Cyber Security Improvement & Remediation

NCC Group's Security Improvement and Remediation services help security teams rapidly reduce their cyber risk by prioritising and fixing security weaknesses in collaboration with the clients. Our services are a natural next step in addressing the risks and making a real-world and tangible impact on the security posture in a trusted advisor position.

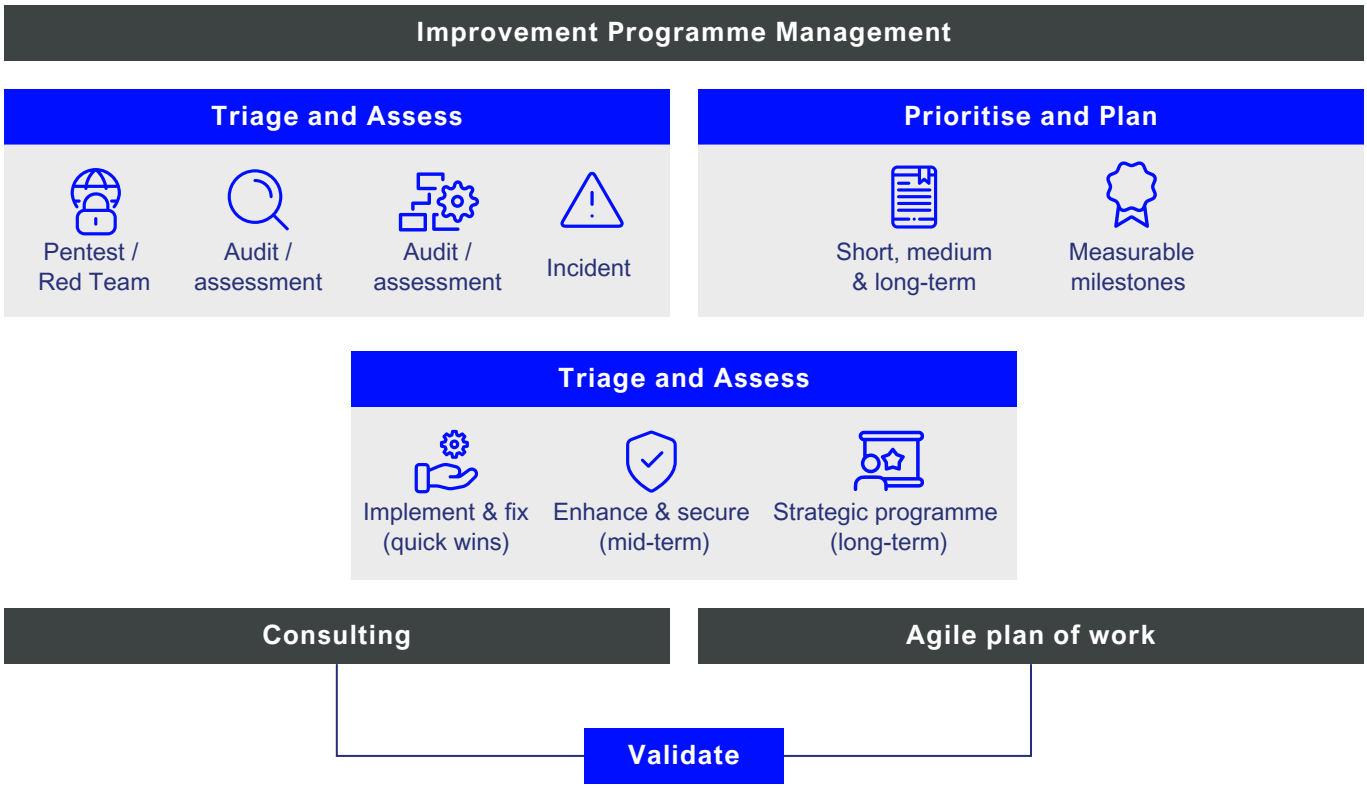
Security assessments, audits and the lessons learned from a breach can all provide valuable insight to understanding risk exposure.

Translating these insights and turning them into an improvement plan can be a challenge for clients.

Skills gaps, capacity and establishing a holistic view of exposure often hinder companies.

Consuming reports and the volume of noise from broad and wide subject matter range is complex.

Our Approach



Triage and Assess

We will leverage existing vulnerabilities and issues from our own assessments as well as other parties, however there is often a need to gather intelligence, enhance or augment the existing information to augment the existing issues list or to uncover wider issues to the full extent.

Prioritise and plan

Security Improvement Plan (SIP) for an agile prioritised approach to risk reduction

We will help make sense of all the issues and vulnerabilities and turn current issues into executable work packages. We will contextualise them, group and combine into business-relevant themes and create a prioritised backlog of tasks. We will:

- Augment with our additional inputs
- Prioritise for security improvement, complexity etc
- Agree estimates and owners
- Identify external dependencies.

Prioritised backlog of actions and tasks

By turning current issues into executable actions, we will develop a comprehensive security improvement plan. Working closely with your organisation, we contextualise threats and prioritise task backlogs based on improvable measures and complexity, by utilising agile platforms or ticketing systems. It enables you to define the key next steps and remain flexible.

