NCSC Certified Assessment Services

NCSC Certified Assessment Services

Cloud First is as relevant to government today as it was when it was introduced, and will remain a flagship technology policy.

Transforming and meeting citizen demand is a key driver for many government bodies, both locally and nationally.

So, if you're worried about your cloud security posture, NCC Group can help:
- Do you know your organisation's cloud risk profile?
- How does that risk profile map to your budget?
- How does your budget map to your business risks?
- How has your risk profile changed in the last 28 days?

We can help you discover the answers. Our consultants know exactly what it takes to assess, deploy and manage cloud strategies and technical services in a government context, to maximise your ability to innovate and minimise risk.

We combine sector relevant technical cyber expertise with advanced processes and thinking, creating a formidable service with proven resource to support Agile deployments that can assure your cloud environments and resolve your challenges head on. We provide full lifecycle Cloud Cyber security services from initial assessments to actively managing your system platforms, giving you the confidence you need to reduce risk in successful service delivery.

With the digital world moving so rapidly, we know every organisation and cloud environment represents a very different challenge. That's why we work hand in hand with you throughout each project, identifying your exact needs to create tailored project or programme plans. Armed with those plans we mould a specialist team around your internal capability and trusted partners to ensure your cloud environment is safe, secure and fit for the future.

Expert Security Testing

NCC Group's CHECK service (ITHC) and Tailored Assurance Service (CTAS) helps you to secure and protect your critical systems in the cloud and data centres along with your wider organisation. Certified staff perform penetration testing at all protective marking levels for the public sector and associated organisations. We do not believe in there being a one size fits all assessment and pride ourselves on tailoring our approach to you.

Key benefits of NCC Group's cloud focused NCSC certified assessment offerings include:

Tailored to you: Assessments are individually tailored to obtain the most appropriate level of assurance in a pragmatic, independent, fashion. NCC Group assesses solutions at source, such as by evaluating build templates rather than conducting numerous build reviews. All scopes are defined with applicable threat actors in mind and utilise the latest relevant threat intelligence.

Impartial risk insight: NCC Group is product agnostic, and cares that the solutions you have chosen are effectively configured and meet your security needs. Risk ratings will factor in context from your organisation but remain impartial and evidence based. All assessments are governed by NCSC CHECK conditions, assuring you of our impartiality.

Safe: All activities are performed to pre-agreed rules of engagement, minimising the risk of any adverse operational impact.

Clear recommendations: We give you clarity on risk, including sufficient detail to allow you to fix issues easily. Our reports are easily consumed at technical, project and board levels. All recommendations are actionable and prioritised in line with risk. We can input risks straight into your management systems, supporting an agile delivery model.

NCC Group's cloud NCSC certified assessment experience and skills:

NCC Group has performed over 1,000 IT Health CHECK assessments in the past year.

Founding members of the CTAS scheme

NCC Group has over 50 fully certified CHECK consultants, split evenly between CHECK Team Member and CHECK Team Leader levels (with holders of Application and Infrastructure specialisms). Such a team allows us to react to your specific requirements with an appropriate test team, capable of delivering work to any protective marking, in timeframes unmatched in the marketplace.

We have several CREST Assessors who set the content of the exams that confer CHECK status to individuals.

Technical assessments can be supported by automated scanning, training and Escrow services.

Contents

NCSC Certified Assessment Services – ITHC & CTAS

Since 2001, NCC Group has been a Green Light Certified CHECK company and has a strong commitment to remain an approved provider. NCC Group have nearly 100 fully certified CHECK consultants, split evenly between CHECK Team Member and CHECK Team Leader levels. This size and knowledgebase means that you can be assured of the value we bring, both in the technical input to your decisions as well as our agile delivery capability.

