HEFESTIS

2020

STOic TTX (Tabletop Exercise) Framework

A STANDARDISED APPROACH TO CYBERSECURITY RESILIENCE EXERCISING

HEFESTIS LTD | Unit 27 Stirling Business Centre, STIRLING, FK8 2DZ

Contents

Introduction

Cybersecurity Incident Response is a focus of the Scottish Public Sector Action Plan but assessing an organisation's readiness and response maturity is extremely difficult without a real or imagined incident to use as a catalyst. An organisation that merely has policies, procedures and plans is not ready for an incident. Rather, the prepared organisation has tested and exercised its policies procedures and plans against the unknown.

To deliver a consistent approach to cybersecurity resilience exercising, there needs to be a standardised approach to use as a point of comparison. A standard framework and trained facilitators help to ensure consistency of results and help to ensure that the results are actionable and comparable from one exercise to another.

The STOic TTX framework provides an approach for organisations to:

- exercise management's and operational teams' cybersecurity incident response
- identify gaps in skills, knowledge, tools, and processes to efficiently respond to cybersecurity events
- assess the organisation's cybersecurity incident response maturity
- produce standardised output so that results can be compared from exercise to exercise
- encourage frequent exercising through engaging and streamlined incident scenario design
- provide remote and in-person delivery methods

While there are multiple sources of cybersecurity tabletop exercise (TTX) scenarios, including the NCSC's "Exercise in a Box", the challenges that most organizations experience in carrying out exercises are found in the complexity and uncertainty of the facilitation process. The success or failure of a tabletop exercise and the organisation's desire to repeat the process of exercising is largely determined by the quality of the facilitation.

Facilitation, like auditing, requires asking the right questions and asking the questions that participants may not be prepared for. Training and experience can help facilitators do this well. STOic TTX seeks to grow and train facilitators from within the organisation itself so that effective and frequent exercising can be performed.

This Framework consists of the elements required to deliver successful tabletop exercises with actionable outcomes to test and improve an organisation's ability to respond to cybersecurity incidents.

The STOic TTX Framework

Strategic, Tactical, and Operational Tabletop Exercises

Every level of an organisation needs to be ready to respond to cyber threats at any time. The STOic TTX Framework is designed to adapt and be presented to the three incident response layers in a typical organisation:

1. **Strategic**: senior management, C-suite, Boards, business leaders, etc.
2. **Tactical**: department management, IR coordination teams, crisis teams, communications teams, legal teams, etc.
3. **Operational**: IR teams, IT specialists, Help Desks, Security Operation Centres, etc.

STOic TTX is designed from the start to encourage frequent exercising. To achieve this, the Framework trains facilitators to deliver fast and flexible scenarios that provide the optimal level of challenge for the participants provides a Scenario Builder to ensure that an organisation always has relevant scenarios to exercise, and makes exercising inclusive and approachable.

STOic TTX is unique in that it is organisation-focused, not attack-focused. That means that the focus is not on the specific technical details of the attack in a scenario, but rather on the organisation's people, processes, and technology poised to respond to attacks. This also means that the facilitator does not need to be a cyber-attack expert to be successful, and that means that people from non-technical backgrounds can facilitate STOic tabletop exercises.

The steps of the STOic TTX Framework are:

1. Pre-Assessment
2. Identifying objectives
3. Identifying attendees
4. Scheduling
5. Building the scenario
6. Delivering the scenario
7. Capturing outputs and actions

The STOic TTX model also includes:

- A certification path to provide assurance to management and to guide the organisation towards maturing in their ability to exercise their incident response capabilities
- Facilitator training to ensure that the organisation can experience high-quality exercises as often as it needs to develop a mature incident response capability

The STOic TTX Process

Pre-Assessment

To ensure that appropriate scenarios are created for a tabletop exercise, the facilitator should identify how familiar the organisation is with tabletop exercises and what Incident Response (IR) documentation is available.

The Framework includes a set of questions that will provide the facilitator with some background information for the organisation. Ideally, this should be done before the initial planning meeting.

STOic TTX Pre-assessment Questions

- Do you have a Cyber Incident Response Plan?
- Have you tested your Cyber Incident Response Plan?
- Do you have a Cyber Incident Response Team?
- Do you have a process to take action on the outcomes of testing your Cyber Incident Response Plan?
- Have your staff received Cyber Security Awareness Training?

