Players:

- Active participants playing their real-life role
- Respond to the evolving scenario
- Collaborate and make decisions
- Should be encouraged to speak freely and without fear of judgment

Observers:

- Typically, from the planning team or external evaluators
- Remain silent, take notes, and report post-exercise insights
- Capture quotes, decisions, breakdowns in process, and strong performances

3.4 Prepare the Environment

This includes both the **physical** or **virtual** setup and the **psychological** readiness of your team.

In-Person Exercises:

- Use a large meeting room with breakout areas
- Projector or screen for slides
- Name placards for roles
- Printed SitMans and inject handouts

Remote Exercises:

- Use a stable and secure platform (e.g., Zoom, MS Teams)
- Share materials via a cloud folder or a PDF
- Designate a co-host to assist with chat and mute functions
- Use breakout rooms for team discussions if needed

Hybrid Exercises:

Hybrid formats (some in-person, some remote) require strong facilitation to keep everyone engaged. Consider using:

- Shared Google Docs or Miro boards
- Dedicated chat channel for injects
- One camera per participant if possible (avoid room-wide webcams)

Psychological Safety:

- Remind participants that this is a safe space to learn
- Avoid blaming individuals
- Keep the tone professional but relaxed
- Allow for humour and openness — people learn better when not stressed

3.5 Pre-Exercise Briefings

A short (30–45 minute) briefing before the actual exercise can dramatically improve participation.

What to Cover:

- Why you doing this exercise (objective)
- Who's participating
- Rules of engagement
- What to expect (e.g., time pressure, decisions, open discussion)
- What is not part of the exercise (e.g., no hands-on incident response)

Last-Minute Tips to Participants:

- "There's no winning or failing — we're here to learn."
- "You don't have to be perfect — just speak honestly about what you would do."
- "We'll gather feedback at the end — your input matters."

End of Phase 2 – Preparation Outcome:

By now, you have:

- A clear and realistic scenario tailored to your risks
- A timeline of injects and response challenges
- Role clarity for all participants and facilitators
- A prepared physical or digital environment
- Psychological readiness and buy-in

You're now fully ready to execute the exercise.

4. Phase 3: Execute the Exercise

This is where everything comes together. The planning and preparation are complete — now it's time to conduct the tabletop exercise.

A well-run TTX is **dynamic**, **engaging**, and **thought-provoking**. It challenges assumptions, reveals blind spots, and helps build resilience. The facilitator is central to success, but all participants must remain actively involved.

4.1 Begin with a Pre-Brief

Start by clearly setting expectations and tone. Many participants will feel nervous, especially if this is their first TTX. Others might be sceptical or distracted. A strong pre-brief creates psychological safety and focus.

Key Messages to Cover:

- Purpose of the Exercise:
  "We are here to test and improve our processes, not people."
- Ground Rules:
  - Speak freely and honestly
  - Stay in role
  - No finger-pointing
  - This is confidential and judgment-free
- Scope of the Exercise:
  - No real systems or tools will be used
  - Focus is on decisions and communications
  - The scenario is fictional, but inspired by real threats

- Flow of the Session:
  - Injects will be presented in real-time
  - Discussion will be open, but guided
  - After the exercise, we'll hold a short debrief and feedback session

Pro tip: Ask participants to introduce themselves and their role — even if everyone knows each other. It resets focus and encourages voice participation.

4.2 Present the Scenario

Once everyone is briefed, begin the narrative.

Example Opening:

"It's Tuesday at 8:15 a.m. The IT team notices unusual traffic from a server in the finance department. That same hour, the CFO reports their laptop behaving strangely. Let's begin."

Distribute the **initial scenario handout (SitMan)** or present it onscreen. Provide only what participants need to start responding. Do not reveal all details at once.

The goal is to simulate the **"fog of war"** — just like in real incidents, teams won't have perfect information.

4.3 Manage the Flow with Injects

Injects are the **key tool** for evolving the scenario and testing how participants adapt to new challenges.

Injects Can Simulate:

- Escalation of technical issues
  "The ransomware spreads to additional systems."
- External pressure
  "A journalist emails the PR team for comment."
- Legal/regulatory triggers
  "Customer data is confirmed exfiltrated."
- Operational disruption
  "Payroll services are interrupted."

