National Cyber Security Centre
a part of GCHQ

NCSC Cyber Incident Response Level 1

Application Form

V1.1 31/03/2022

CONTENTS

SECTION 1: Overview

A. Application Process

All sections of the application form must be completed for the application to be processed. The application has 3 stages as set out below.

You must pass each stage of the application process to progress to the next. Only 2 application attempts will be accepted within a 12-month period.

- **Stage 1: Commercial Questionnaire**
  This questionnaire is required by our Commercial Contracts team and is designed to gauge your commercial viability to contract with the National Cyber Security Centre (NCSC). Every company wishing to join our schemes must complete this questionnaire. If you have recently applied to join one of our other schemes in the last 6 months, please let us know the scheme name and date of application.

  The questionnaire will be sent as a separate document for you to complete and submit alongside this Application Form. Please return the document, saved with the following naming convention:
  COMPANY NAME_COMMQUEST_DATE

- **Stage 2: Application Assessment: (2 parts)**

  Part 1 - Technical Requirements:
  Evidence of methodology and case studies must be provided to demonstrate the competencies and delivery capabilities outlined in the NCSC Cyber Incident Response Technical Standard (Level 1): Cyber Incident Response Technical Standard (Level 1)

  The Standard is also available to download from this page:
  https://www.ncsc.gov.uk/information/cir-cyber-incident-response

  The assessment of the case studies listed in the Application Form (and submitted as attachments) against your methodology, will be reviewed in accordance with the Technical Standard. The assessment will be conducted by representatives of the NCSC Incident Management Team.

  Please refer to the Technical Standard and Application Form Guidance notes (which will be sent to you should you wish to apply for membership) to help shape your case studies.

Part 2 - Business Standard Requirements:

You will be asked to demonstrate compliance with business expectations of the NCSC Cyber Incident Response Scheme. A list of these requirements is in Schedule 5 of the contract and for convenience, a check list is at Annex B in the application form. Please provide details in Section 7 as requested or attach as a separate document where relevant.

- **Stage 3: Head Consultant Interview**
  Subject to passing the Commercial requirements and Application assessment (both business and technical); the proposed CIR Head Consultant (see para 57-61 of the Technical Standard) will be invited to interview with representatives from the NCSC Incident Management Team and the Commercial Assurance Services Team. Questions will be based on the case studies and the Incident Response Methodology you provide in the application form.

B. Completing and submitting your application

All applications will be handled as Official Sensitive. Once complete, please save this application form as a .PDF file, with the following naming convention:
COMPANY NAME_CIR L1_DATE

Please refer to the checklist of documents required alongside this application form in Annexe B. Submitting all required documents with the requested formatted titles will ensure all related documentation can be cross-referenced with your application form.

SECTION 2: Company Name, Point of Contact and Staff Details

Please provide the full name of your company (as registered with Companies House):

Name of Company:	
Address:	

Please nominate the primary person in your company to act as a point of contact for this application (this person should be someone we can contact about application details or discuss progress):

Name:	
Role Title:	
Telephone Number:	
Email address:	

CIR staff and role titles (Please note: Clearances are not required but may be useful).

Please provide details of your Head Consultant (HC): (this person should be someone who meets the requirements in the CIR Technical Standard and is responsible for the technical delivery of the service)

Name:	
Role Title:	
Telephone Number:	
Email address:	
Clearance status if held (DV or SC):	

Please provide details of your Deputy HC (optional):

Name:	
Role Title:	
Telephone Number:	
Email address:	
Clearance status if held (DV or SC):	

Please provide details of a person who will act as a Service Owner: (this person is the primary point of contact for the CIR scheme and is responsible for providing reporting requirements and changes. This may be the same person as the Head Consultant)

Name:	
Role Title:	
Telephone Number:	
Email address:	
Clearance status if held (DV or SC):	

Please list other CIR staff and role titles:

Name	Email address	Role Title	Clearance Status if held (DV or SC)

SECTION 3: Clearances

For each member of staff listed (including the Head Consultant), who holds a clearance (DV or SC), please enter the details for each clearance into the boxes provided in Annexe A.

Please Note: At least one senior member of staff within the Cyber Incident Response Provider (such as the Head Consultant) must hold a Developed Vetting (DV) clearance. The NCSC will sponsor up to two DVs per Cyber Incident Response Provider to give some contingency in case one member of staff leaves. The NCSC will accept a company without a DV while the DV request is being processed if the company meet all other onboarding requirements and the technical assessment.

SECTION 4: Requirement for Technical CVs

The NCSC require Technical CVs for all staff including the proposed Head Consultant and Deputy Head Consultant. Please attach separately to your application submission for each member of staff.

The CV should demonstrate the competencies and delivery capabilities outlined in the Technical Standard. For Head Consultant, the CV should reference relevant certifications for foundational cyber security knowledge as listed in Paras 57- 61 of the Technical Standard.