Key to maintaining technical competence across the UK's largest CHECK team is investment in research that allows all team members to engage and contribute. Each year we invest over 1,500 person days in research across methodology development, offensive and defensive techniques, tooling and horizon scanning on emerging technologies and their security implications. Most of this research results in technical whitepapers, horizon scanning, blog posts, and conference talks (many Tier-1) which allows us to contribute to the cyber security community and demonstrate technical competence. Example recent research and outputs include:

PCloud & Virtualisation Technologies - NCC Group has released open source tools for auditing the security of AWS, Azure and Google Cloud deployments;

Virtualisation Technologies - NCC Group's team members contribute to the Kubernetes CIS benchmark standard and have published extensive research on Docker security;

DevOps – NCC Group has released threat modelling templates and blog often on DevOps and SDLC; we also release many open source tools on our public GitHub to facilitate secure DevOps;

Databases - NCC Group maintains its own proprietary database auditing tool, drawing heavily on output from our penetration tests of classic, cloud and newer database technologies such as NoSQL and Graph Databases;

Networks & Infrastructure – we have presented and blogged on exploitation of Cisco ASA firewalls and have developed a tool for checking the detection capabilities and performance of SOCs

To be current with real-world testing scenarios, our Cyber Defence Operations work closely with our CHECK team to facilitate knowledge transfer of research on emerging threats.

We are driven by you; we want to ensure you get the best service and insight possible. When you choose to use us, you get access to the full capabilities of NCC Group.

Whatever your need, a comprehensive evaluation of your environment, a traditional penetration test of your network or a more focused review of your business critical systems, NCC Group has a bespoke offering customised to your unique requirements to assist you in securing your cloud infrastructure, traditional data centre environments and supporting services.

Our Approach to Securing Your Environment

Location of Testing

TTraditionally the location of testing was a binary choice between remote and on-site, with remote testing conducted from across the Internet and on-site from within a trusted and protected network, typically a data centre or office location. The advent of cloud has blurred this distinction considerably, however the concept remains useful when considering the level of access a would be attacker or NCC Group consultant would have:

On-site Testing – the ability to assess the entire target unimpeded by network level security controls such as a firewall. Whilst firewalls and other mitigating controls are an essential component in a defence- in-depth strategy, many organisations wish to identify the true level of exposure of an individual target system should the network control fail or the attacker have trusted access behind the control. Software defined networks and virtual security appliances allow cloud environments to mimic traditional networks and as such the same considerations apply, albeit the controls are implemented differently, for example Conditional Access Policies within cloud environments.

Remote Testing – predominantly this testing takes place across the Internet and its intention is to mimic the level of access the majority of threat actors would have, be it a cybercriminal or hacktivist. Certain technologies may support remote testing across mediums other than the Internet, such as testing of wireless access points or remote access solutions over PSTN.

Firebase – an internally developed testing platform, Firebase is preconfigured to drop into your chosen network location, whether as a virtual machine or physical appliance. You have sole control of when the Firebase connects via a VPN using digital certificates to NCC Group's secure operations centre in the UK. All traffic is encrypted. Once connected, NCC Group consultants allocated to your project can conduct security testing as if they were physically in your office, data centre or cloud environment. Firebase allows for the level of testing associated with on-site engagements with the flexibility in scheduling and consultant support of remote engagements.

Level of access

A key consideration when commissioning a security test is the level of access and information you provide the testing team. The information can range from next to nothing though to everything available; this ranges from closed box, through partial box to open box testing:

Closed box testing – this is the minimal information necessary to conduct the test. In extreme cases this may consist solely of the target's organisational name with technical findings being confirmed at each stage prior to proceeding with the test plan. It is however more common for a confirmed list of target IP addresses and URLs to be provided prior to testing. This mimics the majority of common threat actors.

Partial box testing – additional information is supplied, yet not to the degree that test results may lose the context of a "hackers eye view". This type of testing is often used when assessing applications where valid user accounts are provided to the test team prior to the engagement. This mimics a malicious yet authorised user of the system.

Open box testing – considerable information is supplied to the test team, with the goal of finding as may issues as possible in an efficient manner as possible. The information supplied can vary considerably depending on the target but would typically consist of administration level user accounts, full system documentation, access to previous test reports, issue trackers and internal threat intelligence.

A greater level of access also enables you to gain a higher level of assurance in a given time period, for example five days of partial box testing may identify the same issues as an invested attacker who spends ten days attempting their attack, which is effectively a closed box assessment.

Often NCC Group delivers our services through a combination of all these methods to provide the level of assurance required. These are blended such that different attack vectors can be assessed, and scenarios explored.

ITHC: Threat Modelling / Architecture Security Review

The purpose of a threat model is to identify the assets to be protected and significant threats they face; the most likely methods by which those assets will be attacked; and the best means of protecting them from those attacks. Threat modelling is good practice with all projects and organisations as it allows you to identify key threats comparatively quickly and easily, it is however even more key in cloud environments where many disparate components are outside your direct control for example the underlying network or base operating systems.

