Incident Response Readiness

NCC Group Incident Response services help organisations achieve improved incident response planning and readiness through maturity gap assessment, development of incident response policies and procedures, incident playbooks and run books, in addition to the provision of organisational training to improve resilience and the ability to respond to cyber attacks.

Improves maturity of incident response capability

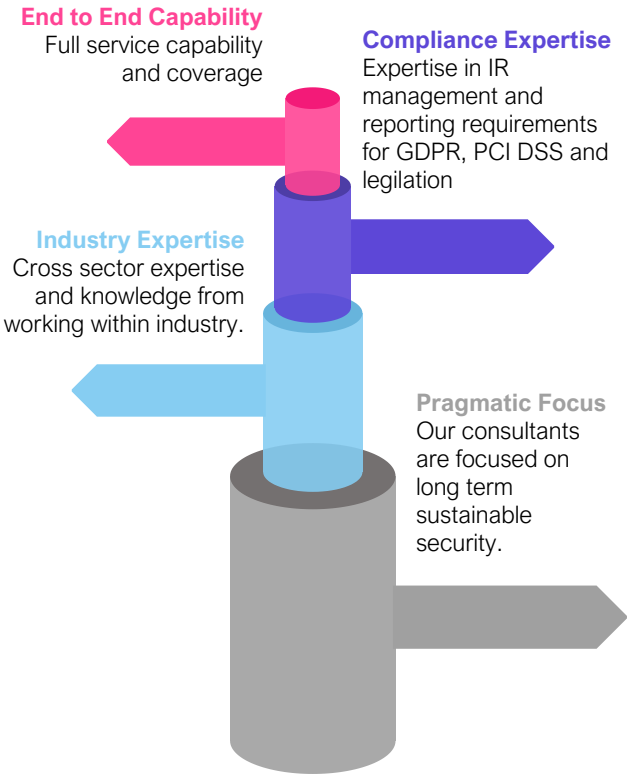
NCC Group's incident response health check has been specifically designed to assess incident management controls and provide assurance of their effectiveness. Its holistic approach will look at controls from the identification of an incident all the way to implementing lessons learnt.

Provides alignment to industry incident response models

Changing business objectives or structure may sometimes render incident management controls ineffective. Therefore, this review is aligned to your business and corporate objectives whilst considering industry best practice standards. NCC Group will combine this with its experience of the cyber threats in your sector to ensure your health-check report is clear and understandable to a wide audience of stakeholders.

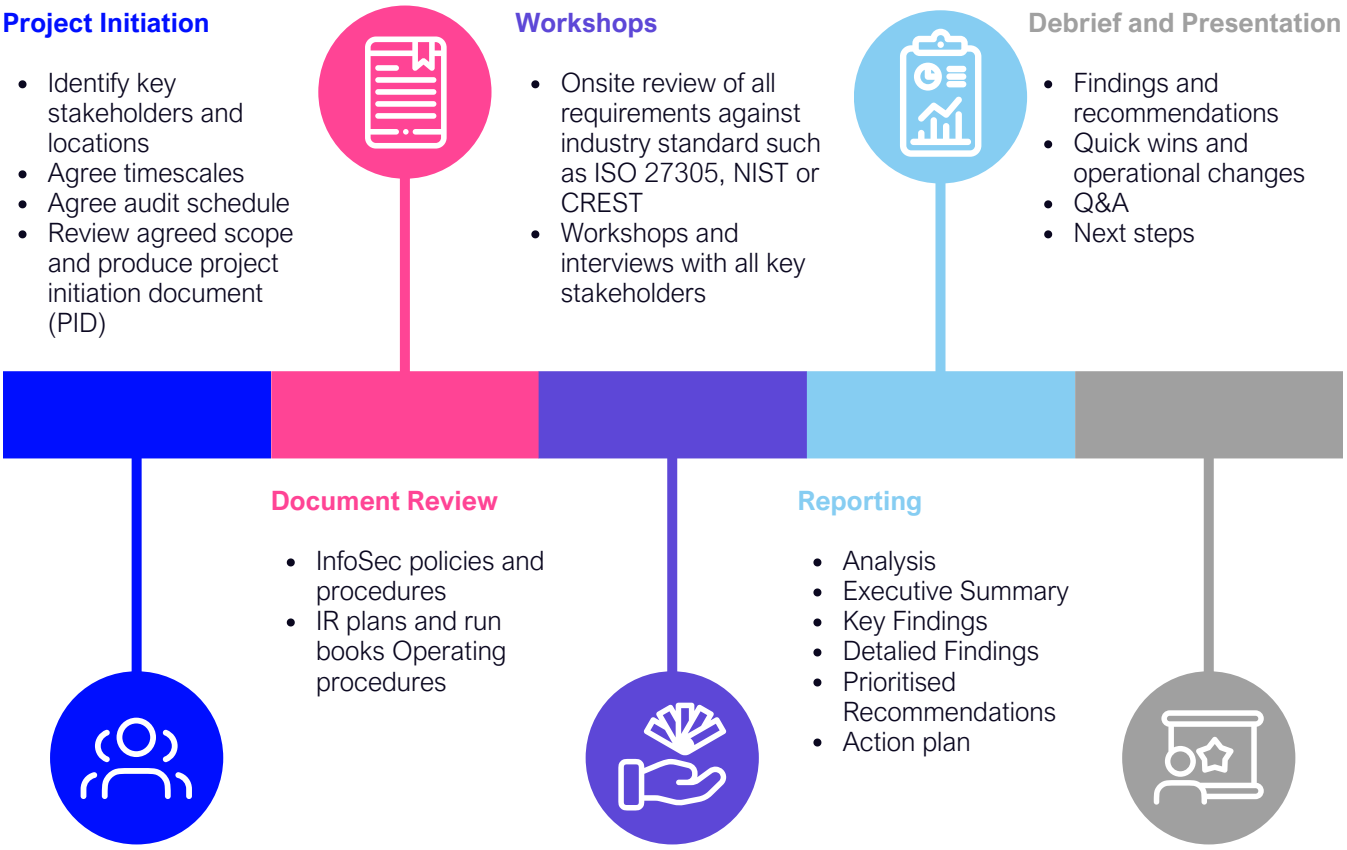
Improves awareness of incident management within the organisation