Answers gauge the organisation's level of experience with tabletop exercises from 0 – 5 with 0 being limited or no experience and 5 having some experience.

Once the organisation's readiness for tabletop exercises is established, the next step is to identify what is desired from conducting an exercise in the organisation by setting some objectives for the exercise.

Identifying Objectives

To measure the success of the TTX programme, clear objectives need to be identified before each event. This also allows for appropriate scenarios to be created that are aligned to the objectives. There is no point in having a scenario test an organisation's response to a stolen laptop containing confidential data if the main objective is to test the organisation's ability to detect and properly react to hostile activity.

Appendix B includes an example form used to identify what stakeholders expect from a series of tabletop exercises. The typical objectives of a tabletop exercise are listed in the table below. The levels associated with each objective relate to the expected STOic TTX certification path levels. However, an organisation can set their own objectives no matter what certification level the organisation might be.

Objectives of TTX	Level
Test effectiveness of the organization's incident response plans	Bronze
Test ability to detect and properly react to hostile activity	Silver
Test the organization's capability to determine operational impacts of cyber attacks and implement proper recovery procedures	Silver
Test the effectiveness of communications processes during an attack	Bronze
Understand the implications of losing access to IT systems and test the workarounds for such losses	Silver
Expose and correct weaknesses in cyber security systems, policies, and procedures	Silver
Determine what enhancements or capabilities are needed to protect an information system and provide for operations in a hostile environment	Bronze
Enhance cyber awareness, readiness, and coordination	Silver
Develop contingency plans for surviving the loss of some or all IT systems	Silver

Determine the effectiveness of cyber training provided to staff	Bronze

Once the objectives are understood, it will be clearer who from the organisation should attend the exercise. For example, if the main objective is to test the effectiveness of communications processes during an attack, then participation from the communications team, and probably representation from HR and Legal will be required, not just participants from IT.

Identifying Attendees

The attendees of a tabletop exercise are related to the identified objectives and the level of the exercise (Strategic, Tactical, or Operational). Who to choose to attend will also depend on the roles and responsibilities those people hold within the organisation.

Research has shown that exercises with more than ten participants present a challenge for everyone to provide their valuable perspectives. To get the most from the exercise, and to ensure everyone can provide input, attendance should be limited to around ten people. Although, if there is a point where a staff member would be required for a small amount of time, the facilitator can arrange a window of time in the exercise, so the staff member does not have to sit through the entire exercise.

Examples of who should attend which scenario:

Level	Who	Why
Strategic	Executive Leadership Team	As there can be a tendency for executive leaders to underestimate the importance of security, giving executive leaders hands-on practice in a scenario where they have to: - make critical decisions (e.g. whether or not to pay a ransom) - create and approve communications statements regarding a breach - make decisions on sharing breach information (e.g. with Police) Exercising these scenarios will provide the skills to enable executive leaders to respond effectively during the stress of a live scenario.
Tactical	Senior Management	Participation will exercise skills in: - understanding the impact on the organisation - making critical business decisions regarding services shutdown/runtime - giving authorisation to departmental resources - enforcing policies

Operational	IT – Department	For IT staff, participation will exercise the focus on creating smooth handovers, escalation protocols, crisis management and communication channels. As well as testing their capabilities to: - uphold and enforce security policies - ensure response processes are in place
Operational	IT – Front Line Helpdesk	To test front line teams' ability to monitor and triage alerts efficiently and effectively and give staff the confidence and knowledge to escalate events when necessary
Operational	IT – 2nd/3rd Level	Improving teamwork and knowledge in procedures, keeping skills sharp, knowing your responsibilities in a crisis.

Scheduling

Once objectives and attendees have been identified, a date and duration for the event should be arranged.

Tabletop exercises that are being delivered remotely should, ideally, be no longer than 90 minutes. With the actual exercise lasting around 60 minutes and time before for introductions and time after the exercise for the "hotwash" session to document actions, and general review. This timescale is for tabletop exercises for bronze maturity level organisations. Those with silver or gold maturity levels should consider a minimum of 2 hours with comfort break(s) at convenient points in the exercise.