In a threat modelling assessment, NCC Group will work with your organisation to produce a threat model of the systems under review. The threat model can be based on standards such as STRIDE.

The assessment consists of multiple steps, tailored to your individual requirements, but usually includes:

- A review of all relevant system documentation prepared by yourselves.
- A round of interviews with key stakeholders to understand the intended functionality, the rationale behind specific design decisions, the business significance of specific assets, and the potential for compromise.
- The final report produced by NCC Group will include a full threat model for the systems under review, including a list of potential attack vectors and means to mitigate these.

Optional Add-on Components

If desired it is possible to extend the exercise to include one of or both of the following:

- Threat Ranking Workshop
- Development of a technical testing programme

The documentation reviewed often includes:

- System architecture diagrams.
- Data flow diagrams.
- Database entity diagrams and data dictionaries. Functional specifications.
- Technical specifications.
- Use cases.
- User stories.
- Test cases.

Stakeholders to be consulted include:

- System architecture diagrams.
- Data flow diagrams.
- Database entity diagrams and data dictionaries. Functional specifications.
- Technical specifications.
- Use cases.
- User stories.
- Test cases.

ITHC: Infrastructure Security Assessment - External

Organisations are increasingly migrating systems and applications from their internal networks to the cloud; furthermore, external facing systems that were historically hosted on dedicated servers are increasingly leveraging the scalability and management advantages of the cloud. It is now more important than ever to accurately identify the assets to be protected and significant threats they face; the most likely methods by which those assets will be attacked; and the best means of protecting them from those attacks.

The purpose of an external infrastructure test is to simulate the access an Internet based threat actor may be able to achieve should they undertake a concentrated and professional attack against your cloud and Internet facing systems.

This phase of testing across the Internet will focus on retrieving as much publicly available data as possible about the hosting environment.

After this passive research, various tools will be used to actively gather information about the systems under review and their topology. Information such as OS identification and software type or version information, along with associated potential vulnerabilities, will be collated and researched. Where appropriate and agreed, attempts will be made to exploit the systems.

This assessment will typically include the following phases:

- Initial assessment – conducting an external black-box security assessment on hosts associated with the infrastructure, identifying devices and potential vulnerabilities. This will give a hacker's-eye view of the environment.
- Active attack – attempting to attack visible servers with no valid user credentials or trust.
- Perimeter bypass – circumventing the cloud conditional access controls, firewall and router perimeter security to directly access and exploit other components of the system. This phase will typically involve the chaining of vulnerabilities.

Unless specifically stated, the assessment will take place from NCC Group's secure testing labs.

Optional add-ons:

It is common should the environment contain particularly sensitive systems for there to be additional more focused tests conducted as detailed in "Focused Assessments". Systems typically selected for this further testing include:

- Networking equipment such as routers, switches and load balancers
- Security devices such as firewalls, IPS and content proxies
- Application servers such as email, web, CRM and ERP

Testing in-depth

Information retrieval activities include:

- Domain-based discovery
- Viewing the customer's website (if available)
- Review of Network Solutions and RIPE databases
- DNS zone transfer attempts to listed DNS servers
- Open information source vulnerability checks
- Web, newsgroup, IRC searches, company databases, social networks

Automated identification and enumeration activities include:

- UDP and TCP port scanning
- Operating system fingerprinting
- Service identification
- User enumeration
- Network mapping

Manual assessment of all live hosts and exposed services focuses on:

- Host and service configuration.
- Patching vulnerabilities
- Use of insecure credentials or protocols NCC Group use all information gathered to date to attack the services exposed.

All exploitation is done in strict accordance with agreed rules of engagement and is highly dependent on circumstances.

Once exploits have succeeded, we use any access and privileges gained to attempt to escalate access rights to the highest level possible within the scope of the agreed assessment.

All exploits are risk-assessed to minimise disruption to live systems

ITHC: Infrastructure Security Assessment - Internal

Organisations are increasingly migrating systems and applications from their internal networks to the cloud, primarily to leverage the scalability and management advantages offered. Depending upon the deployment method selected, Infrastructure, Platform or Software as a Service, the responsibility for securing the differing aspects of the environment will fall upon different organisations and often any confusion over ownership will result in an insecure and exploitable environment.

