

# PCI DSS QSA Consultancy Services

---

**NCC Group has a large, dedicated and truly global team of PCI DSS accredited QSAs who can help you with all of your PCI DSS requirements. NCC Group provides a full suite of services to help you achieve and maintain compliance whether you are at the beginning of your journey or already compliant and seeking re-certification. NCC Group provides this service to many organisations across all sectors, from small local companies to large global corporations, with all sizes of Cardholder data environments. This experience allows NCC Group's experts to provide pragmatic, sustainable recommendations and the support required to implement them.**

### **What is PCI DSS?**

The Payment Card Industry Data Security Standard (PCI DSS) compliance is mandatory for organisations that store, process or transmit cardholder data as part of their merchant agreement with their acquiring bank. The PCI DSS is a set of information security requirements designed to reduce payment card fraud. For organisations that have to be PCI DSS compliant it is not an insignificant challenge. There are over 300 requirements that must be designed, implemented and managed across your organisation's Cardholder Data Environment. Without expert advice it is difficult to achieve given everyday constraints which often includes legacy platforms, multiple service providers, staff shortages, business growth and constant change.

### **How can NCC Group help?**

NCC Group is accredited by the Payment Card Industry as a Qualified Security Assessor (QSA) and as a PCI Approved Scanning Vendor (ASV). NCC Group offers specialist PCI consultants with extensive, practical, experience and specialist knowledge to support your compliance efforts. NCC Group also has a team of Technical Security Consultants able to deliver penetration testing and scanning. This allows NCC Group to help you at all stages of PCI compliance. The QSAs job isn't just about helping you become PCI DSS compliant. It is also about your organisation gaining PCI DSS compliance cost effectively and ensuring it is sustainable.

### **Benefits**

- Achieve Business-led (rather than audit-driven) outcomes across industry sectors
- Significant focus on strategic PCI DSS scope and cost reduction
- Significant experience within Central Government and public sector
- Creation of pragmatic, sustainable and actionable remediation plans
- Excellent relationships with acquiring banks create a 3-party collaborative approach
- QSAs with Cloud security expertise, understanding the challenges and solutions
- Experience across all technology stacks, leveraging company-wide expertise
- Continuity of QSA resource, providing the best service and relationship
- Fully scalable and flexible service offerings, to fit your needs.

# Our PCI DSS Services

## CI DSS services offered:

- Introductory awareness sessions to your staff
- PCI DSS Programme management and strategy definition
- Scoping definition to identify the relevant systems and processes involved
- Gap analysis of your current situation
- Internal and external (ASV) vulnerability scanning
- Penetration testing
- Remediation support
- PCI DSS solutions options analysis
- PCI DSS network design review
- Report on Compliance (ROC) assessments
- SAQ support and validation
- End user training and awareness
- Incident response training
- Software development life cycle (SDLC) training to help your teams to design, develop and deploy secure software
- Policy and procedure development.

| Analysis Phase                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                   | Support Phase                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Accreditation                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Scoping Study</b> <ul style="list-style-type: none"><li>• Define Cardholder Data Flows.</li><li>• Confirm Merchant/Service Provider Level and PCI DSS requirements.</li><li>• Define your Cardholder Data Environment (CDE).</li><li>• Provide options for de-scoping.</li></ul> | <b>Gap Analysis</b> <ul style="list-style-type: none"><li>• Identify gaps against the standard.</li><li>• Advise on impact or remediation and compliance.</li><li>• Provide prioritised recommendations.</li><li>• Produce PCI DSS remediation roadmap.</li></ul> | <b>Remediation Support</b> <ul style="list-style-type: none"><li>• Call Off agreement.</li><li>• PCAD production (see in remediation support section).</li><li>• Progress reviews.</li><li>• Policy development.</li><li>• Technical/design assistance.</li><li>• Design/validation of compensating controls.</li><li>• Options analysis.</li><li>• Procurement support.</li><li>• Penetration testing.</li><li>• ASV scanning.</li><li>• Incident Response Planning.</li><li>• Training and awareness.</li><li>• Secure SDLC training.</li><li>• Configuration standards.</li></ul> | <b>Report on Compliance</b> <ul style="list-style-type: none"><li>• Formal on-site assessment.</li><li>• Regular reporting and updates.</li><li>• Rolling issue log.</li><li>• Non-compliance remediation support.</li><li>• RoC and AoC production.</li></ul> |
| <b>Gap Analysis</b> <ul style="list-style-type: none"><li>• Combined Scope and Gap Review designed for smaller merchants.</li></ul>                                                                                                                                                 |                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                |
| <b>PCI Strategic Review</b> <ul style="list-style-type: none"><li>• Strategic-level Scope and Gap Review for Multi-National Corporation/Enterprise scale organisations.</li></ul>                                                                                                   |                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <b>Supported SAQ</b> <ul style="list-style-type: none"><li>• On-site support completing SAQ.</li><li>• Scope confirmation.</li><li>• Evidence validation.</li><li>• QSA sign off.</li></ul>                                                                    |