Head Consultant qualifications held as listed in Paras 57-61 of the Technical Standard (valid in date)	
Qualification Name	**Expiry date**

CVs for all CIR staff members will be reviewed at point of application and submission of scheme reports. Updated CVs will also be required within 14 working days on a change of the Head Consultant or Deputy HC.

SECTION 5: Methodology

Please provide evidence of your organisation's CIR methodology and processes.

Once complete, please save as a separate document using the following naming convention: COMPANY NAME_CIR L1_METHODOLOGY_DATE (Using this file naming format will enable documentation to be cross-referenced to this application)

The methodology document must be no longer than 10 A4 pages.

Consult the Application Form Guidance Notes for further details of the information expected to be evidenced within your methodology and process document.

The requirement to submit methodology and process documentation is for the initial application to join the scheme, then following that will be requested at 4 yearly contract renewal periods.

SECTION 6: Case Studies

Please provide 4 case studies of work conducted in the last 24 months.

Please ensure you list the following information at the top of each case study:

- Target Organisation (or relevant Target Organisation set if case study needs to be anonymised)
- Customer Sector
- Start and end date of work
- Case Study (number or name)

Save each case study separately with the following naming convention: COMPANY NAME_CIR L1_CASE STUDY NAME_DATE

Each case study must be no longer than 2 sides of A4 pages, utilising the template provided with the application form.

Please read the Application Form Guidance Notes for further details on the level of detail required to be demonstrated across the range of case studies submitted.

The requirement to provide case studies is for the initial application to join the scheme, then following that will be requested at 2 yearly intervals.

To assist in the review of the 4 case studies, please confirm below the technical capabilities listed from the Technical Standard that you used and indicate below in which case study the capabilities are reflected in:

Technical Capability	**Used** *(Y/N)*	**Represented in which case study** *(Please enter name of case study which provides main example use of each capability listed)*
Endpoint Detection and Response		
Log collection and analysis		
Network traffic inspection		
Digital investigation/analysis		
Malware reverse engineering		
Use of Threat Intelligence		

SECTION 7: Business Requirements

There are core business working practices and expectations that the NCSC require a CIR Provider to have in place and you will be supplied with a blank contract as reference for these upon application. Please indicate that you have these in place where requested below or supply any evidence required in this section of the application form. Additionally, updated information will be requested as part of the annual scheme report or reviewed at audit.

Business Requirements

Quality Management and Service Improvement

We expect all CIR Providers to follow good Quality Management processes that demonstrate they offer an ongoing high-quality service and have processes in place which help to continually review, maintain and improve delivery of the service they offer.

Training

To ensure that the required skills and experience remain current to deliver the service in accordance with the technical standard, the company should have a training and development plan in place.

Customer feedback

CIR Providers shall endeavour to procure feedback from the customer organisations to whom a company has provided Assured Services. Where feedback has been received in relation to the performance of the CIR company, this should be shared with the NCSC, in an anonymised form if required.

Complaints process

The CIR Provider shall notify the NCSC as soon as reasonably practical if they receive a complaint which is in connection with the delivery of services under the scheme.

Business Continuity Plan

CIR Providers will have a defined Business Continuity Plan that will assist them in continuing to offer services offered in the event of an accident, disaster, or emergency.

Please indicate that you have plans or processes in place for the following business requirements:

Document/Processes	Contract Clause(s)	Yes/No
Quality Management	Para 4.3	
Continuous Service Improvement	Para 4.3	
Training and Development	Para 23.1 (and Para 56.6 CIR Standard)	
Customer feedback	Para 10.6	
Complaints process	Para 5.8 and Para 26.2.6	
Business Continuity Plan	Para 8.5	

Cyber Essentials

CIR Providers are required to be certified under the NCSC's Cyber Essentials scheme which covers the service to be provided and its supporting infrastructure. Please provide details of your CE or CE+ certification including Certificate number and award date.

Please provide details of your Cyber Essentials certification below. Certificates must be in date and if due to expire please specify when you applied for recertification.

Cyber Essentials / Cyber Essentials certification number:	
Date certificate issued:	
Recertification date if applicable:	

Code of Conduct Declaration

All personnel involved in delivery of the service must have seen and agreed to abide by the spirit of the UK Cyber Security Council's Code of Conduct.

By signing below, the Head Consultant declares that all staff involved in delivery of CIR services have read and agree to adhere to spirit of the UK Cyber Security Council's Code of Conduct.