The health check process will include reviews of all relevant parts of the business, not just the IT team. The review will consider other functions of the business that maybe be involved such as data protection, legal and marketing. Creation of incident response plans will include plans for all these business functions so they are actively involved in the event of an incident.



Benefits

- Improves maturity of incident response capability
- Provides alignment to industry incident response models.
- Improves awareness of incident management within the organisation
- Provides repeatable processes for incident response handling
- Reduces potential cost and impact from security incidents
- Ensures cyber incident and breaches are correctly reported.



IR Health check

NCC Group will assess the current position of the organisation's Incident Response plan, capture and validate security controls that are currently operating. NCC Group will focus on the design and operational effectiveness of the organisation's incident response processes against the industry standard controls. This is normally aligned to ISO27035:2016 or NIST SP800-62.

To undertake this review, NCC Group:

- Uses its tailored ISO27035:2016 standard questionnaire and worksheet to capture current status;
- Reviews existing documentation as provided by the organisation; and
- Conducts interviews with organisations stakeholders.

The detailed findings of this activity are provided in the separate NCC Group Incident Response Assessment workbook, where the controls compliance dashboard is provided to show a high-level view of the status for both Part 1 and Part 2 of the ISO and/or NIST standard.

The use of the workbook will aid organisations in tracking remediation against the observations, where the dashboard will provide a current state of the control posture. The NCC Group tool will also act as a benchmark against which organisations can assess their status and identify priority remediation activities.

Cyber Incident Response Policy

NCC Group will create a standard policy defining the relevant policy statements for the organisation including:

- Scope
- Roles and responsibilities
- Defined policy statements

Incident Response Management Plan

NCC Group will create an incident response procedure based on industry best practice and including:

- Scope
- Governance and roles and responsibilities
- Planning and Preparation
- Triage and Classification of Incidents
- Escalation Procedure
- Containment and Evidence gathering
- Handling procedures
- Recovery
- Reporting and Lessons Learned

IR Run Books

NCC Group will create an incident response run books, based on industry best, and that will include triage, containment and recovery for incidents related to specific defined scenarios such as:

- Ransomware
- Denial of Service
- Data Loss
- Malicious Network Behaviour
- Social Engineering
- Insider Abuse

The run books can be tailored to focus on key scenarios that are specific to the organisation's methods of operation, or high-risk areas.

Summary

The NCC Group's Incident response health check allows organisations to gain an overall view of their IR maturity against industry best practice standards. NCC Group can help organisations reach the required level of IR maturity by supporting the creation of incident response policies, plans and run books. NCC Group supports clients in reducing the potential cost and impact from cyber security incidents. NCC Group's consultants are highly skilled and have been supporting organisations in different industry sectors for many years. NCC Group's IR capability and experience is unparalleled with a fully global Cyber Incident Response Team and specialist IR consultants.

Incident Response Readiness Review

- Review of people, processes and technology IR controls
- Maturity based scoring
- Prioritised recommendations to help improve your IR service

Incident Response Framework

- Development of tailored IR management plan
- Development of technical run books for multiple scenarios such as malware outbreak and forensic evidence containment
- IR Testing Plan and IR Checklist

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