Cloud Security Assessment Review (CSAR) – Baseline Proposal

CLIENT

November 2024

Version 2.1

Author: NCC Group cloud security team

Document Control

Proprietary Information

Document Version Control

Data Classification	
Client Name	CLIENT NAME
Assignment Reference	
Document Title	Cloud Security Assessment Review (CSAR) – Proposal
Author	

Document History

Issue Number	Issue Date	Issued By	Change Description
2.0	09112024	name	Initial Draft
2.1	12/11/2024	name	redraft
2.2	12/11/2024	name	QA
2.3			Final

Contents

1 Background 4
2 Scope (SOW) 5
2.1 Cyber Security Cloud Governance Assessment. 5
2.2 Cyber Security Technical Cloud Configuration Assessment 5
2.3 Organisational Design and Operating Model Assessment 7
2.4 Out of Scope 7
3 Investment Schedule 8
3.1 Pricing Notes: 8
4 Description of Services 9
4.1 Cyber Security Cloud Governance Assessment. 9
4.2 Cyber Security Technical Cloud Configuration Review 10
4.3 Organisational Design and Operating Model Assessment 11
5 Client Engagement 11
5.1 Debriefing and Next Steps 12
6 Description of Client Responsibilities 14
6.1 Timely review of draft deliverables 14
7 Description of Project Deliverables 15
8 About NCC Group 17

1 Background

This proposal follows a series of discussions with CLIENT Limited (CLIENT) and consultants from NCC Group. The meetings addressed the CLIENT requirement for security consultancy services aimed at assessing the organisation's corporate and cloud services environments to assure and enhance its cloud security posture. CLIENT wants a focused security review of its three major cloud infrastructure environments from a configuration perspective, the outcome of which is to be mapped against a known and agreed NIST 2.0 (Cyber Security Framework).

NCC Group is to provide a report outlining all identified vulnerabilities and a brief road map of priorities to be addressed by CLIENT's security teams. Additionally, to understand, at the organisational level, the current processes managing all three cloud providers, NCC Group is proposing a high-level Target Operating Model exercise as part of the overall assessment for completeness.

For CLIENT, the security and integrity of data and information systems is vital, a breach could have a major ramification on its core service delivery to clients and corporate operations. CLIENT has approached NCC Group to provide an independent security assessment in support of reducing exposure to vulnerabilities and risks and providing recommendations that CLIENT can consider with a view to take action to address these in a timely fashion.

Our Cloud Security Consultants will be tasked with conducting a Governance and Technical Configuration review of the cloud environments and strategy and to include the existing documentation, architecture, licencing, resource skillsets and understanding and training requirement. It has been agreed at this stage that a detailed technical assessment is not required.

2 Scope (SOW)

The services described in this proposal will be delivered within the scope of the CLIENT response to the NCC Group Cloud Scoping Meeting to a baseline level of detail. The level of detail is a time bound exercise that covers all the control areas of interest to a level of detail and evidencing allowed within the allotted time bound period of engagement for each area of the scope.

The engagement scope is understood to be as outlined below. The deliverables in this scope of work are subject to the existing MSA Framework between CLIENT and NCC Group Security Services Limited XXXXXX

2.1 Cyber Security Cloud Governance Assessment.

A holistic assessment of the CLIENT Cyber Security Programme reported against the NIST CSF (Cyber Security Framework) v2.0.

- Output - A NIST CSF score for the CLIENT Production estate in both policy and practice with explanation of why they have been scored at a particular level. Scores will be mapped to the latest version of NIST CSF (v2.0).
- A prioritised set of recommendations with details of remediation measures that could be undertaken to address any areas of concern.

2.2 Cyber Security Technical Cloud Configuration Assessment

The Cloud Governance Assessment is augmented with a Cloud Configuration Assessment (CCA) which is a technical review of CLIENT’s IaaS and PaaS environments. This includes the assessment of vulnerabilities across the areas of cloud compute, tenancies and deployed configurations and of network segregation and roles, users and groups. We will utilise any pre-existing platform security reviews already undertaken by cloud vendors.