Implement and improve

Once you have a clear understanding of your resilience in cyber security terms, we will help you implement fixes to provide a rapid and effective improvement of your security posture. Implement improvements in cloud or on premise like Active Directory, AppLocker, LAPS, InTune or JAMF. We work in an agile approach. This model allows us to provide shorter planning sessions with multiple deliveries and iterations, enabling us to be flexible and involve our clients throughout the sprints.

Enhance and secure: Fix and implementation collaboration and guidance

We will assist you in materially improving their security posture. We offer the following levels of tailored service:

- Hands-on implementation – end to end consideration and in collaboration with the client
- Trusted advisor and security partner model
- Third-party assurance and security risk advisor model.

Defensive capability and logging enhancement for detection

The key to the success of our security, risk and remediation teams is in our collaboration, partnership, and agile approach with our clients, in a mutual transfer of knowledge. Our programmes are dedicated to always respecting any change request processes or production deployment rules from clients.

Business enablement through integration and coherence with security policies and procedures.

We work to ensure that the right risk, governance and management controls are effective. We look to address and remediate the technical risk areas while simultaneously providing the right people and process platforms for successful resilience and preparedness.

Prioritise and plan

Security Improvement management

If you require help in leading transformative remediation, we will design an improvement program and help managing it. Our services include:

- Key communication with the IT staff, the C-suite/board, technical leadership of collaborative NCC Group/client sprints/plans
- Client and 3rd party interactions and problem solving, regular stand-ups / progress reviews
- Track velocity, resource utilisation, external dependencies, risk register, maintenance and planning of the outstanding task list
- Weekly highlights report.

Security Improvement and Remediation Advisor Consultancy

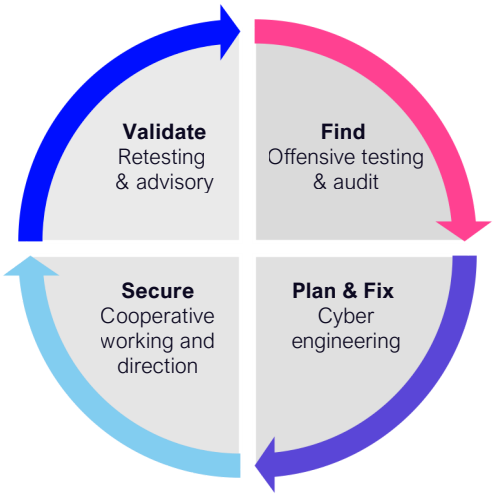
If you need help to focus on security improvement, we will provide strategy, technical direction, and clear path to security improvement. The work will include assessing and enhancing pre-existing risk and security information including incident reports, red team findings, penetration tests and security audits.

This consultancy crosses disciplines, such as AppSec, Cloud, Infrastructure, Strategy, Risk and Governance and will include engagement with senior leadership. Engagements include projects such as vulnerability management, patch management, or any other form of remediation delivery.

Example engagements and projects

Technical Rapid Security Improvement

A rapid security improvement, in a find, fix, validation loop, performed in close collaboration with the client. This is an agile workstream building on offensive and defensive capabilities across the entire NCC Group for a targeted and impactful risk reduction in the fastest possible time.



Find the issues using pen-testing and audit techniques

Make sure that the issues are managed and grouped for fixing effectively and in an agile way

Assist with the fixes – hands-on approach in collaboration with you

Check they have worked as expected

Application Security Development Remediation

Implement improvements in the SDL like scanner tooling in CI/CD and results interpretation. This is most useful where the SDL practice has performed a gap analysis and suggested remedial work to the client. Alternatively, a significant amount of web application or API testing has uncovered systemic vulnerabilities that require remediation. The work can be hands on and include people and process and a mix of application and infrastructure skills. It will adhere to your change control and can be facilitated through FireBase, cloud user accounts or both.

Staff Augmentation: Fixed term / Cyber Security Engineer (CSE)

We will provide a Cyber Security Engineer to work as part of your security team to help close capacity or capability gaps and to assist you perform various IS (Information Security) tasks:

- Assist in enhancing current security posture
- Develop plans to enhance security long term in a collaborative approach
- Enhance your capability to defend and monitor your network and data.

Additional IT Engineering expertise when you need it most

We can provide knowledgeable staff to support internal IT in recovery and remedial efforts – rebuilding stronger than before to reduce the likelihood of a repeat incident by increasing resilience. Our consultants can rapidly deploy to add engineering capacity in the following ways:

- To recover from an incident, rebuilding systems and restoring services
- Accelerate existing internal security improvement programmes
- Immediately implement recommendations made as part of an incident response.

Why NCC Group?

Wide range of qualifications on most technologies

Across our, near 2,000 consultants, we hold a range of qualifications and skills to address technology challenges.

World class knowledge and expertise

Our skills are honed through our consultancy, our staff develop a deep knowledge of the impacts around security decisions. This knowledge can be tapped to help accelerate your remedial timelines. Validate Retesting & advisory Find Offensive testing & audit Secure Cooperative working and direction Plan & Fix Cyber engineering Find Offensive testing & audit Validate Retesting & advisory

Security clearances

NCC Group staff hold the full range of government clearances and can respond in a timely manner.

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