



National Cyber
Security Centre
a part of GCHQ

Assured CIR Scheme Buyer's Guide

v1.0 March 2025

Document history

Date	Version	Change history details	POC
	1.0	n/a	CIR Scheme Management Team

A review will take place October – December of each year for publication by the following February.

Document owner

National Cyber Security Centre (NCSC). All material is UK Crown Copyright ©.

Abbreviations and definitions

CIR Scheme Standard	Means the standards which must be met to be part of the CIR scheme. Referred to as the Standard.
Company/Companies	Means organisations which are assured against one of the NCSC CIR Standards
Customer	Means the organisation which contracts with the Company for CIR services.
We/Us/Our	Means the NCSC.
You/Your	Means the buyer of the CIR service.

Introduction

1. This document provides guidance and clarity around the NCSC's Assured Cyber Incident Response Scheme and is intended for buyers of Cyber Incident Response services. Please send any feedback or suggestions for additional content to ncscindustryassurance@ncsc.gov.uk.
2. The NCSC recommends that all organisations operating in the UK use an [NCSC-assured Cyber Incident Response provider](#) when dealing with cyber incidents. To help buyers navigate the market, we rigorously assess the technical and organisational competence of Cyber Incident Response companies. We assure companies at two levels: Enhanced Level and Standard Level. Note that while the NCSC owns the CIR Scheme as a whole, our Delivery Partners (CREST and IASME) deliver the Standard Level of the scheme on our behalf.

Cyber Incident Response – 'Enhanced' and 'Standard' Levels

3. Companies assured against the **Enhanced Level** are able to respond to the full spectrum of cyber incidents and have significant breadth and depth of experience and technical capability. We strongly recommend that you choose a Company assured against the Enhanced Level standard if your organisation meets one or more of the following criteria:
 - a. operates in a specifically regulated sector.
 - b. operates in more than one country.
 - c. is likely to be specifically targeted by nation state backed attackers and other sophisticated adversaries.
 - d. is part of the Critical National Infrastructure (CNI) – noting paragraphs 7 and 8.
 - e. is part of UK Central Government.
4. Companies assured against the **Standard Level** are able to respond to a sub-set of cyber incidents and have more limited breadth and depth of experience and

technical capability. Organisations which fall outside of the descriptions given in paragraph 3 should find that their needs can met by both Standard and Enhanced Level members of the CIR scheme. Such organisations may include:

- a. smaller and medium-sized businesses operating in sectors outside of the CNI.
- b. schools.
- c. charities.
- d. local authorities.
- e. organisations operating solely in the UK.

Summary of Assurance Criteria for each Level

5. All Companies (ie those at both Enhanced and Standard Levels of assurance) are able to:

- a. Respond to incidents resulting from cyber criminal attacks.
- b. Conduct basic malware analysis.
- c. Carry out log analysis on smaller estates.
- d. Inspect network traffic.
- e. Undertake digital forensics activities.

6. In addition, Companies assured against the Enhanced Level standard of the scheme are able to:

- a. Respond to Advanced Persistent Threat attacks (which we define as 'A sophisticated, ongoing cyber attack which occurs when an intruder covertly infiltrates a network and remains hidden with the intention of stealing confidential information over an extended period of time.') Such attacks are typically linked to nation states or their proxies.
- b. Respond to incidents involving organisations in specifically regulated sectors.
- c. Respond to incidents affecting multinational companies.

- d. Respond to incidents involving Law Enforcement and/or external legal counsel.
 - e. Produce cyber threat intelligence and use it during incidents.
 - f. Conduct advanced malware analysis.
 - g. Deploy end point detection.
 - h. Carry out log analysis on larger estates.
7. For more information on the two levels, please read the associated standards available from the NCSC website:
- a. Enhanced Level: [Cyber Incident Response \(CIR\) - Enhanced Level - Standard v1.0](#)
 - b. Standard Level: [Cyber Incident Response \(CIR\) Technical Standard \(Standard Level\) v1.5.1.](#)

Bespoke and Specialist Technologies

8. Buyers in CNI or specifically regulated sectors may need to find CIR - Enhanced Level providers with knowledge and experience of specialist or bespoke technologies, such as Operational Technology and Industrial Control Systems.
9. We have not assessed any Company's ability to respond to incidents involving such technologies. Some Companies may have relevant, specific knowledge and experience to meet your requirements, but you should put in place additional steps to verify any claims made by prospective suppliers. You should also consider whether you need additional support from a third party such as the vendor or specialist provider of your technologies.