It assesses customer security capabilities and operational practices and processes which includes the areas of:

- High-Level Identity and Access Control Reviews
- An architecture and Configuration Review
- Logging, Monitoring, Auditing and Reporting
- And Data Protection areas including areas such as Access Controls, Data Classification and Encryption

The CCA is performed in combination with the governance elements assessed in section 2.1 above.

The cloud configuration reviews will **exclude** the following specialist services. If these services are found during testing, we will be able to scope additional assessments to cover them.

- **Azure:** Functions, SQL, Key Vault, Automation Account, Analytics, Event Hub.
- **AWS:** Lambda, RDS, KMS, Secret Manager, SQS, SNS, SES.
- **GCP:** Cloud Run, SQL/RDS, Key Management, Secret Manager.

2.3 Organisational Design and Operating Model Assessment

An assessment of the organisational design / operational model and its ability to execute against the current roadmap.

- A review of roles and responsibilities across the team.
- A review of the skillsets maintained on the team to execute against the roles and responsibilities.
- A review of the capacity of the team
- A ‘people’ benchmark to ensure CLIENT is investing and compensating correctly against industry.

2.4 Out of Scope

- Software Code and application functionality is out of scope.
- Any productivity suites such as Microsoft 365 or Google G Suite.
- Third party tooling or Software as a Service (SaaS) solutions.

3 Investment Schedule

Based on our experience in successfully completing similar projects we estimate this project will require a total of two months elapsed time to complete and be conducted by a blend of consultants to cover the agreed scope of technologies. The project will be scheduled to start on the earliest mutually agreeable date, not sooner than two (2) weeks after the execution of all required legal documents and agreements.

The pricing schedule is summarized below.

Details	Total rice [GBP]	Total rice [GBP]
Cyber Security Cloud Governance Assessment (20 days)	NIST-CSF v2.0 Assessment and reporting of the CLIENT cloud environments.	XXXX
Cloud Configuration Assessment (30 days)	Technical Configuration review of the CLIENT Cloud Environments and selective operational workloads.	XXXX
Organisational Design and Operating Model Assessment (12 days (incl. PM)	Target Operating Model review and recommendations	XXX
TOTAL		**XXX**

- All prices are for guidance purposes, and illustrative based on scoping data available. Final prices will be issued subject to review and final approvals.
    - Pricing excludes VAT and any Travel and expenses per the governing CLIENT MSA (available upon request reference number XXXXXX).
- The above are Fixed Price based on a time limited approach: the number of days effort NCC will provide its best efforts.
- NCC Group propose to take a time limited approach where we will try to achieve the best coverage possible in the assigned time, but this coverage may not be comprehensive. If additional assessment is deemed to be required, our consultants will recommend the necessary additional days of testing (at an additional cost).

3.1 Pricing Notes:

This schedule is dependent upon the timely availability of Client resources necessary to complete each task described in this Proposal and the schedule.