Something worth considering is "hijacking" an existing regular meeting where all/most optimal attendees will be present. In real life, there is no prior warning to organisations that they are about to be attacked. Hijacking brings with it the element of surprise which can make the tabletop exercises more true-to-life as participants will not expect or be prepared for the event.

Once the date for the tabletop exercise has been scheduled, with confirmed availability of those required to be in attendance, the next step is to build the scenario.

Building Scenarios

The facilitator will build the scenario using the STOic TTX Scenario Builder or a pre-made scenario, in line with the defined objectives of the tabletop exercise and the level of the exercise (Strategic, Tactical, or Operational). The scenario will consist of an initial outline brief of the cyber incident including any assumptions, artificialities, and simulations. There will also be a series of injects to drive the objectives of the exercise, these will be designed not to overwhelm the training audience.

The table below lists the STOic TTX Core Scenarios and the objectives that are tested within each.

Scenario	Description	Meets objectives
Virus	A user has clicked a link in a spear-phishing email, This has installed malicious software on the device.	01, 02, 03, 04, 05, 06, 10,
Denial of Service (DoS)	An abnormally high amount of network traffic is being experienced and is visible in system performance statistics and the volume of log data. Additional notification from users about reduced network capability or inability to access the website has been received.	01, 02, 03, 04, 05, 06, 07,08, 09, 10
Unauthorized computer on network	An attempt is made to connect an unauthorized laptop to the organisation's network.	01, 03, 06, 07, 08, 10
Malicious external scanning	An in-depth, long-running external scan of the organisations' network is being performed.	01, 02, 03, 04, 05, 06, 07, 08
Malicious internal scanning	A device on the network is performing scans on the internal network.	01, 02, 03, 05, 06, 07, 08, 09
Computer compromise	Unattended computers with no password screensaver lock have notes in the on-screen text editor that the computer has been compromised.	01, 02, 03, 04, 06, 07, 08, 09, 10
Phishing via email	A phishing email is sent to multiple employees attempting to capture credentials.	01, 02, 03, 04, 06, 07, 08, 09, 10
Ransomware	Core servers and many endpoints have been infected with ransomware and are non-functional.	01, 02, 03, 04, 05, 06, 07,08, 09, 10

Delivering STOic TTX Scenarios

Most participants, if not all, will not be informed of the scenario until they are participating in the exercise. This helps to make the scenario as realistic as possible. There is no advanced warning given in real attacks.

Participants will be asked to suspend reality and not "fight the scenario." There are often events in the real world that do not occur as one might expect. The intention of a tabletop exercise is not to argue about whether something could happen, but to explore how participants would act/respond if it did happen. If participants are fighting the scenario, one question that can refocus the participants is, "If this did happen as described, what would have had to happen to make that possible?"

It will also be made clear to attendees that this is not a test nor an audit. There is no score. This is an opportunity to practice the organisation's decision-making in a safe setting. In a live incident where emotions are high, facts are few and time is not on your side, clear decisions based on preparation will shorten the time to recovery. This is a learning opportunity, not a personal test or exam. It is a training exercise to identify gaps in skills, tools, knowledge, and procedures.

A typical sequence within an exercise:

Step	Notes
Introductions	• Introductions from participants and their role in the exercise
Explanation to Participants: **Don't Fight the Scenario**	• Explain the exercise • No time pressures • Safe environment • not recorded, only actions/outcomes logged • No right or wrong answer • Not a test or exam • Exercise designed to stimulate discussion • the more you engage, the better the outcome • Treat it as a real scenario
Begin Exercise	• Facilitator introduces the scenario • Let discussions evolve naturally • Identify risks and issues, steps to be followed, etc. • Identify internal and external participants in the scenario • Use leading questions to stimulate conversation. For example, "what would you do this in this situation?" • Facilitator will provide injections as needed
Document the Exercise	• Take notes during the discussions • Forms a basis for after-exercise review • Note areas that need more research • Summarize action items • Document issues identified

After Exercise Review	• Review exercise objectives • One participant will summarise the discussion and recommendations • Feedback from all participants • Facilitator will document concerns and actions to be taken forward by the organisation

TTX Output and Actions

The facilitator will complete the STOic TTX Exercise O&A Report, which details all outputs and action items generated from the exercise.

It will be of great benefit to complete all actions before a similar exercise is performed, otherwise, a subsequent exercise is likely to uncover similar key findings to those already identified.