Injects should be **timed** or **triggered** by participant actions. For example, only introduce the ransomware note if the team fails to act quickly during the phishing discovery.

Inject Presentation Tips:

- Deliver injects verbally and/or visually.
- Encourage reaction: "How do you respond now?"
- Record key decisions and rationales.
- Avoid overloading — give time for discussion between injects.

Injects should:

- Challenge assumptions
- Surface hidden dependencies
- Reveal gaps in policy, communication, or responsibility

4.4 Facilitate the Discussion

The facilitator's job is to guide, not dominate.

Your Role as Facilitator:

- **Ask questions**, not give answers:
  "What would you do next?"
  "Who is responsible for this decision?"
  "Do you escalate internally or externally?"
- **Balance participation:**
  - Encourage quieter voices
  - Redirect overly dominant participants
  - Reinforce that there are no wrong answers — just learning
- **Keep discussions on track:**
  - If someone dives into deep technical details, refocus on the process "That's a good point — how would that decision be communicated to leadership?"
- Track time and energy levels:
  - Plan natural pauses or mini breaks
  - Adjust the pacing if discussions are too slow or too fast

Handling Difficult Dynamics:

Challenge	What to Do
Silent participants	Invite them directly: "Legal, any concerns from your side?"
Blame or finger-pointing	Re-center the group: "Let's focus on solutions, not fault."
Overtalking/ dominance	Redirect: "Great input — let's hear from others before deciding."
Confusion or disengagement	Re-explain: "Here's where we are in the scenario..."
Technical rabbit holes	"Let's park the technical detail and return to policy implications."

4.5 Document Decisions and Observations

Have one or more note-takers (or observers) write down:

- Key decisions made by the group
- Who made them, and under what rationale
- Delays or confusion during escalation or communication
- Missed or unclear responsibilities
- Strengths and good practices observed

This documentation feeds directly into the **After-Action Report** in Phase 4.

If you're recording the session (with permission), timestamp when major injects are delivered and how long it takes to respond.

4.6 Wrap Up the Exercise

Once all planned injects are delivered and the team has discussed a response to the full incident:

1. Summarise the storyline and response timeline.
2. Ask a few reflection questions:
    - "What surprised you?"
    - "What would you do differently next time?"
    - "Was communication effective?"
    - "Did you feel your responsibilities were clear?"

Then move into a short break, followed by the formal **debriefing and evaluation** in Phase 4.

End of Phase 3 – Execution Outcome:

By the end of this phase, the team should have:

- Worked through a realistic cyber incident under pressure
- Identified decision points, bottlenecks, and uncertainties
- Practised cross-functional coordination
- Begun surfacing lessons to improve future readiness

This is not the end — it's just the critical **moment before improvement begins**. Section 4 will help you capture those lessons and turn them into action.

5. Phase 4: Evaluate and Improve

A tabletop exercise is only as valuable as the lessons it produces. No matter how well the simulation runs, its long-term impact ultimately depends on what comes next: capturing observations, reviewing outcomes, and translating insights into **tangible change**.

This phase involves conducting a structured debrief, gathering formal feedback, and documenting outcomes in an **After-Action Report (AAR)**.

5.1 Conduct the Hotwash

A **hot wash** is the immediate post-exercise discussion, usually held right after the scenario concludes. It captures fresh impressions, emotional reactions, and reflections while they're still top-of-mind.

How to Run a Hotwash:

- Bring all participants together
- Keep it informal but focused
- Use a whiteboard or shared screen to collect responses
- Ask open-ended guiding questions

Key Questions:

- What went well?
- What was confusing or unclear?
- What decisions were difficult to make?

- Did everyone understand their roles?
- What would you do differently in a real incident?

Pro tip: Encourage honesty but avoid finger-pointing.

Participants should feel **safe** to speak candidly. This is not a performance review — it's a learning moment.

5.2 Collect Structured Feedback

After the hot wash, allow participants to **reflect individually** and submit their written feedback.

Use a simple survey (online or paper) with prompts like:

- On a scale of 1–5, how realistic was the scenario?
- Did you feel your role was clearly defined?
- Were communication channels clear and effective?
- Were the objectives of the exercise met?
- What gaps or weaknesses were identified?
- What improvements would you recommend?

Allow for open comment fields to collect qualitative insights.