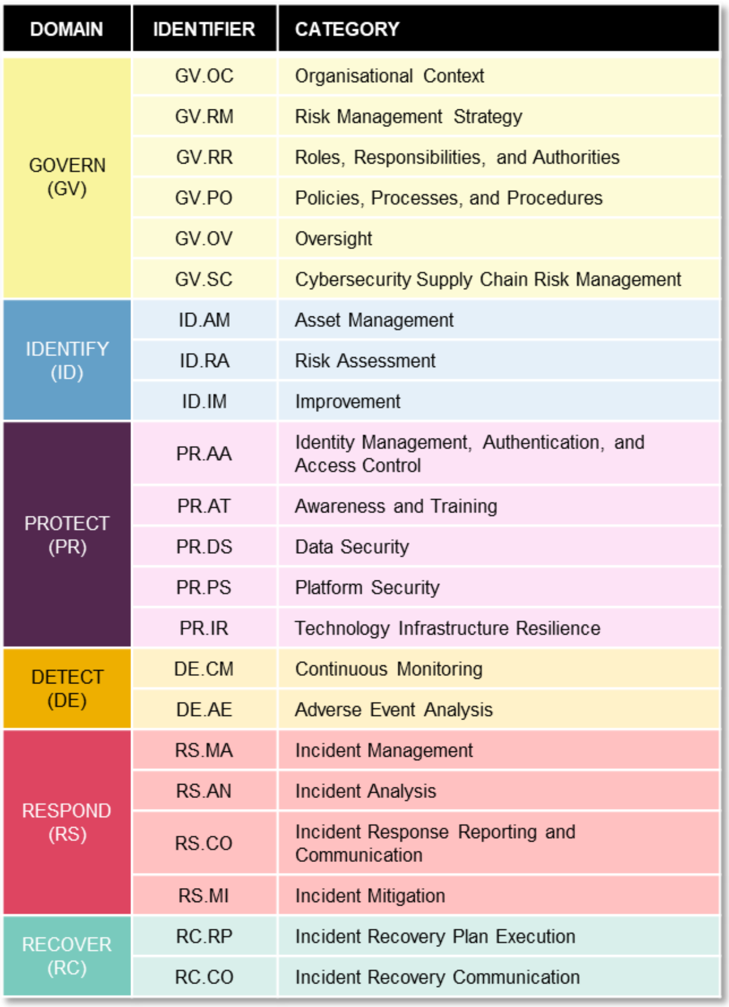
NCC group will invoice CLIENT in full upon the completion of the project /assessment and in any case no later than the date of the Final report provided to CLIENT.

4 Description of Services

NCC Group will perform a Cloud Security Assessment Review (CSAR) to establish a baseline understanding of cloud security across the core CLIENT cloud corporate and sample Client service hosting environment.

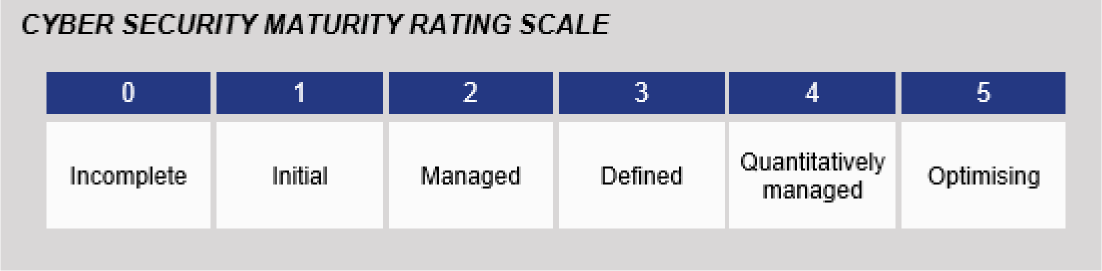
4.1 Cyber Security Cloud Governance Assessment.

NCC Group will conduct the assessment using the NIST CSF (v2.0) comprising six high-level domains – Govern, Identify, Protect, Detect, Respond and Recover – to define the end-to-end cyber security and resilience lifecycle state of the organisation. The NIST CSF comprises of control categories which specify activities and objectives that should be considered for implementation to help treat information security risks.



DOMAIN	IDENTIFIER	CATEGORY
GOVERN (GV)	GV.OC	Organisational Context
	GV.RM	Risk Management Strategy
	GV.RR	Roles, Responsibilities, and Authorities
	GV.PO	Policies, Processes, and Procedures
	GV.OV	Oversight
	GV.SC	Cybersecurity Supply Chain Risk Management
IDENTIFY (ID)	ID.AM	Asset Management
	ID.RA	Risk Assessment
	ID.IM	Improvement
PROTECT (PR)	PR.AA	Identity Management, Authentication, and Access Control
	PR.AT	Awareness and Training
	PR.DS	Data Security
	PR.PS	Platform Security
	PR.IR	Technology Infrastructure Resilience
DETECT (DE)	DE.CM	Continuous Monitoring
	DE.AE	Adverse Event Analysis
RESPOND (RS)	RS.MA	Incident Management
	RS.AN	Incident Analysis
	RS.CO	Incident Response Reporting and Communication
	RS.MI	Incident Mitigation
RECOVER (RC)	RC.RP	Incident Recovery Plan Execution
	RC.CO	Incident Recovery Communication

