Cyber Incident Exercising Technical Standard

v1.4

September 2023

Contents

1. Definitions used in this document

Assured Service Provider

The organisation(s) assured under the CIE scheme to provide CIE services to client organisations.

Client Organisation

The organisation that is the recipient of the CIE service.

Cyber attack categorisation system

A categorisation system for cyber incident prioritisation, used primarily by the NCSC, UK law enforcement and government partners. For more information refer to the NCSC website.

Cyber Incident Response (CIR)

Cyber incident management assistance provided to client organisations during and immediately after a cyber incident.

JESIP

The Joint Doctrine: interoperability framework sets out a standard approach to multi-agency working.

NIST

The National Institute of Standards and Technology, an American government agency. NIST supplies industry, academia, government, and other users with over 1,300 Standard Reference Materials.

MITRE ATT&CK

MITRE ATT&CK is a knowledge base of adversary tactics and techniques used as a foundation for the development of specific threat models and methodologies in the private sector, government, and in the cyber security community.

Structured Threat Information eXpression (STIX)

STIX is a standardised language which has been developed by MITRE in order to represent structured information about cyber threats.

Threat Intelligence (TI)

Information about threats that have been aggregated, analysed and enriched to provide useful context for the decision-making process.

TTPs

Tactics, Techniques and Procedures of an attacker. Patterns of activity or methods associated with a specific threat actor or group of threat actors.

2. Scheme Introduction

2.1 Cyber Incident Exercising (CIE) provides a controlled, scenario-based opportunity for organisations to practise, evaluate and improve their cyber incident response plans in a safe environment. The Cyber Incident Exercising Scheme is for organisations providing tailored exercises for client organisations which already have cyber incident response plans in place.

2.2 In general, a client organisation will assess its own maturity and understanding of its cyber incident response plan and use that assessment to determine what it needs from a Cyber Incident Exercise service.

2.3 This document sets out the standard that Assured Service Providers must meet to be members of the NCSC's Assured CIE Scheme. The primary audience for this document is, therefore, potential and current Assured Service Providers. Client organisations in receipt of CIE services may also find this document useful to better understand what services an Assured Service Provider offers under the scheme and how they are assessed.

2.4 The NCSC evaluates cyber exercising services against the 'Design, Develop, Conduct and Evaluate' life cycle of exercise delivery, as defined by The National Institute of Standards and Technology's (NIST) SP 800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities (pdf). Although this standard refers to SP 800-84 and other industry recognised documentation, these are intended as points of reference only and are not specific requirements.

3. Service offerings

3.1 CIE Assured Service Providers must deliver both the CIE services. The CIE services are defined by:

- the Incident scale, and
- the Exercise method

Incident scale

3.2 Exercises that simulate cyber incidents which will have a significant impact on the single client organisation are classified as **organisationally significant** exercises. Typically, these incidents will have the potential for a significant operational, financial, or regulatory impact on the victim. This may include Category 3, 4 and 5 incidents on the UK's Cyber Attack categorisation system.

3.3 Currently, the assurance of exercising Category 2 and Category 1 cyber incidents is beyond the scope of this standard.

Exercise method

3.4 CIE Assured Service Providers will be assured for both the following delivery methods:

a. **Tabletop exercises** - discussion-based sessions where representatives from relevant teams meet to discuss their roles and responsibilities, expected activities and key decision points (in accordance with an incident response plan). Discussion is facilitated by the provider and driven by a prepared cyber incident scenario.
b. **Live play exercises** - team members execute their roles and responsibilities in response to controlled injects which represent a given cyber incident scenario. Different participants will typically receive different sets of injects. Activities and decisions happen in close to real-time although the incident pace and timeline is governed by an exercise controller. Live play exercises are best suited to mature organisations looking for in-depth validation of plans.

Assured Services

3.5 Client Organisations should therefore consider which service offering best reflects the service that they require:

a. *Organisationally significant tabletop exercises*
b. *Organisationally significant live play exercises*

3.6 The NCSC acknowledges that Assured Service Providers may offer additional exercising services which are not assured under the NCSC CIE Assured Scheme.

3.7 NCSC assured status is specific to relevant services. Any service provider who is NCSC assured to offer CIE services, cannot therefore claim NCSC assured status for any other services that it provides, without having first been assured against the associated NCSC technical standard(s) for it.

3.8 The NCSC will not typically participate in exercises delivered under the assurance scheme. If it is perceived that the NCSC should be involved and the client organisation has an existing relationship with the NCSC (for example government or Critical National Infrastructure organisations), the Assured Service Provider should advise the client organisation to contact the NCSC.

3.9 CIE Assured Service Providers must advise client organisations that:

a. they are members of an NCSC Assured Scheme

b. as part of their membership they are required to submit to the NCSC limited, non-attributable information about the exercise.

c. the NCSC will use this information for trend analysis purposes, to inform the NCSC's future advice and guidance to the UK, and to improve the NCSC's products and services.

3.10 The following areas are out of scope for this standard:

a. Activities that primarily evaluate a client organisation's information security defences (for example, penetration testing and vulnerability assessments). Client organisations requiring this service should consider the NCSC's CHECK service.
b. Activities which are predominantly designed to identify and develop skills of individuals within a client organisation (for example, technical training or media spokesperson assessments).
c. Assurance of a sector or client organisation's specific technical expertise (for example, specific technologies or regulatory frameworks). In such cases, client organisations should seek additional assurance from CIE providers that they possess the necessary required specialist knowledge or expertise.
d. Crisis response activities which focus on general business continuity plans rather than cyber incident response plans.
e. Exercising for Category 1 and Category 2 cyber incidents, as described in the UK's Cyber Attack categorisation system.