You can also:

- Hold short follow-up interviews with key roles (e.g., facilitator, PR lead, executive).
- Ask observers for their impressions and timelines.

5.3 Develop the After-Action Report (AAR)

The **After-Action Report (AAR)** is the formal document that summarises:

- What happened
- What was learned
- What needs to change

It serves as a roadmap for future improvement and provides an audit trail for compliance, regulators, or internal oversight.

AAR Structure:

Section	Description
1. Executive Summary	Overview of purpose, scenario, and outcomes
2. Objectives and Scope	Recap of SMART objectives, departments involved
3. Scenario Recap	Timeline of injects and participant actions
4. Strengths Identified	What worked well (policies, teams, decisions)
5. Gaps and Weaknesses	Process breakdowns, unclear roles, communication failures
6. Recommendations	Specific, actionable steps with responsible owners and deadlines
7. Appendices	Participant list, materials used, evaluation forms, raw feedback

Tips for Writing a High-Impact AAR:

- Be clear and concise — 5–10 pages are typical
- Avoid blaming individuals — focus on systems and procedures
- Prioritsze findings by **risk impact** and **ease of implementation**
- Assign **owners and deadlines** for each action item

5.4 Drive Follow-Up Improvements

Once the AAR is completed, don't let it sit in a drawer. Use it to drive actual organisational change.

What to Do:

- Present key findings to leadership
- Integrate lessons into policy updates
- Update the Incident Response Plan (IRP) if needed
- Modify playbooks, contact lists, and escalation protocols
- Create or revise training materials based on weak points
- Schedule follow-up training or a focused mini-TTX

Best practice:
Review progress on AAR action items monthly until completed.

Example Improvements:

Weakness Identified	Action Item	Owner	Deadline
Delay in external notification	Create crisis communication checklist	PR Lead	June 15
Confusion over legal obligations	Conduct legal awareness session for IT	Legal	May 30
Unclear roles during escalation	Add escalation chart to IRP	CISO	July 1

5.5 Track and Share Lessons Internally

A TTX creates knowledge beyond the participants. The rest of the organisation can also benefit.

- Share anonymised lessons learned across departments
- Use insights in internal newsletters, wikis, or learning portals
- Highlight positive examples of collaboration and fast thinking
- Recognise individuals or teams who responded well

This strengthens the **organisational culture of preparedness** and positions the TTX as a valuable investment of time and effort.

End of Phase 4 – Evaluation Outcome:

If done well, this phase produces:

- A trusted record of the exercise
- Honest insights into strengths and weaknesses
- Specific action items for improvement
- Increased confidence across the organisation

This is the moment where planning meets execution, and execution leads to measurable progress.

Your tabletop exercise is now complete, but your improvement cycle is just beginning.

6. Practical Tips and Common Pitfalls

Even the best-planned tabletop exercises can fall flat without careful attention to dynamics, structure, and tone. This section presents **valuable lessons** from experienced TTX facilitators and cybersecurity professionals.

6.1 What to Do – Practical Tips for Success

Start with Clear Intentions

Before doing anything else, ensure everyone involved understands:

- Why is the exercise being held
- What are the expected outcomes?
- Who is responsible for what? This helps prevent confusion and ensures the TTX is outcome-oriented.

Design Around Real Threats

Your scenario should reflect the organisation's actual risk landscape — don't choose a ransomware scenario just because it's trending. Consider:

- Your industry's top cyber risks
- Recent incidents (internally or in the supply chain)
- Weaknesses discovered in audits or penetration tests. A relevant scenario increases engagement and leads to meaningful lessons.

Keep It Time-Bound and Tight

A good TTX typically lasts 2–3 hours. Stick to that:

- Too short, and you lose depth
- Too long, and people disengage

Structure your timeline carefully:

- 10–15 min introduction
- 60–90 min scenario play
- 20–30 min hotwash
- Optional follow-up survey post-exercise

Use Facilitators with Real Experience

The best facilitators:

- Are calm under pressure
- Understand both technical and business perspectives
- Know when to let the group discuss vs when to move forward
- Ask probing, open-ended questions without leading participants

You can use internal staff, external consultants, or hybrid facilitation teams — just make sure they're respected and neutral.