The review will use following scale, based on the Capability Maturity Model Integration (CMMI), to rate control maturity:



CYBER SECURITY MATURITY RATING SCALE

0	1	2	3	4	5
Incomplete	Initial	Managed	Defined	Quantitatively managed	Optimising

The assessment will be interview driven using a workshop structured approach, NCC Group would expect the following stakeholders to participate and provide relevant information and evidence to support the assessment. Some of these roles may be covered by a single individual. These will include but not limited to:

- IT Operations – to understand how IT is managed and run within the organisation.
- Infrastructure/IT Management – to gain an overview of systems and of the main ways in which data is secured, such as use of encryption and access control.
- Information Security/CISO/InfoSec Manager – to gain an understanding of the existing information security management processes and procedures in place.
- Network Support/Management – to understand the network topology, segregation and external links into the corporate IT network.
- DevOps team(s) – to understand how applications are developed, tested, launched and maintained.
- Operational staff – to understand business level processes that could impact the security/privacy of the in-scope systems and data assets
- Network/Infrastructure/Security Architects – to understand how the network/applications/security requirements are defined and implemented.
- Legal, Risk/Audit, HR, Sales and Marketing – to understand the processing of personal data relative to GDPR.

Supporting vendors, consultants and representative from the Project Management Office may also be included as appropriate and time permitting.

At the end of the interview sessions the NCC Group consultant(s) will present back their initial findings and key stakeholders will have an opportunity to qualify and clarify findings.

4.2 Cyber Security Technical Cloud Configuration Review

NCC Group will perform a thorough Cloud Configuration Assessment, in addition to reviewing specific workloads (maximum of four representative workloads per platform) as a sample set of those currently in operational use, we will assess the following applicable to each environment:

- Access keys and root account status
- Segregation of resources
- Network Security Groups and ACLs
- Region in which data is held
- Identity and Access Management configurations & password policy

- User groups and privileges
- Encryption of snapshots and volumes

The Cloud Configuration Assessment will give a broad overview of the security of your cloud computing estate.

Due to the large number of cloud resources in scope NCC Group proposes a sampled configuration review which will provide a solid representation of CLIENT's wider estate. This will guide future assessments and the CSAR process.

4.3 Organisational Design and Operating Model Assessment

Assessing an organizational design and operating model's ability to execute against the current roadmap is essential for success. NCC Group's process for conducting such an assessment will include:

- Review Roles and Responsibilities - Analysing roles and responsibilities across the team. Ensure that each role is well-defined, aligns with strategic objectives and contributes directly to the roadmap. Identify any overlaps or gaps in responsibilities and make necessary adjustments to streamline workflows.
- Skillset Evaluation - Determine whether the security team members possess the required competencies to fulfill their roles effectively. Identify areas where skills may be lacking and develop plans for upskilling, training, or hiring to bridge these gaps.
- Capacity Assessment - Evaluate the capacity to deliver on the current roadmap. Considering factors such as workload, resource availability, and constraints. Adjust team sizes, workload distribution, or resource allocation as needed to ensure sufficient capacity for successful execution.
- People Benchmarking - Comparing the organization's compensation, benefits, and investment in personnel with industry benchmarks. Ensuring that people-related investments are competitive, helping attract and retain top talent. Adjust compensation and benefits packages as necessary to align with industry standards.

Based on the findings from the above steps, NCC Group provide recommendations to include role adjustments, skill development, capacity enhancements, and compensation changes. Assign responsibilities and set timelines for implementation.