It is now more important than ever to accurately identify the assets to be protected and significant threats they face; the most likely methods by which those assets will be attacked; and the best means of protecting them from those attacks.

This purpose of an internal infrastructure test is to simulate the access a local threat actor, be they a legitimate user of the environment or an external attacker who has gained a foothold, may be able to achieve should they undertake a concentrated and professional attack against your internal systems.

This phase of testing will focus on gathering information about the systems under study and their topology. Information such as OS identification and software type or version, along with associated potential vulnerabilities, will be collated and researched. Where appropriate and agreed, attempts will be made to exploit the systems.

This phase is planned to include:

- Initial assessment – conducting a network-based black-box security assessment on hosts associated with the infrastructure, identifying devices and potential vulnerabilities. This will give a hacker's-eye view of the environment under review.
- Active attack – attempting to attack visible servers with no valid user credentials or trust.
- Perimeter bypass – circumventing the cloud conditional access controls, firewall and router perimeter security to directly access and exploit other components of the system.

Testing will be conducted from one or more subnets within the environment. Multiple connection points are utilised in order to assess the target systems unobstructed by firewalls, as such the number required is heavily dependent upon the topology of the environment.

Optional add-ons:

It is common should the environment contain particularly sensitive systems for there to be additional more focused tests conducted as detailed in "Focused Assessments".

Testing in-depth

Discovery:

- All address ranges are scanned across most typically used protocols (TCP, UDP, & ICMP) to identify live hosts.
- Active Directory domains and forests are identified, and account information is enumerated.
- UNIX servers are scanned for running services such as Telnet, SSH, X11, r-services, SNMP, and NFS.
- Web, database and other key services are identified.

Connectivity and Network Architecture:

- The connections to and from the servers, including firewalled segments are reviewed.
- Network appliances such as routers and switches are identified.
- Ingress and egress connectivity is evaluated to determine the effectiveness of proxies and outbound firewall rules.

Research Phase

- During this phase we will research any weaknesses in the identified services using up-to-the-minute vulnerability databases.

Assessment

- NCC Group uses all information gathered to attack the services, subject always to agreed rules of engagement.
- Privilege escalation techniques are used to elevate access levels. Local and domain password files are obtained and cracked where possible.
- Database services are reviewed for default or weak accounts, credentials, the presence of dangerous stored procedures and SQL injection.
- Authentication processes are attacked in a safe manner using both default credentials and brute-force techniques.

All exploits are risk-assessed to minimise disruption to live systems. All remnants of any attack are removed

ITHC: Web Application Security Assessment

The uptake of cloud technologies has never been higher, and a key use case of these platforms is the provisioning of web applications to support either business to business or business to customer transactions. Increasing levels of security around encrypted channels and certificates has improved the security posture of many applications, however these measures have little impact on what a trusted user of the application could accomplish, or indeed an attacker who is able to self-register.

The adoption of cloud technologies has altered the threat profile of web applications, they can no longer be assessed in isolation and their DevOps support mechanisms need to be included to address the current methods of secrets management, source code control and release management.

The primary areas of concern in web application security are therefore authentication bypass, injection, account traversal, privilege escalation, and data extraction.

The purpose of the web application assessment will be to identify security vulnerabilities that may be exploited to compromise either the server-side application or ordinary users of the application. The assessment will involve the following broad areas of work:

- **Recon and analysis** – NCC Group will map the application's content and functionality, analyse its behaviour, identify all possible entry points for user input, and develop a clear understanding of the attack surface exposed by the application.
- **Assessment of access handling** – NCC Group will test the application's core security mechanisms, including authentication, session management, and access control, to identify any defects that may enable an attacker to gain unauthorised access to functionality and data.
- **Assessment of input handling** – NCC Group will test the application's resilience to numerous kinds of unexpected input throughout its functionality, looking for code injection and other vulnerabilities. Assessment of application logic – NCC group will probe for defects within the application's logic, including inappropriate reliance on client-side controls and logic flaws within server-side functionality

OWASP Top 10;

Our methodology covers all of the OWASP top ten web application security risks and more.

