Cyber - General Exercising Principles

In today's constantly evolving cyber threat landscape, organisations must be prepared to detect and respond to incidents quickly to minimise financial, operational, and reputational impact. Cyber exercising allows organisations to test their readiness and help and identify gaps that could hinder an effective response to a real-world cyber incident.

This Loss Prevention Standard provides guidance on undertaking cyber incident response exercises.

Version: 1.0
Date: 9th March 2026

Cyber - General Exercising Principles

Introduction

With the ever changing and evolving threat landscape, it's crucial that organisations develop and maintain resilience to cyber incidents.

Organisations need to be able to detect and subsequently respond quickly and effectively to a cyber incident with the objective of reducing the financial, operational and reputational harm it can cause. Therefore, having effective cyber security incident response plans and procedures in place is crucial, as is their effectiveness.

These plans need to be effectively tested, typically during quieter periods, as cyber exercising forms an integral part of building resilience and providing a level of assurance. At the broader level, cyber exercises help organisations practice their response, build confidence in the teams responding and identify any gaps.

Cyber exercising can take many forms and the most appropriate solution is dependent on many factors, including the cyber maturity of an organisation. Discussion based exercises, known as tabletop exercises (TTXs) are most commonly implemented initially, progressing to more technical and involved exercises, such as live play simulations.

The benefits of cyber exercising are wide reaching, from identifying key gaps and weaknesses in an organisations response, to building confidence in relevant teams to respond effectively during an incident.

Pre Cyber Exercise Activities

Before developing a cyber exercise and an exercise programme, there are various key factors that should be considered:

- Cyber incident response plans need to be implemented and ratified prior to engaging in planning a cyber exercise.
- Ensure that your cyber incident response plan is socialised with key stakeholders in your organisation, especially those who will need to attend a cyber exercise.
- Ensure there is good buy in from senior management, it's crucial for the success of an exercise and subsequent exercise programme.
- Consult your risk register, ensure that any scenarios you wish to develop are linked back to the risk register.
- Set clear objectives from the outset. This is fundamental to a successful exercise.
- Think reasonable worst-case scenarios and those that are likely to happen, try to avoid doomsday scenarios.
- Don't overcomplicate it, it's better to start small and build from there.
- Consider wider business continuity, disaster recovery and crisis management plans.

- Consider what resources you have available, both in terms of people and financial cost. You can utilise freely available resources for TTXs.
- Foster a positive environment for cyber exercises; remember there are no wrong answers and it is not a test.

Tabletop Exercises

TTXs can prove especially beneficial. They are generally scalable, discussion-based workshops around a scenario where key stakeholders, who are involved in the response to an incident, come together to walk through their response to a simulated cyber incident. TTXs also help identify any gaps in an organisations response, build confidence in the teams response, improve communication and help ensure preparedness in case of a real cyber incident. They are generally not conducted in real time, a scenario that would play out over hours or days can be condensed into a few hours.

The **National Cyber Security Centre** (NCSC) has a freely available tool, Exercise in a Box, which has around 20 exercises that organisations can use. These cover key topics such as ransomware, supply chain and data breaches. ARMS Cyber recommends organisations visit this resource (linked at the end of the document) as a first stop for thinking about TTXs.

Live Play Exercises

A cyber live play exercise is a fully immersive simulation where participants, in a controlled environment, respond to an incident allowing them to participate in their respective roles as they would do during a real-world cyber incident.

Live play exercises are generally recommended for organisations that are more cyber mature and have already had a robust exercising programme in place.

General Cyber Exercising Principles

Whether organisations are looking to run a TTX or a live simulation, there are a number of underpinning principles that can help ensure the success of the exercise. These principles apply if you are designing an exercise in house or using a paid service.

Exercise Control Team

No matter the size of your organisation, having a dedicated temporary Exercise Control team (EXCON) is key. Ensuring the nature and detail of the exercise is kept in a protected, closed environment is crucial to ensuring a real, non-rehearsed response from participants. EXCON are responsible for:

- Ensuring the right internal and external stakeholders are involved in the exercise.
- Ensuring the exercise remains realistic and proportionate.
- Maintaining oversight during the exercise itself to ensure there's no scope creep.
- Identifying lessons throughout the planning and delivery process to factor into future exercises.
- Scheduling the exercise during anticipated quieter periods for the business.
- Assigning a facilitator role for the exercise.
- Assigning a name to the exercise.