5 Client Engagement

The assignment begins with a Project Initiation Meeting conducted by our lead consultant and CLIENT stakeholders. The purpose of this meeting is to:

- Confirm the scope of the project and agree appropriate terms of reference, objectives, and deliverables.
- Agree reporting lines.
- Agree appropriate timescales for delivery of the work, including document reviews, workshops, midpoint project reviews and evidence collection.
- Confirm the staff and other contacts involved.
- Identify and mitigate sensitive issues that may impact the review.

We will produce a Project Initiation Document for agreement by both parties, which will act as the key reference point for completing the project. This document will incorporate the above points and a high-level agenda / itinerary.

When undertaking engagements of this type, it is essential that we have a clear understanding of your risk posture and the key issues that your organization faces or is likely to face. We will then be in a better position to make specific recommendations relating to the ongoing security activities that you should perform. During this phase we will:

- Discuss your business objectives and operating processes to gain an understanding of:
- Review the business technology and cloud strategy and goals as well as expectations for future cyber security maturity;
- Technology requirements that support the strategy;
- Current and future security requirements.
- Identify your risk management approach;
- Define the scope of the project;
- Undertake a preliminary identification of the key information assets, systems and services owned, managed and/or utilized.

5.1 Debriefing and Next Steps

In collaboration with your project sponsor our consultancy team will provide a high-level roadmap for cyber security improvement. The roadmap will give you a tangible view of where your strengths and weaknesses are, and prioritization of the recommendations to address them and achieve an agreed target maturity.

On the basis of the review and production of the recommendation’s roadmap, our clients have found that this often aids them in developing an information security Programme with clearly designed deliverables. Our consultants have been instrumental in providing reasoned advice and support in delivery of technical solutions, policies and procedures, and cyber and information risk management strategies.

Additionally, our clients have requested that we review their progress and conduct further cyber security reviews to test their security controls and provide their latest maturity and improvement to clearly demonstrate the investment made and the reduction of risk.

Following delivery of the report, our consultant will conduct a formal presentation to you. This can be delivered in a number of formats to be agreed during the project, however, this typically includes:

- Executive briefing to the board and project sponsor;
- Presentation to the technical teams and discussion of recommendations and proposed high-level roadmap.

6 Description of Client Responsibilities

NCC Group has used this information in establishing the Project Schedule and Fees for this project. In the event an item identified below does not occur in the manner or time frame shown, such circumstance shall constitute a change that may require an adjustment to the Schedule and/or Fee. In connection with the services performed by NCC Group under this proposal, the Client will provide NCC Group with:

- Timely access to key personnel, business operational and technical information resources required for the delivery of the services identified in this proposal and not limited to individual business unit managers, and IT security operations staff.
- A client identified key stakeholder and or project manager or other point of contact, to ensure that the relevant IT operations staff and business unit managers are briefed and aware of NCC Group's engagement, testing and interview tasks being undertaken.
- Notification of any compliance or regulatory efforts that the results of NCC Group's assessment may be used to support and/or that will require additional deliverables (i.e., PCI-DSS etc.)
- Permission to perform testing and interview any third-party vendors that either own applications, services or infrastructure that is in the scope of the engagement.

6.1 Timely review of draft deliverables

Client will provide review and feedback on deliverables no later than five (5) business days after submission.

NCC Group will revise and resubmit the deliverable within five (5) business days after the receipt of the reviewers' comments.

The number of review/revision cycles will not exceed three (2) for any individual deliverable.

Deliverables will be deemed to be in DRAFT unless specifically stated as FINAL. Until such time, DRAFT documents will not be subjected to full NCC Group Quality Assurance.

7 Description of Project Deliverables

The engagement is time bound based on NCC Group experience with similar outline scoped environments. This reflects the verbal nature of the scoping discussions that do not support a detailed resource level of scoping accuracy.