A1: Injection
A2: Broken Authentication
A3: Sensitive Data Exposure
A4: XML External Entities (XXE) A5: Broken Access Control
A6: Security Misconfiguration
A7: Cross-Site Scripting (XSS)
A8: Insecure Deserialization
A9: Using Known Vulnerable Components
A10: Insufficient Logging and Monitoring

ITHC: Cloud Platform Assessments

Cloud Platforms offer infrastructure-as-a- service (as well as software-as-a-service and platform-as-a-service) systems for enterprise customers. Cloud Platforms are often the single largest outsourced element of an organisation's IT infrastructure. They are often vital to a company's business, but their complexity, and the nature of cloud systems, mean that they are also often misconfigured and vulnerable to attack.

During a Cloud Platform Assessment, NCC Group's consultants will examine your IAAS system configuration first from a network perspective – examining the system from outside for vulnerabilities that would be obvious to an attacker – before performing a full configuration review of the platform's environment settings to ensure these are following best security practice.

Assessments vary on a case-by-case basis, but usually include reviews of authentication mechanisms, user access rights, at-rest data encryption, VM operating systems, and any software installed on the systems. In addition to the three main providers detailed to the left we have experience in assessing Oracle Infrastructure, IBM Cloud and Alibaba Cloud.

Cloud Platform Assessments can be augmented with focused assessments against serverless technologies such as Docker and Kubernetes.

A Cloud Platform Assessment will give a broad overview of the security of your whole cloud computing estate, giving you freedom from doubt as to the security of your systems.

amazon web services

- EC2 Instances
- EBS Volumes
- S3 Bucket Storage
- RDS Instances
- IAM roles for EC2 instances
- Cloud Trail
- Outbound EC2 access restrictions

Azure

- Virtual Machine Instances
- Page Blobs/Managed Disks
- Blog Storage
- Database Instances
- Azure Active Directory
- Logging
- Outbound VM access restrictions

Google Cloud

- Compute Engine Instances
- Persistent Disks
- Cloud Storage
- SQL/Spanner Instances
- IAM roles
- Logging and Reporting
- Outbound Compute Engine access restrictions

Common checks across all platforms:

- Access keys and root account status
- Policy configuration
- Use of zones
- VPN configuration
- Password policy
- Tenancy mode
- Region in which data is held
- Network Security Groups and Access Control lists
- User groups and privileges
- Encryption of snapshots and volumes
- Monitoring
- MFA configuration

ITHC: Focused Infrastructure Security Assessments

This purpose of an NCC Group focused assessment is to dig deeper into the configuration of particular systems.
These engagements are performed with interactive access to the device, typically as either the Administrator or root user, such privileged access allows NCC Group to comment on configuration elements we would not otherwise be able to from an unauthenticated network perceptive.

Focused assessments have further advantages, firstly they have a lower false positive rate as it possible to cross reference potential issues against several configuration sources; and secondly, they can be more efficient in the case of voluminous or difficult to enumerate sources such as a firewall rule base.

During these targeted assessments, we will undertake a comprehensive review of the operating system builds and the configuration of key components. This will focus on assessing the build security quality of the device, encompassing areas such as:

- Installed OS components
- System services running
- Core security configuration (firewall, automatic updates, etc.)
- Patch levels
- User accounts
- Password policies (strength, expiration, lockout policies, etc.)
- Registry configuration / permissions
- User rights assignments
- Audit policies
- Event log management
- Kernel settings
- Boot services
- Network services
- User accounts and rights, password policies, system access, authorisation, and authentication
- Application security settings (Email service configuration, firewall rule base or IDS rules etc.)

Dedicated Testing Methodologies

NCC Group are capable of reviewing all devices against security best practice and have formalised methodologies for the more commonly encountered:

- Operating Systems – Windows, Apple Mac and all variants of Linux
- Network devices – switches, routers, Wi-Fi access points & load balancers
- Security devices – firewalls, IDS/IPS, anti-virus, content filtering and security proxies
- Application services – Email server, web server, SharePoint, Hadoop, Jenkins and SAP etc.
- Active Directory
- Database servers – RDBMS, NoSQL, key value stores, and graph databases
- Infrastructure services – DNS, NTP and DHCP

ITHC: Remote Working Security Assessment

Remote working and the use of bring your own device have both become more prevalent over recent years and with them the rapid erosion of the traditional network perimeter. These changes combined with the uptake of the cloud results in organisations adopting "Zero Trust" initiatives that no longer rely on the concept or trusted networks, but instead rely upon the robust verification of users and systems wherever they may be located.