---

# Additional Supporting Services

## PCI ASV and Internal PCI Scanning Managed Service

NCC Group's PCI ASV and internal PCI scanning managed services are designed to significantly reduce the risk of a card holder data breach that originates from weaknesses in your systems. These services are delivered from NCC Group's in-house Security Operations Centre (SOC) which is staffed by a large team of vulnerability management and penetration testing experts. They use the latest high-end security scanning tools and augment these with specialist knowledge to provide your PCI scanning as a managed service.

In addition to your external PCI ASV scans, NCC Group can also conduct your internal PCI scans to provide you with a full PCI DSS managed scanning compliance package, including:

- Quarterly PCI ASV scans against any external infrastructure and application hosts in your PCI DSS environment.
- Internal PCI scans of your infrastructure and application hosts.

NCC Group's scanning services can be used individually, or you can allow NCC Group to manage all of your PCI scanning requirements by taking out a joint scanning package. Results from each scan are available in the web-based customer vulnerability management portal and via direct reports emailed to you.

## PCI Security Application and Infrastructure Testing

NCC Group's application and infrastructure PCI penetration tests are performed by experienced Technical Security Consultants who have a wealth of knowledge in diverse IT disciplines including policy, design, implementation and development. Having the largest security testing team of its type in the world allows NCC Group to take on PCI testing projects of all sizes, often at short notice and with challenging delivery timescales. NCC Group's comprehensive and far-reaching in-house research and development program ensures that the consultants have access to the latest tools and exploits to mimic the most sophisticated criminals. This ensures that if you remediate the vulnerabilities identified during scanning and testing you can limit your exposure to attack and keep ahead of emerging threats.

## Training and Awareness

Within PCI DSS there are a number of areas where specific training requirements are called out:

- Train developers in secure coding techniques.
- Provide training for personnel to be aware of attempted tampering or replacement of devices.
- Implement a formal security awareness programme to make all personnel aware of the importance of cardholder data security.
- Provide appropriate training to staff with security breach response responsibilities.

## PCI DSS, PA-DSS and P2PE

NCC Group is one of the world's leading providers of PCI QSA and Payment Application (PA) QSA services. Operating throughout the world, we employ a large team of QSA's for PCI, PA and point to point encryption (P2PE). NCC Group operates successfully in all sectors including retail, e-commerce, finance, transport and telecommunications, from large Level 1 entities to the smallest, local Level 4 merchants.

NCC Group's approach to helping clients with their PCI compliance programs is advisory in nature rather than audit-based, and has services including; Scope Review and Validation, Gap Analysis and Project Review, Strategic Options Analysis (e.g. P2PE, Tokenisation, Segmentation), Distressed Project Review, Remediation (remote and onsite support), Compliance Manager, PCI Client Advisory Documents (PCADs), Pre-Assessment and Assessment. NCC Group has successfully guided more than 300 organisations through their PCI compliance journey and currently performs around 50 formal PCI assessments per year.

---

# PCI Card Production Audits

By conducting security inspections of your card production facility, NCC Group is able to advise you of areas of improvement against requirements. NCC Group works with you to achieve compliance to payment scheme requirements including:

- MasterCard
- Visa Inc. and Visa Europe
- China Union Pay (CUP)
- American Express

NCC Group is the only organisation globally that can audit against all four card brands above and has delivered the first approved remote assessment during the COVID-19 lockdown.

## Other Services for the Payment Card Industry

### Consultancy

We provide sound advice and practical assistance to card vendors building up their facilities from 'zero' or introducing new services into the current layout. We can both review and document new policies and procedures, design network architecture, provide guidance on High Security Area (HSA) physical design layouts, gap analysis, pre-assessments and much more.