What does NCSC-Assured mean for CIR Companies?

10. When we assure a Company, we have confidence that it meets our scheme standards. Broadly speaking, these standards cover:

- a. The Company's overall ability to meet the NCSC's defined levels of capability.
- b. At the Enhanced Level, the technical competence of the CIR Head Consultant. At the Standard Level, the technical competence of the Team Leader.
- c. The Company's ongoing commitment to service improvement and continuous development of its specialist, dedicated staff.
- d. Basic due diligence around the Company's financial and security status. This means that:
 - i. for **Standard Level** Companies, our Delivery Partners undertake due diligence on applications to ensure there is no reputational risk in the association of the NCSC with that application and that they are a reputable Company of good standing.
 - ii. for **Enhanced Level** Companies, we check:
 - 1. whether the Company or its officers have been convicted of certain offences which might constitute mandatory grounds for exclusion from government contracts (such as convictions for fraud or tax evasion).
 - 2. the "risk indicator" for the Company's Dun and Bradstreet Rating (D&B Rating, as explained here: <https://www.dnb.co.uk/about-us/our-analytics/predictors-scores-ratings/scores-ratings.html>). However, depending on a Company's circumstances and any possible mitigations, a higher risk indicator (3 or 4, or where there is insufficient information to assign an indicator) will not necessarily exclude it from the Scheme. This is only a basic creditworthiness check made when a Company joins the Scheme and potentially at periodic points thereafter, but in each case, it only gives a snapshot of the Company's financial risk at the time at which it is performed. It remains

your responsibility to perform all financial due diligence that is necessary and appropriate to your relationship with the Company.

- iii. For Enhanced Level Companies only, we check that at least one senior member of the CIR team holds a DV clearance. However, we do not sponsor all the clearances. If you need a supplier to hold clearances, it is your responsibility to assure yourself that they are valid and acceptable to your organisation. You may do this either by checking with the United Kingdom Security Vetting (UKSV) team or, where GCHQ sponsors the clearance, by emailing ncscindustryassurance@ncsc.gov.uk. Please allow as much time as possible to conduct these checks, owing to resource constraints in both teams.
- e. In addition to these clearance checks, the NCSC reserves the right to carry out background security checks (which might include checking for potential reputational impact on the NCSC) on a Company (and, in some cases, those checks may result in exclusion from the Scheme). However, any additional checks carried out are likely to be context-specific and will only assess risk at the time at which they are made (which, as with ii. above, is the point when the Company joins the Scheme and potentially at periodic points thereafter). Therefore, you should not rely on a Company's status as a member of the Cyber Incident Response Scheme as being a guarantee on the NCSC's part that your use of that Company will be risk-free from a security perspective. If you have any particular security concerns, please contact the NCSC for help at ncscindustryassurance@ncsc.gov.uk;
- f. That all CIR - Enhanced Level Companies have a Cyber Essentials Plus certificate as a minimum, and that all CIR – Standard Level Companies have a Cyber Essentials certificate as a minimum.

11. We assess all Companies on joining the scheme and review their membership at least every two years thereafter to ensure they continue to meet our standards.
12. We meet regularly with the Cyber Incident Response community for knowledge sharing and feedback purposes.
13. The standards and associated documents for both levels of the CIR scheme are all available on the NCSC's website (available [here](#)). We strongly encourage you to familiarise yourself with the contents so that you know what to expect from a member of the scheme.

Feedback

14. To maintain high standards, we value feedback on scheme members' work. Therefore, please respond to any request to provide feedback, whether that request is from the Company itself, from the NCSC, or (for Standard Level members) from our Delivery Partners (CREST and IASME). You are welcome, at any time, to provide feedback independently by emailing ncscindustryassurance@ncsc.gov.uk.