Name:	**Date:**

SECTION 8: Membership Obligations and Declaration

Membership Obligations

If your application to become a CIR Level 1 Provider is successful, you will be required to submit regular updates of information you have supplied with this application form. Information is required in Schedule 5 of the contract and is summarised below:

The scheme report should be sent to the CIR mailbox at intervals indicated and shall include but may not be limited to the following:

Required Information	**Frequency**
Varied timescales:	
Notification of change to Head Consultant or Deputy HC and other staff changes	Within 14 working days
Case Studies	4 case studies every 2 years
Methodology	6 months before contract renewal (4 yearly)
Annually:	
Complaints and legal proceedings	Annually or at any escalation point (advanced notice required of impending comms/press)
Updated technical CVs	Annually (or within 14 working days upon change of Head Consultant or deputy)
Head Consultant qualifications	Annually
Customer feedback	Annually
Record of customer incident response engagements	Annually (number, sector and type of incident) UK customer engagements only
Updated clearance details	Annually
Revalidated CE certificates	Annually

Explanatory notes:

Notification of staff changes

To ensure we have correct point of contact details for management of the scheme, CIR Providers must notify the CIR mailbox and the NCSC Commercial team when any changes are made to CIR team personnel, specifically the Head Consultant and the scheme Point of Contact. Changes must be communicated to the NCSC within no less than 14 working days of the impending changes.

Case Studies

New case studies must be submitted to the CIR mailbox every 2 years. Case studies must document evidence in accordance with the CIR Technical Standard (Level 1) Annexe B, to demonstrate the competencies and delivery capabilities outlined in the standard.

Methodology

Updated Methodology must be submitted to the CIR mailbox at the point contract renewal. Methodologies must be evidenced in accordance with the CIR Technical Standard (Level 1) Section 3.22 and demonstrate a repeatable methodology for capturing findings and recording decisions in accordance with Section 6.39.

Complaints and Legal proceedings

The NCSC would like to be informed of any complaints relating to the IR service being delivered if they risk damaging the reputation of the NCSC or the CIR Scheme. Any normal supplier-client conflicts should be dealt with through the relevant contract clauses the two parties have.

Updated technical CVs

Required annually for all IR staff. CVs should demonstrate the competencies and delivery capabilities outlined in the Technical Standard. For Head Consultant, the CV should reference relevant in date certifications for foundational cyber security knowledge as listed in Paras 57- 61 of the CIR Technical Standard (Level 1).

Head Consultant qualifications

Copy of valid in-date qualifications or certificates in accordance with the criteria in the Technical Standard should be sent to the CIR inbox.

Customer feedback

The CIR Provider shall use its reasonable endeavours to procure customer feedback from clients in relation to the incident response service received. The Provider should be prepared to share with the NCSC where practicable.

Record of customer incident response engagements
Anonymised information is requested annually for the number of IR engagements and is also to be made viewable by related sector and type of incident. This data will contribute to the NCSC understanding of how cyber resilience is improving within the UK.

Updated clearance details
The CIR Provider point of contact is to submit updated clearance details for members of staff when clearances for personnel previously notified to the NCSC have expired or are due to expire within 6 months.

Revalidated Cyber Essentials certificates
Certification number and award date are required of a current Cyber Essentials certification. If the certificate is due to expire within 3 months, you must provide evidence to show that you have applied for recertification.

Declaration

If the NCSC becomes aware that requirements are not met and/or you have not provided notification, this may result in a requirement for an audit which may lead to suspension or termination of the contract.

By signing below, you declare that the information provided in the application form and in Annexe A is true and correct to the best of your knowledge and belief and that you have read and accept the terms of the example contract provided with the application.

Name:	**Date:**

Annexe A: Clearance details

Provide details within Annexe A of any staff listed within Section 2 (including the Head Consultant) who holds a clearance.

Please list the Clearance Authority (DV/SC Sponsor/Holding Authority), Expiry Date and Date of Birth so that we can confirm and validate the clearances:

Staff Name	
DV/SC Sponsor/Holding Authority	
DV/SC Expiry Date	
Date of Birth	

Staff Name	
DV/SC Sponsor/Holding Authority	
DV/SC Expiry Date	
Date of Birth	

Staff Name	
DV/SC Sponsor/Holding Authority	
DV/SC Expiry Date	
Date of Birth	

Staff Name	
DV/SC Sponsor/Holding Authority	
DV/SC Expiry Date	
Date of Birth	

Staff Name	
DV/SC Sponsor/Holding Authority	
DV/SC Expiry Date	
Date of Birth	

Annexe B: Checklist of documents required

Please ensure you have completed all sections of the application form, including the four declarations. Incomplete or missing items may result in application delay or return. Please mark the tick boxes to indicate inclusion of the following attachments with this completed application form:

Documents added as separate attachments:

☐ Completed Commercial questionnaire (fill in as a separate attachment)

☐ Technical Methodology and processes (not to exceed more than 10 A4 pages)

☐ 4 Case studies (up to 2 sides of A4 pages each)

☐ Technical CVs for all members of staff, including HC and Deputy HC (attach each separately)

☐ Cyber Essentials or Cyber Essentials + details.

☐ Valid in date qualifications for Head Consultants