Document in Real Time

Assign one or more note-takers or observers to document:

- Who made key decisions
- Where confusion arose
- How communication flowed (or didn't)
- Missed opportunities or protocol violations

This information becomes the backbone of your After-Action Report.

Create a Culture of Learning

Remind participants throughout:

"This is not a test. This is a safe space to learn and improve together."

A healthy exercise culture encourages honesty, transparency, and improvement, not blame.

Involve Leadership (Meaningfully)

Getting senior executives in the room (or on the call) dramatically increases:

- Perceived importance of the exercise
- Visibility into cross-functional coordination
- Speed of follow-through on improvements

Executives don't need to be involved in every detail, but they should participate in strategic decisions and communication elements.

6.2 What Not to Do – Common Pitfalls to Avoid

Designing Overcomplicated Scenarios

Resist the urge to impress participants with overly complex information.

Common mistakes:

- 10+ injects that confuse or overload participants
- Unclear timeline ("what's happening when?")
- Unrealistic or technically implausible events

Instead: Focus on **clarity**, **relevance**, and **decision points**.

Making the Exercise a Performance Review

A TTX is not the time to measure individual performance or assign blame.

What happens when this occurs?

- People go silent to avoid looking bad
- Managers dominate discussions
- Real issues stay hidden

Shift the mindset to: "We succeed together by identifying and fixing what doesn't work."

Letting One Group Dominate

Security or IT staff often take the lead, sometimes too much.

But cyber incidents involve:

- Legal compliance
- Reputation management

- Customer communication
- Business continuity

If IT makes every decision in the exercise, you're missing the real-life complexity of cyber crisis response.

Instead: Ensure every function gets a chance to lead decisions tied to their expertise.

Neglecting Non-Technical Functions

Some organisations treat cybersecurity as a purely technical issue.

But in reality:

- **PR manages media fallout**
- **Legal handles breach disclosure**
- **HR addresses internal violations**
- **Finance manages payouts and budgets**
- **Executives own risk**

If you exclude these groups, your exercise won't reflect real-world dynamics, and the lessons will be incomplete.

Skipping Documentation

If you don't record what happened during the TTX:

- Lessons are lost
- Improvements go unassigned
- Leadership never sees the value
- Compliance documentation is incomplete

Always assign a note-taker. If possible, record the session (with consent) for accuracy.

Doing One-Off Exercises

A single tabletop every few years does little for real resilience.

Instead:

- Run annual or semi-annual TTXs
- Rotate through threat types and scenarios
- Incorporate new policies, tools, or hires
- Track lessons over time in a maturity roadmap

Summary of Best Practices

Do This	Not This
Design around real threats	Use generic or irrelevant scenarios
Keep scenarios focused	Add unnecessary complexity
Foster open discussion	Blame or shame participants
Involve business functions	Make it an IT-only event
Document and follow up	Forget what you learned
Repeat and improve	Treat it as one-and-done

7. Templates and Checklists

Templates simplify planning and make your exercise feel organised and professional. This section includes two core tools you can use immediately:

- **A TTX Planning Worksheet**
- **A Post-Exercise Evaluation Checklist**

These are meant to be practical, editable, and scalable — suitable for both small and large organisations.

7.1 Cyber TTX Planning Worksheet

Use this template to plan your exercise from goal setting to logistics.

TTX Planning Worksheet

Field	Description	Example
Exercise Title	Name of the TTX	Operation Shadow Breach
Date & Time	Schedule for the exercise	May 28, 2025, 10:00–13:00
Duration	Total session time	3 hours
Location / Platform	Physical location or virtual platform	Conference Room A / MS Teams

Field	Description	Example
Facilitator(s)	Lead(s) guiding the session	John Smith, Cyber Resilience Officer
Scenario Type	Chosen threat or incident	Phishing > Credential Theft > Ransomware
SMART Objectives	Clear, outcome-driven goals	Test communication and legal escalation flow
Scope	Full organization or selected teams	Finance, IT, PR, Legal
Participants	Names and departments	List with roles assigned
Observers	Evaluation support staff	Cyber training team / consultants
Inject Timeline	Outline of scenario progression	Inject 1: Suspicious activity (10:15), Inject 2: Ransom note (10:30)
Supporting Materials	Documents or handouts	SitMan, role cards, escalation chart
Contact List	Emergency/ role-specific contacts	CISO, Legal Counsel, PR Director
Notes / Special Considerations	Other factors to keep in mind	Notify reception, no laptops during session

Customise this template for each exercise based on scale and objectives.