### Over-The-Air (OTA) Personalisation Assessments

NCC Group has significant experience in delivering consultancy services and certification assessments of the mobile provisioning facilities. Our understanding of the commonalities and differences between the OTA provisioning standards of the major payment schemes helps us efficiently deliver combined certification assessment in a single visit.

### Cloud-based Payment Provider Security Assessments

Introduction of Host Card Emulation (HCE) technology is a significant development in the mobile payment industry which supports contactless payments made using NFC-enable mobile devices that removes the need to have a secure element on these devices. NCC Group works with the Cloud-Based Payment Platform providers to assess physical and logical security systems supporting all stages of the HCE-based payment.

### 3-D Secure Assessments

The three domains of the 3-D Secure service (Issuer, Acquirer and Interoperability Domains) provide secure protocols enabling enrolment of cardholders in the 3-D Secure service and secure exchange of data between the issuer and merchant in order to authenticate the cardholder during the e-commerce purchase. NCC Group is accredited to perform certification assessments of facilities seeking Visa Inc. 3-D Secure certification (also known as Verified by Visa or VbV) of Access Controls Server and Enrolment Server services.

### PIN Security Assessments

NCC Group is accredited to perform PCI PIN Security assessments. Compliance to PCI PIN Security is mandatory for any organization providing management, processing, and transmission of personal identification number (PIN) data during online and offline payment card transaction processing at ATMs and attended and unattended point-of-sale (POS) terminals.

NCC Group has been certified to perform PIN Security Assessments since 2015 and has performed assessments in Europe, Middle East, Africa, Asia, North and Central America.

### PCI DSS, PA-DSS and P2PE

NCC Group is one of the world's leading providers of PCI QSA and PAQSA services. Operating throughout the world we employ a large team of QSA's for PCI, PA and P2PE. We operate successfully in all sectors including retail, e-commerce, finance, transport and telecommunications, from large Level 1 entities to the smallest local Level 4 merchants. Our approach to helping our clients with their PCI compliance programs is advisory in nature rather than audit-based, and our services include; Scope Review and Validation, Gap Analysis and Project Review, Strategic Options Analysis (e.g. P2PE, Tokenisation, Segmentation), Project Review, Remediation (remote and onsite support), Compliance Manager,

PCI Client Advisory Documents (PCADs), Pre-Assessment and Assessment. We have successfully guided more than 300 organisations through their PCI compliance journey and currently perform around 50 formal PCI assessments per year

---

When producing payment cards, whether manufacturing the cards or applying information in the personalisation process, security is paramount.

Any failings in your systems could compromise that security with potentially catastrophic results for your business. Compliance shouldn't be a tick box exercise, but rather an on-going task at the heart of your business. If security is not comprehensive, the risk of fraud is heightened leaving the card production bureau to deal with the consequences.

As a service provider to MasterCard, Visa, American Express, China Union Pay and GSMA, we provide logical and physical assessments for Payment Card Scheme Certification globally. We were the first company to conduct card production assessments on behalf of the payment schemes and have over many years gained unrivalled experience and expertise in the card vendor industry. We will work with you and your staff to achieve compliance to the payment scheme requirements in the most pragmatic and efficient way.

We are without equal in this area and our industry experience will guarantee that your security measures are up to the job. As a service provider to all major payment schemes, we provide logical and physical assessments for Payment Card Scheme Certification globally. We have a reputation for providing the very best service, and we will make sure that your reputation matches ours.

## **Mobile Phone and Internet of Things Security**

### **GSMA SAS-SM Audits**

There is an increasing use of embedded SIMs (eUICC) in phones, smartwatches, automobiles, smart meters and other products, facilitating 'over the air' provisioning of subscriber tailored services.

A GSMA Security Accreditation Scheme-Subscription Management (SAS-SM) audit is a logical and physical security assessment which takes place at facilities where they personalise the "Profile" that is applied via "Remote SIM provisioning" to either an eSIM or iSIM.

NCC Group has been accredited as a GSMA SAS-SM security assessor to perform assessments of remote SIM provisioning for either a consumer device or a M2M/IoT device.

NCC Group also provide consultancy services to GSMA SM service providers who either wish to develop a brand new provisioning facility or to expand their operations within a current location. We can both review and document new policies and procedures, design network architecture, provide guidance on High Security Area (HSA) physical design layouts, gap analysis, pre-assessments and much more.

---

# 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](mailto:bidteam@nccgroup.com)**