Indicators of a successful tabletop exercise are:

- Objectives of the tabletop exercise have been met
- Participants are exhausted but hopeful
- Attendees should feel like they have been through an ordeal and emerged triumphantly on the other side.
- Senior management has confidence their IT department has a plan to handle security incidents.
- All departments have a better understanding of what is required from them during an incident.

A timescale and date for the next tabletop exercise should be agreed upon. The specific date does not need to be arranged at this time, as the objectives and attendees will need to be agreed upon, but the approximate timescales when the next exercise should occur should be recorded.

Additional Resources

Certification

Organisations need to be able to assure that their TTX programme is progressing, is meeting objectives and that the organisation is better able to respond to cyber incidents. STOic TTX includes a high-level, self-certification path that can provide this assurance.

The scope of this certification is determined by the organisation. The scope could cover the entire organisation or certain departments.

Level	Description
Bronze	Participated in four Core Scenarios
Silver	Participated in four Core Scenarios, three of which included two additional injects

Gold	Participated in any four scenarios with an expert Cyber Professional in attendance to present adaptive injects

Facilitator Training

Facilitator training is delivered via the STOic TTX Facilitators Training Programme. This is achieved through a guide, a series of online training videos and participation in STOic TTX events.

There are a lot of resources a facilitator needs to feel properly equipped, supported, and resourced to confidently deliver a successful STOic TTX. Some of these resources the facilitator may already have. The STOic TTX Facilitators Training Programme is designed to address the gaps in these requirements and prepare facilitators to run engaging scenarios and achieve the goals of the framework.

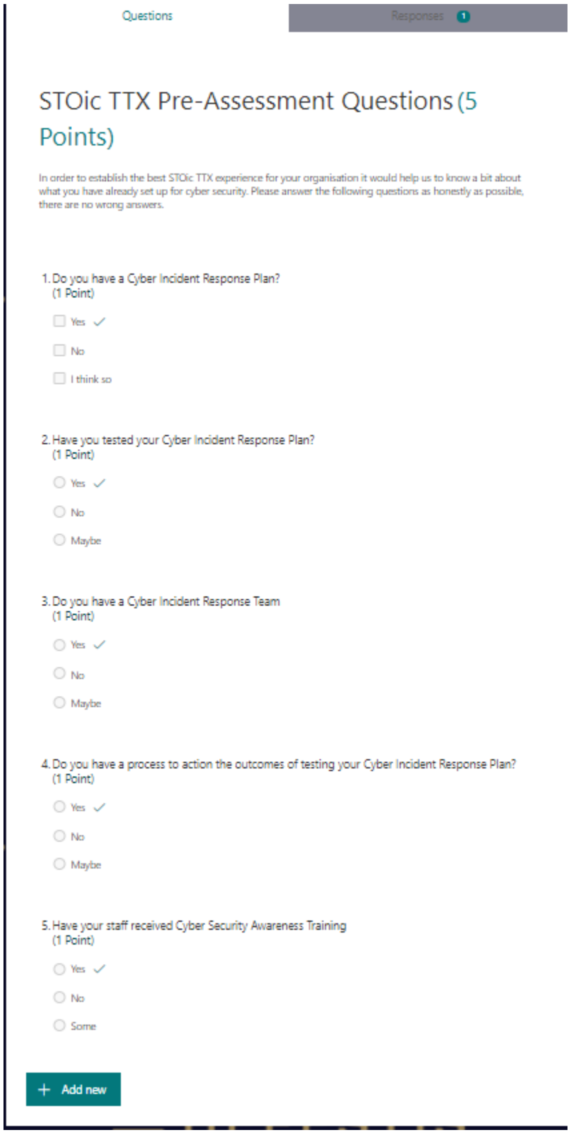
The video training series can be found here:

https://www.youtube.com/playlist?list=PLMPfYFGpMbH4rYomEC6xLBrMZ9mcOUdlX

Appendices

A – TTX in Your Organisation (Form)

Below is a screenshot of an example form that can be used to assess the organisation's readiness for testing and to determine the appropriate level of testing.



STOic TTX Pre-Assessment Questions (5 Points)

In order to establish the best STOic TTX experience for your organisation it would help us to know a bit about what you have already set up for cyber security. Please answer the following questions as honestly as possible, there are no wrong answers.