Note: Use the term 'EXERCISE EXERCISE EXERCISE' in all correspondence relating to the exercise, this helps avoid any potential confusion that it's a real incident

Exercise Metrics

EXCON needs to ensure that there are clear metrics to measure performance during the exercise. Failure to do so could lead to confused reporting and bias. Metrics to consider include:

- Participants following agreed response plans.
- Timeliness of acting on assigned tasks.
- Effectiveness of any actions taken.
- Quality of decisions made and any associated response material produced.

An example of some exercise metrics that can be used are not at all confident / slightly confident / somewhat confident / fairly confident / completely confident.

Exercise Scenario Development

The exercise scenario needs to link back to the exercise objectives and your risk register. There are some key points to bear in mind when developing the exercise scenario to ensure its relevance to your organisation:

- Proportionality – keep it reflective of the types of incidents that could impact the organisation.
- Reasonable worst case – don't be tempted to go to the worst possible incident.
- Threat based – where possible, use open-source information to research what threats your type of organisation faces

Exercise Injects

An inject is information that participants receive during the exercise, providing updates to the evolving scenario. These can be provided verbally or in writing during the exercise. It is important to ensure they are technically correct, so engage with the relevant teams responsible for each area for input and direction. Injects also need to be clear and concise, with a measurable outcome to prompt a response from participants.

Participant Guidance

Having clear guidance for participants is crucial, this should be sent out a few days ahead of the exercise. Key considerations include:

- Exercise rules.
- Expectations of participants, encouragement to not 'fight the scenarios' and to feel comfortable to make decisions based on incomplete information.
- Provide an exercise directory.
- A feedback form for each participant.

Lessons Identified and Post Exercise Report

It is crucial that action points and feedback are recorded throughout the exercise and discussed at the end in a hot debrief. A hot debrief is simply a discussion on what went well, what didn't and an overall discussion on how the participants found the exercise while it's fresh in the minds of participants.

These form the lessons identified, owners need to be assigned to each lesson with a deadline applied and them being implemented ahead of the next exercise.

The post exercise report forms an important part of the process, try to keep it short and impactful covering the following areas:

- Overview of the exercise objectives and how they were met.
- Recap of the scenarios and injects with associated key observations.
- Lessons identified, with assigned owners and deadlines.
- Next steps, including an overview of a forward look for more exercises.

The exercise report should, where appropriate, be briefed to senior management so they are aware of the outcomes of the exercise.

It is recommended that following an initial exercise, a forward-looking programme is developed for one to two years to maintain momentum, helping to continually strengthen cyber resilience.

Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services at preferential rates via our network of Specialist Partners.

For more information please visit: Aviva Risk Management Solutions – Specialist Partners

Sources and Useful Links

- The NCSC has a wealth of freely available resources on TTX's, including their 'Exercise in a Box'. For more information please visit: Effective steps to cyber exercise creation - NCSC.GOV.UK

Note: Whilst UK standards and legislation are referenced in this document, other international standards and legislation should be referenced where applicable.

Additional Information

Relevant Aviva Loss Prevention Standards include:

- **Cyber Security: Top 12 Tips to Protect Against Cyber Attacks**
- **Cyber Security: Respond and Recover**
- **Cyber Security: The Internet of Things**
- **Ransomware – Cyber Loss Prevention Standard**
- **Cyber Essentials – Accreditation**
- **Cyber – Social Engineering – Fundamentals**

To find out more, please visit Aviva Risk Management Solutions **or speak to one of our advisors.**

Email us at riskadvice@aviva.com or call 0345 366 6666.*

*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

Please Note

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise, and Aviva recommend that you obtain specific advice relevant to the circumstances.

9th March 2026

Version 1.0

ARMSGI3962026