Organisations are expanding their perimeter in a variety of ways, from remote access to the organisation's networks from either business or personal devices, to the use of terminal services, all commonly deployed within the cloud. Whichever solution you have selected, NCC Group have an assessment that can ensure you remain secure.

Mobile Device Management System Assessment – This engagement will ensure that your MDM software is configured securely, that the policies the software implements are appropriate for your organisation's use cases, and that the infrastructure on which the software runs is safe from compromise. NCC Group's consultants will review the software itself for known vulnerabilities, ensure that policies cannot be violated, assess the authentication methods used, and ensure that the software used can correctly enforce remote upgrades and wipes.

Mobile Device Assessment – NCC Group's mobile device review will assess the security of your devices from three different perspectives – as someone who has found or stolen a device but has no valid credentials, as an attacker who has also obtained a username and password for the device, and as a malicious staff member who is attempting to use the device to compromise the internal network.

BYOD Assessment – NCC Group will assess your organisation's BYOD security policy, ensuring that it provides the proper balance between corporate security and your employees' rights as owner of the device. In particular, we will ensure that your policy only allows up-to-date, secure, versions of operating systems such as iOS and Android, that you have an up-to-date list of authorised users and devices, and that your mobile device management software is correctly configured to apply all appropriate security patches to the users' devices. We will assess the lists of authorised and unauthorised applications, to ensure that no insecure software is allowed on the devices, and will ensure that your mobile device management software is able to remotely wipe any confidential data from a lost or stolen device, and that it can revoke access at any time.

Stolen Laptop Assessment – NCC Group's stolen laptop review will assess the security of your laptops from two perspectives – as someone who has found or stolen a machine but has no valid credentials, and as an attacker who has also obtained a username and password for the laptop.

Remote Desktop Breakout Assessment – During a remote desktop test, NCC Group will connect remotely to the server as a typical user (using a username and password supplied by you) and will use standard techniques to try to run unapproved software which, if successful, will allow us to gain administrative rights to the remote desktop server. We will also attempt to take advantage of server vulnerabilities to take control of other devices on the internal network, as well as checking the server configuration against best practices.

VPN/RAS Assessment – A review of the VPN endpoints to ensure that they are configured in line with industry best practices and have been securely deployed. The assessment will include a general administration review of patching levels and administration configuration (users, protocols, ACLs etc.) as well as the suitability of split tunnelling and other VPN configuration options such as peer configuration, crypto map usage and the IKE policy.

ITHC: Secure Development Lifecycle

Whether you use the latest agile methodology with three-week iterations or have a traditional waterfall process and are on 24-month release cycles, NCC Group can help you understand your current practices and identify how security can be better integrated into your development lifecycle. Ensuring your cloud native and cloud dependent applications are secure.

NCC Group will perform a gap analysis of the current practices and activities within the software development lifecycle (SDLC). As part of this analysis, NCC Group will undertake the following activities:

- Understand the risk profile of the business and the software solutions being developed.
- Conduct required workshops and meetings with stakeholders, relevant architects, development leads, and testing staff.
- Review pipeline management and the use of CI / CD tooling.
- Assess existing development practices and activities with regards to security activities.
    - Requirements phase.
    - Design and architecture.
    - Development.
    - Testing and quality assurance.
    - Sustainment and incident response.
- Perform a gap analysis on any existing development processes and procedures to identify key areas for improvement.
- Provide a report against current development practices and the use of SDLC:
    - Against industry best practices.
    - Against the risk profile of the business and the software solution being developed.
    - Against a target state in Microsoft SDL, BSIMM or OpenSAMM models if desired

Secure Development Lifecycle Principals:

Whether you are happy with your SDLC in general and want to add security activities, or want to modify your SDLC as well as securing it, there are some general principles which apply:

- For successful adoption and sustainability, security standards need to be embedded into the general development standards, rather than existing in parallel.
- For successful adoption and sustainability, the development team needs to have a sense of ownership over the secure development standards

Security Standard:

A software development security standard should cover or exceed all of your external compliance requirements. This standard will evolve as you progress in your implementation of the security improvements roadmap. The standard covers mandatory and recommended security activities in the following areas:

- Secure training
- Security requirements
- Secure architecture and design
- Coding standards
- Code review guidelines or checklist
- Testing methodology
- Incident response procedures

Tailored Assurance Service (CTAS)

The purpose of a Tailored Assurance Service (CTAS) is to provide answers to assurance questions and concerns from accreditors, which are usually from the pre-deployment stage. A tailored evaluation is then conducted and key results that may impact business are highlighted.