The time bound approach means the activities will be broad, to cover the agreed scope of the CLIENT Cloud environments (excluding 3rd party assets and solutions) and will execute to a depth allowable during the defined timescales. This does not preclude the option to extend this, if in agreement with CLIENT it is deem appropriate, otherwise NCC Group will highlight any areas for more detailed assessment as an elective recommendation in its findings.

NCC Group will document its findings to reported against the NIST CSF (Cyber Security Framework) v2.0.

This finding will be produced in a report format to include:

1. Executive Summary
    a. Summary of Findings
    b. Impact
    c. Prioritized Recommendations
    d. Conclusion

2. NIST Assessment Results
    a. Assessment Methodology
    b. Summary of Findings and Recommendations
    c. Detailed scoring of controls against NIST-CSF 2.0 Maturity Framework
    d. Scoring Definitions
    e. Controls Marked as N/A
    f. Summary of NIST-CSF Control Maturity Ratings

3. Technical Cloud Configuration review, providing a RAG status of configuration findings together with recommendations.

4. CLIENT Target Operating Model assessment and recommendations, with a particular requirement to provide a ‘people’ focused benchmark.

5. Recommendations and prioritisation roadmap plan for remediation – strategic, operational and technical

6. Appendices - Cybersecurity Maturity Rating Detail by Control

On delivery, NCC Group will review our key findings and recommendations with the Client either in person or via teleconference.

Location of Work:	REMOTE
Building Name:	
Address Line1:	
Address Line2:	
City:	
Postcode:	
Country:	United Kingdom
Client Legal Entity Name:	
Invoice Address:	
Address Line1:	
Address Line2:	
City:	
Postcode:	
Purchase Order Number*	

please complete the below signature box in order to confirm acceptance of this proposal and the commercial values stated within it.

Signed:	
Position:	
Date:	

NOTE: If the location, or the scope of this project changes post order acceptance, a change request and updated purchase order will be required to authorise the project continuation.

8 About NCC Group

NCC Group is a leading global information assurance firm, providing freedom from doubt that all critical material is available, protected, and operating as it should be at all times. Information assurance is delivered through escrow and verification, security testing, audit and compliance, software testing and web performance services.

Our independence from hardware and software providers ensures the advice we offer is unbiased and impartial. We focus on developing intelligent solutions to real business issues and building lasting partnerships through our comprehensive portfolio of information assurance services.

With a head office in Manchester and offices throughout England, continental Europe, and the USA, NCC Group serves the needs of a wide variety of clients worldwide.

We are listed on the Official List of the London Stock Exchange.

ISO 27001:2013 & ISO 9001:2008

NCC Group's Information Security Management System is certified to ISO 27001:2013. (LRQ 0963077). NCC Group Services is accredited to ISO 9001:2008 and has held ISO 9001 status since 1994.

NCSC (formerly CESG) CIR

The National Cyber Security Centre (NCSC) has approved NCC Group to provide cyber incident response services to organisations that have been victims of advanced attacks and those that form part of the critical national infrastructure

CREST Cyber Security Incident Response (CSIR) Scheme Certified

NCC Group is a certified member of the CREST CSIR scheme, endorsed by CESG and CPNI demonstrating that members are able to provide effective cyber security incident response services.

CBEST

NCC Group is an approved CBEST Threat Intelligence supplier and testing capability

CREST Council of Registered Ethical Security Testers

NCC Group is an active member of CREST, the standards-based organisation for security assurance testing suppliers aimed at ensuring the very highest standards of leading-edge security testing.

CESG CHECK

NCC Group is accredited under the Government's CESG Check scheme for network penetration and testing services. We have been classed as a 'Green' service provider, the highest attainable standard, continuously since 2001. Unless specifically stated this assignment will not be performed under CHECK terms and conditions.

CESG Tailored Assurance Scheme Provider

NCC Group was selected as one of the first companies to provide the CESG Tailored Assurance Service (CTAS), a brand-new service from CESG which is intended for a wide range of IT products and systems ranging from simple software components to national infrastructure networks.