4. CIE competencies

4.1 All CIE Assured Service Providers must demonstrate the following competencies:

4.1.1 Knowledge of how the UK government manages cyber incidents. Where appropriate to the exercise participants and objectives, the application must include evidence of:

a. working with the NCSC during a cyber security incident
b. knowledge of the role of law enforcement and ActionFraud in cyber incidents
c. application of Joint Emergency Services Interoperability Programme (JESIP) principles, as necessary.
d. knowledge of the role of the Information Commissioner's Office in cyber incidents
e. knowledge of legal and regulatory thresholds and obligations related to a cyber incident.

4.1.2 Applicants must also show that they:

a. have knowledge of cyber threats - demonstrated through the development of credible, up to date, evidence-based scenarios. These scenarios must be aligned to the threats facing the client organisation.
b. are able to use Threat Intelligence products/services and real world Tactics, Techniques and Procedures (TTPs). This use must be consistent with accepted methodologies and terminologies (such as those contained within the MITRE ATT&CK framework and Structured Threat Information eXpression (STIX).
c. use Threat Intelligence to inform the development of exercise scenarios.
d. understand cyber incident response plans, incident management best practices and wider business continuity considerations. This may include the NCSC's Incident Management guidance and NIST's Computer Security Incident Handling Guide (pdf).

5. Communication Requirements

5.1 CIE Assured Service Providers must demonstrate how they communicate effectively across technical and managerial staff.

5.2 CIE Assured Service Providers reports must be written so that they can be widely understood across the Client Organisation. Where it is impossible to remove jargon, technical wording or company-specific words, clear explanation must be given.

6. Exercise delivery

6.1 Cyber Incident Exercising must be a defined service which is regularly delivered by the provider. CIE Assured Service Providers must:

a. have defined exercising personnel with relevant exercise delivery experience
b. employ a defined and repeatable delivery model for exercising
c. have knowledge of the NCSC's Exercise-in-a-Box product, cyber exercise creation guidance and Board Toolkit.

6.2 CIE Assured Service Providers must demonstrate experience delivering exercises to at least two of the three levels within client organisations (separately or as part of an integrated exercise):

a. Board level – should include, where appropriate: strategic business impact assessment and decision making; reporting to legal and regulatory bodies; and external facing communications.

b. Managerial level – should include, where appropriate: translation from operational detail to business risks; tactical decision making; and wider stakeholder engagement.

c. Operational level - should include, where appropriate: operational activities carried out as part of an incident response plan including initial triage and escalation.

6.3 Throughout exercise delivery, CIE Assured Service Providers must work collaboratively with relevant stakeholders. This will be dependent on the client organisation providing sufficient internal resources and suitable knowledge about the organisation.

Design phase

6.4 CIE Assured Service Providers must develop a scope of work with the client organisation which includes, but is not limited to:

a. timescales
b. context of the work
c. services and deliverables
d. assumptions and dependencies, including expected resource commitment from the client organisation
e. approach and work plan
f. roles and responsibilities
g. fees

6.5 An initial scope of work must be defined and approved before the work has begun. It should be reviewed and updated as necessary for the duration of the exercise development and delivery.

6.6 CIE Assured Service Providers must also:

a. Develop exercise objectives which are aligned to the client organisation's needs and capabilities, and which have been agreed by both parties.
b. Review appropriate existing client information such as threat intelligence, previous lessons identified, incident response plans and system design documents for use during exercise development. This will be dependent on the client and will typically require an appropriate non-disclosure agreement to be in place.
c. Ensure the exercise delivery reflects the maturity of the client organisation (for example, CIE Assured Service Providers should not deliver a complex cyber exercise to a client that does not have a cyber incident response plan in place).

d. Assemble an appropriate delivery team which includes appropriate client organisation representatives and subject matter experts. CIE Assured Service Providers should manage situations where members of the delivery team may also be participants in the exercise to avoid distorting the lessons identified.
e. Identify required exercise participants and stakeholders with appropriate seniority and subject matter expertise. Participants and stakeholders external to the client's organisation may be included. Understanding of required participation may evolve during development.

Development phase

6.7 CIE Assured Service Providers should work with the client organisation to iteratively develop an exercise which is aligned to the agreed objectives. The provider must demonstrate:

a. an understanding of the client organisation's incident response plan and operating environment
b. an understanding of the client organisation's risk appetite
c. the ability to create technically credible cyber scenarios that accurately reflect the type of incident that the client organisation might face.
d. the ability to create exercise injects which are appropriate to the exercise objectives and participants (for example, injects for a board level exercise will be different to those for an operationally focused exercise)
e. selection of appropriate, professional delivery and communications methods for the conduct of the exercise

6.8 Live play exercises will require additional development effort (compared to tabletop exercises) to reflect the increased complexity of exercise delivery.

Conduct phase

6.9 CIE Assured Service Providers must demonstrate:

a. an approach to final review and, where necessary, rehearsal, which is proportional to the complexity of the exercise
b. appropriate pre-exercise communication with participants
c. exercise delivery capabilities appropriate to the services being offered
d. exercises delivered in a safe and inclusive environment, and which provide a challenging, realistic but positive experience for all participants
e. exercise facilitation by professionals with appropriate experience and expertise (including effective communication skills)
f. effective observation and monitoring of exercises
g. adjustment of delivery in response to player performance and aligned to exercise objectives

6.10 Live play exercises will require additional capabilities and resources (compared to tabletop exercises) to create an appropriate, controlled environment and to capture lessons.

Evaluation phase

6.11 CIE Assured Service Providers must demonstrate:

a. appropriate exercise debriefing and feedback mechanisms
b. identification of clear, actionable lessons for the client organisation which are aligned to the exercise objectives and based on live observations and participant feedback
c. delivery of relevant and appropriate post-exercise reporting
d. the use of feedback from client organisations for continual service improvement