1. Do you have a Cyber Incident Response Plan?
(1 Point)

□ Yes ✓

□ No

□ I think so

2. Have you tested your Cyber Incident Response Plan?
(1 Point)

○ Yes ✓

○ No

○ Maybe

3. Do you have a Cyber Incident Response Team
(1 Point)

○ Yes ✓

○ No

○ Maybe

4. Do you have a process to action the outcomes of testing your Cyber Incident Response Plan?
(1 Point)

○ Yes ✓

○ No

○ Maybe

5. Have your staff received Cyber Security Awareness Training
(1 Point)

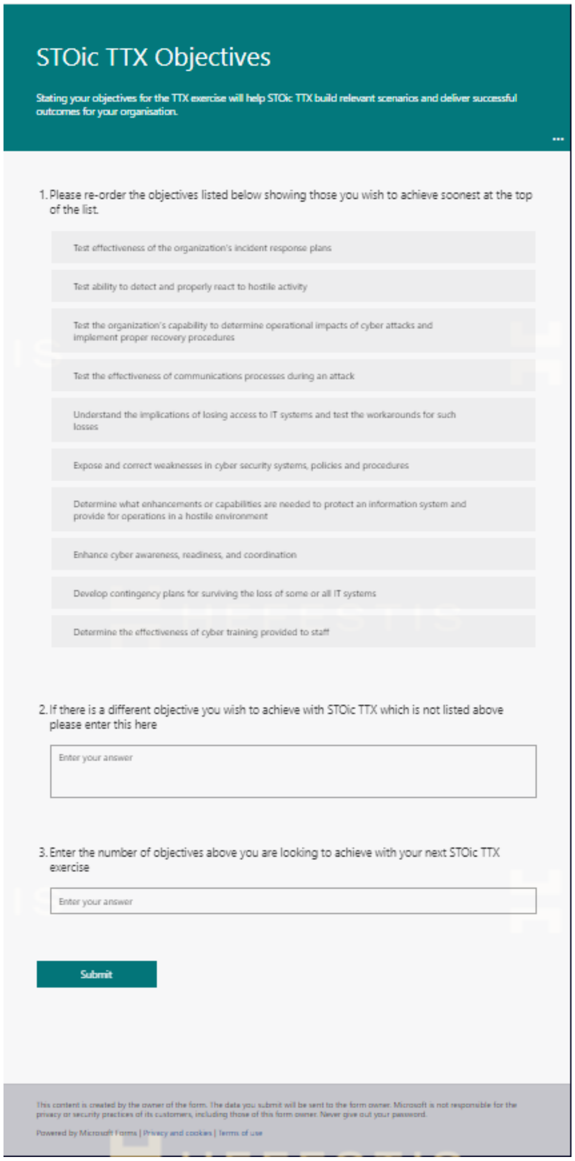
○ Yes ✓

○ No

○ Some

B – STOic TTX Objectives (Form)

Below is an example of a form that can be used to assess what expectations the TTX stakeholders have in regards to testing objectives.



STOic TTX Objectives

Stating your objectives for the TTX exercise will help STOic TTX build relevant scenarios and deliver successful outcomes for your organisation.

1. Please re-order the objectives listed below showing those you wish to achieve soonest at the top of the list.

- Test effectiveness of the organization's incident response plans
- Test ability to detect and properly react to hostile activity
- Test the organization's capability to determine operational impacts of cyber attacks and implement proper recovery procedures
- Test the effectiveness of communications processes during an attack
- Understand the implications of losing access to IT systems and test the workarounds for such losses
- Expose and correct weaknesses in cyber security systems, policies and procedures
- Determine what enhancements or capabilities are needed to protect an information system and provide for operations in a hostile environment
- Enhance cyber awareness, readiness, and coordination
- Develop contingency plans for surviving the loss of some or all IT systems
- Determine the effectiveness of cyber training provided to staff

2. If there is a different objective you wish to achieve with STOic TTX which is not listed above please enter this here

Enter your answer

3. Enter the number of objectives above you are looking to achieve with your next STOic TTX exercise

Enter your answer

This content is created by the owner of the form. The data you submit will be sent to the form owner. Microsoft is not responsible for the privacy or security practices of its customers, including those of this form owner. Never give out your password.

Powered by Microsoft Forms | Privacy and cookies | Terms of use