7.2 Post-Exercise Evaluation Checklist

Use this checklist during and after the exercise to evaluate performance, communication, and coordination.

Post-Exercise Evaluation Checklist

1. Objective Fulfillment

- Were the exercise goals clearly defined?
- Did the scenario allow testing of key decision points?
- Were all SMART objectives addressed?

2. Participant Engagement

- Did all participants actively contribute?
- Were participants comfortable sharing perspectives?
- Did each function (IT, Legal, PR, etc.) have opportunities to lead decisions?

3. Scenario Effectiveness

- Was the scenario realistic and relevant?
- Did the injects simulate real escalation pressure?
- Were time constraints appropriate?

4. Communication Flow

- Were incident communications escalated promptly?
- Was there clarity in who communicates what (internally and externally)?
- Did teams coordinate effectively under pressure?

5. Decision-Making Process

- Were decisions timely and aligned with policy?
- Did executive-level roles step in appropriately?
- Were there any decision delays due to unclear authority?

6. Role and Responsibility Clarity

- Did each participant understand their role?
- Was there confusion over ownership of key actions?
- Did escalation flow align with the IRP?

7. Gaps Identified

- Were any weaknesses found in policies or plans?
- Were there missed or delayed actions?
- Were there inconsistencies in communication or escalation?

8. Improvement Opportunities

- Have recommendations been documented?
- Have follow-up actions been assigned?
- Has a timeline been proposed for improvements?

Optional Participant Feedback Questions:

- What surprised you the most during the exercise?
- What part of the scenario felt most realistic?
- What would help you respond better in a real event?
- Any confusion or uncertainty you experienced?

Distribute via online forms, printed surveys, or follow-up interviews.

These tools not only improve exercise execution, they also support **documentation**, **compliance**, and **continuous improvement**. You can adapt them into branded templates or add them to your incident response playbooks.

8. Final Recommendations

Conducting a cybersecurity tabletop exercise is not a checkbox activity. It is a strategic investment in your organisation's ability to withstand and respond to digital threats. Whether you are a government agency, private enterprise, or nonprofit, the insights gained from a TTX can expose blind spots, build bridges between departments, and ultimately protect what matters most: your people, your operations, and your reputation.

Here are our final recommendations:

Make It a Recurring Practice

- Conduct at least one TTX per year
- Vary the threat types and departments involved
- Align with risk assessments and changes in the threat landscape

Build a Culture of Preparedness

- Encourage open, blame-free communication during and after exercises
- Normalise continuous improvement and feedback
- Recognise and reward participation and leadership

Turn Lessons into Action

- Use After-Action Reports (AARs) to drive measurable improvements
- Update incident response plans and playbooks accordingly
- Track follow-up tasks and assign ownership with deadlines

Include the Right People — Every Time

- Cross-functional participation is essential: technical, legal, PR, executive
- Don't let one department dominate the exercise
- Make sure decision-makers are present and involved

Use Tools and Templates

- Standardised templates save time and improve consistency
- Build an internal library of past scenarios, injects, and reports

Final Thought

Cybersecurity is no longer just an IT issue — it is an organisational responsibility.

A tabletop exercise is one of the **most cost-effective and impactful ways** to prepare your team for the inevitable. The time to test your plan is **before** the crisis, not during it.

Run the exercise. Learn from it. Improve continuously.

References

1. **Robert Lelewski and John Hollenberger**. *Cybersecurity Tabletop Exercises: From Planning to Execution*. No Starch Press.2025

2. **Global Forum on Cyber Expertise (GFCE)**. *Introduction to Tabletop Exercises (TTX): A Practical Guidebook for Organizations*. March 2023.

3. **CISA Tabletop Exercise Package (CTEP)**. *Exercise Planner Handbook*. Cybersecurity and Infrastructure Security Agency (CISA).

4. **Lukáš Bátora**. *Tools for Conducting Cybersecurity Tabletop Exercises*. Bachelor's Thesis, Faculty of Informatics, Brno, Fall 2023.

5. **Department of Defense**. *Cyber Table Top Guide, Version 2.0*. Director of Defense Research and Engineering (Advanced Capabilities), 16 September 2021.