A CTAS evaluation consists of a Preparation phase and an Evaluation phase.

Preparation phase:

Ensures the evaluation is appropriately scoped so that it is able to answer the Accreditor's assurance questions and that the activities will meet HMG and sponsor requirements. Within this phase there are two stages "Definition and Planning".

Definition - Defining the scope of the evaluation through creation of a Security Target (ST) document for the Target of Evaluation (ToE).

Planning - Planning the evaluation through the creation of an Evaluation Work Programme (EWP) detailing activities to be used throughout the activity stage of the Evaluation phase.

Once both stages have been completed and signed off, the evaluation can move to the next phase.

Evaluation phase:

Completion of the agreed evaluation activities and then compile the evidence and act on the results. The phase consists of two stages "Activity" and "Reporting".

Activities may include:

- Documentation reviews including security architecture, design, test evidence, development and operational procedures.
- Audit of development, delivery and installation and/or operational procedures.
- Analysis and review of source code and vulnerability analysis.
- Testing of security functional requirements to provide verification of a developer test, or a security test with easy to define input data and outcome.
- Penetration testing or ITHC. This includes any testing bespoke to the ToE and tests that require a large amount of specific expertise. Included in this work are also activities such as build and configuration reviews of ToE components.

Reporting will consist of:

- Provision of a full evaluation report for NCSC and Accreditor review.
- Creation of a draft Assurance Maintenance Plan (AMP) that will detail activities and responsibilities for ongoing assurance of the target under evaluation.

Optional maintenance phase:

The maintenance phase is recommended but not required by NCSC. The purpose of the phase is to manage low risk changes to the ToE and consists of two recurring activities:

- Evaluation activities – perform and review all audit activities as detailed in the EWP.
- Reporting – updating of the evaluation report and producing assessment statements for NCSC.

Goals of the Evaluation:

- Deliver a testing programme customised to the Target of Evaluation focused on the appropriate security attributes
- Answer the Accreditors assurance questions
- Provide a programme of work that meets the requirements of HMG, MOD and the wider public sector
- Provide continued assurance through configuration changes in the optional CTAS maintenance phase

Reporting and Deliverables

NCC Group's consultative engagements support a number of vulnerability scoring systems including:

- Risk (default) – Issues are assigned a criticality rating of Critical, High, Medium, Low or Info
- CVSSv2/CVSSv3 – The Common Vulnerability Scoring System is a vendor-independent industry open standard,
- CWSS - The Common Weakness Scoring System (CWSS) provides a mechanism for prioritizing software weaknesses in a consistent, flexible, open manner.
- MS BugBar – Microsoft SDL Security BugBar.
- DREAD - Classification scheme for quantifying, comparing and prioritizing the amount of risk presented by each evaluated threat

Symbol	Risk	CVSSv2	Explanation
	CRITICAL	9.0 - 10	This vulnerability requires resolution as quickly as possible.
	HIGH	7.0 - 8.9	This vulnerability requires resolution in the short term.
	MEDIUM	4.0 - 6.9	This vulnerability should be resolved as part of the ongoing security maintenance of the system.
	LOW	1.0 - 3.9	This vulnerability should be addressed as part of routine maintenance tasks.
	INFO	0 - 0.9	This finding should be addressed in order to meet leading practice.
	N/A	N/A	Good security practices were being followed or an audit item was found to be present and correct.

Optional information channels:

Daily wash-up meetings – an opportunity to discuss progress, any issues and findings to date. Any high or critical issues are always reported as they are identified.

End of engagement presentation – A post assessment briefing can be provided to give you an opportunity to discuss the engagement's findings and recommended next steps.

Findings in CSV format – to allow for the importing of findings into any GRC and issue tracking systems you utilised.

About NCC Group

NCC Group is a global expert in cyber security and risk mitigation, working with organisations to protect their brand, value and reputation against the ever-evolving threat landscape.

With our knowledge, experience and global footprint, we are well placed to help organisations identify, assess, mitigate and respond to the risks they face.

We are passionate about making the Internet safer and revolutionising the way in which organisations think about cyber security.

For more information from NCC Group on our G-Cloud 15 service, please contact:

+44 (0)161 209 5200

bidteam@nccgroup.com